Oldenbourg Verlag

Marie-Theres Tinnefeld, Benedikt Buchner,
Thomas Petri

Einführung in das Datenschutzrecht

Datenschutz und Informationsfreiheit in europäischer Sicht

5. Auflage

Einführung in das Datenschutzrecht

Datenschutz und Informationsfreiheit in europäischer Sicht

von
Prof. Dr. iur. Marie-Theres Tinnefeld
Hochschule München

Prof. Dr. iur. Benedikt Buchner
Universität Bremen

Dr. iur. Thomas Petri
Bayerischer Landesbeauftragter für den Datenschutz

5., vollständig überarbeitete Auflage

Oldenbourg Verlag München

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Rosenheimer Straße 145, D-81671 München
Telefon: (089) 45051-0
www.oldenbourg-verlag.de

Lektorat: Christiane Engel-Haas, M.A.
Herstellung: Constanze Müller
Titelbild: thinkstockphotos.de
Einbandgestaltung: hauser lacour
Gesamtherstellung: Grafik & Druck GmbH, München

Dieses Papier ist alterungsbeständig nach DIN/ISO 9706.

ISBN 978-3-486-59656-4

Inhaltsverzeichnis

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

1.2 Internetkommunikation und technischer Grundrechtsschutz

Im Zusammenhang mit den neuen **Technologien** zeichnet sich zunehmend eine **kulturelle Wende** in Verbindung mit einer globalen Kommunikationsstruktur ab.[69] Das Denken und Tun des Menschen ist zwar nach wie vor durch seine Kultur (in Stamm, Volk, Nation, Religion, Klasse usw.) geprägt. Es wird aber mehr und mehr durch die Internetkommunikation verändert.

> *„Wir sind sprachliche Wesen. Wir verstehen uns nur im Gespräch mit anderen. Erzählend entwickeln wir unsere Vorstellung von uns selbst. Von unserer Herkunft erfahren wir durch die Geschichten, die erinnerten, die erfundenen unserer Vorfahren, von uns selbst erfahren wir durch die Reaktionen der anderen. Als solche sprachlichen Wesen, die sich dialogisch, mit und durch andere begreifen, sind wir abhängig davon, dass wir unsere Erfahrungen in eine Geschichte betten können. Wie mäandernd sich unsere Leben auch ihren Weg bahnen, suchen wir doch danach, den Verlauf in ein Narrativ bringen zu können.[…]. Durch Anerkennung oder Abweisung der Gegenüber zeichnen sich unsere Eigenarten und Andersartigkeiten, Ähnlichkeiten und Verschiedenheiten, unsere Individualität also, erst ab und aus.“*[70]

Oder anders ausgedrückt: Andere Menschen bilden online und offline das soziale Umfeld, in dessen Rahmen sich der Einzelne kulturell entfaltet.[71]

Im Internet konnte bisher niemand sicher wissen, wer der Kommunikationspartner war. Jedem war es möglich, prinzipiell jedwede „Identität“ annehmen, die nichts oder wenig mit ihm als „Persönlichkeit“ zu tun hat. Die Zeit, in der das Internet ein anonymes Medium war, wo jeder in der Maske eines Anderen auftreten konnte, wo, so die Worte auf der berühmten New Yorker Karikatur von Peter Steiner (1993) „nobody knows you’re a dog“, wandelt sich. Das Internet wird zunehmend zu einem Medium der personalisierten Suche und Analyse, wo die Ergebnisse für neue Zwecke (z. B. durch Auslesen von Profildaten für das Beschäftigtenverhältnis, für speziell ausgesuchte Werbung oder für „Friendfinder“ in sozialen Netzwerken) verwandt werden.[72] Die umstrittene anlasslose Speicherung von Daten über die näheren Umstände einer Telekommunikation (Verkehrsdaten) für Zwecke der Strafverfolgung ist ein besonders aussagekräftiges Beispiel für die Tendenz, unbeobachtete menschliche Kommunikation zu eliminieren. Vor dem Hintergrund dieser Entwicklung ist es fraglich, ob und wie Kommunikationspartner noch anonym an vertrauliche Nachrichten gelangen können.

Zahlreiche Menschen, insbesondere Jugendliche, erproben neue kommunikative Rollen im World Wide Web (WWW). In welcher Gestalt und in welcher Rolle (identifizierbar, anonym oder pseudonym) wollen und können sie ihre Privatheit und Selbstbestimmung leben? Im Zusammenhang mit den technischen Möglichkeiten und Maßnahmen zum Schutz der Privat-

---

69 Raschèr/Reichenau in Mosimann/Renold/Raschèr (Hg.), Kultur, Kunst und Recht (2009), 1. Kap. § 1 Rn. 10.

70 Emcke, Stumme Gewalt, ZEITmagazin Leben 37 2007, S. 45.

71 Dazu Suhr, Entfaltung des Menschen durch den Menschen (1976), S. 78 f.

72 Übersicht bei Pariser, The Filter Bubble (2011), S. 6 ff.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

heit sind die dafür wesentlichen Begriffe der Anonymität, Pseudonymität und Vertraulichkeit näher zu betrachten.

Die Sprache gibt erste Hinweise auf die Bedeutung von **Anonymität**. Das Wort ist griechischen Ursprungs. „An-onymus“ ist der Namenlose, aber auch der Un-Bekannte, den man nicht kennt oder der nicht identifiziert werden kann. Menschen identifizieren sich gegenseitig vornehmlich über ihren Namen. Damit wird bereits deutlich, dass Anonymität sich auf zwei oder mehrere Parteien beziehen kann.

Beispiele: Der Sender einer Nachricht will gegenüber seinem Kommunikationspartner unerkannt, also anonym bleiben. Der Patient möchte nicht, dass seine Kommunikation mit einem Arzt gegenüber Dritten offenbar wird. Sie soll „geheim“ und vertraulich bleiben. In der Verbindung Arzt-Patient wird der Inhalt der Kommunikationsbeziehung als solche durch das Patientengeheimnis und ggf. durch das Telekommunikationsgeheimnis geschützt.

Rechtlich handelt es sich um „Senderanonymität“, wenn der Empfänger einer Nachricht nicht weiß, wer sie verschickt hat. Dagegen spricht man von „Empfängeranonymität“, wenn der Sender eine Nachricht abschicken kann, ohne, dass er weiß, wer der Empfänger ist. Technisch gesehen wäre bei einer Web-Anfrage Senderanonymität gegeben, wenn der Rechner nicht einem bestimmten Webserver zugeordnet werden kann.[73]

Beispiel: Ein Aidsverdächtiger möchte, dass sein HIV-Test anonym durchgeführt wird. Der Getestete kann zu diesem Zweck ein Codewort mit der testenden Stelle vereinbaren und darüber das Ergebnis der Blutuntersuchung erfahren. Das Verfahren ist aufgrund des Selbstbestimmungsrechts der betroffenen Person geboten und auch möglich, da die testende Einrichtung bei einem positiven Ergebnis keine namentliche Meldepflicht an das Robert-Koch-Institut in Berlin hat, das für seine Zwecke nur die Anzahl der infizierten Personen, nicht aber die persönliche Zuordnung der besonderen (sensiblen) Information benötigt.[74]

Anonymität hat pragmatisch betrachtet immer auch etwas mit den konkreten Gefährdungslagen zu tun, aus denen heraus sich der wesentliche Inhalt, das Ausmaß und die Wirkungen des grundrechtlichen Schutzes bestimmen lassen.

Beispiele: Bankräuber maskieren sich, um eine Bank auszurauben. Sie wollen anonym bleiben, damit ihnen die Tat nicht zugerechnet werden kann. Whistleblower, die erhebliche Missstände in ihrer Firma öffentlich machen, wollen anonym bleiben, um vor einer Kündigung durch den betroffenen Arbeitgeber geschützt zu sein. Wenn ihnen die Meldung nicht zugerechnet werden kann, ist es aber für einen anderen angeschuldigten Mitarbeiter wesentlich schwerer, sich zu rechtfertigen. Datenschutzrechtlich ist ein Verfahren zu suchen,

73 Ausführlich Brunst, Anonymität im Internet (2009), S. 7–31.

74 Vgl. § 7 Abs. 3 Nr. 2 i.V.m. Abs. 2 IFSG. Damit identische Fälle nicht mehrfach erfasst werden, muss eine fallbezogene Verschlüsselung übermittelt werden.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

dass auch den Angegriffenen schützt.[75] Strafverfolgungsbehörden nutzen deanonymisierende Elemente wie biometrische Merkmale, DNA-Material, Daten aus einer Videoüberwachung, um verdächtige Personen zu identifizieren oder anlasslos gespeicherte Telekommunikationsdaten, um mögliche Täter zu finden.[76]

Beispiel: Informanten von Journalisten wollen anonym bleiben. In Fällen schwerer Kriminalität und Menschenrechtsverletzungen (z. B. Folter) hängt häufig der Schutz ihres Lebens davon ab, dass sie unbekannt bleiben. Der EGMR hat den Schutz journalistischer Quellen als eine der Grundbedingungen der Pressefreiheit und als wichtigen Beitrag zur Meinungsfreiheit anerkannt.[77] Anonymität steht daher häufig nicht nur im Zusammenhang mit dem Schutz der Privatheit, sondern auch mit den Möglichkeiten der freien Meinungsäußerung und der Informationsfreiheit.

In der Realität liegt Anonymität immer nur relativ vor. Die Frage ist, welche zusätzlichen Informationen mit welchem Aufwand für eine De-Anonymisierung notwendig sind. Roger Dingledine formuliert treffend: „[…] the question shifts from, is it anonymous? to is it anonymous enough?“[78] Es gibt verschiedene Auffassungen darüber, wie Anonymität zu definieren ist. Die Informatik orientiert sich an internationalen Standards (z. B. an ISO 15408) und spricht von einem Zustand, in dem jemand oder etwas innerhalb der ihn umgebenden Subjekte nicht identifizierbar ist (Anonymitätsset).[79] Das Risiko personenbezogener Datenspuren im vernetzten Internet lässt sich durch Maßnahmen der Nutzer oder durch die Inanspruchnahme von Anonymisierungsdiensten (z. B. von AN-ON) oder anderen datenschutzfördernden Techniken (z. B. attributbasierter Zertifikate) selbst minimieren. Sie sind Teil begrenzter Möglichkeiten des **Selbstdatenschutzes**. Werden mehr als nur die erforderlichen Informationen offenbart, dann erhöht sich die Gefahr des Identitätsmissbrauches, etwa im Rahmen mobiler sozialer Netzwerke. Ein gewisses Dilemma ergibt sich allerdings für die Sicherheitsbehörden: Der kriminelle Nutzer soll enttarnt, der unbescholtene Nutzer aber nicht identifiziert werden.

In vielen Fällen, in denen von Anonymität die Rede ist, handelt es sich allerdings um pseudonyme Konstruktionen. Unter dem aus dem Griechischen kommenden Begriff **Pseudonym** wird ein Deckname verstanden. Die Handlungen eines pseudonymen Nutzers sind mit einer alternativen Identität, etwa einem frei gewählten Nutzernamen oder auch einer Nummer verbunden.

Beispiel: Ein weltberühmtes Pseudonym war „Deep Throat“. Unter diesem Decknamen gab der wichtigste Informant in der Watergate-Affäre (1972–1974) Journalisten der Washington Post Einblicke in korruptes Regierungsverhalten, die zum Rücktritt des US-

75 Tinnefeld/Rauhofer, DuD 2008, 717 ff. m.w.N.

76 Zur Verfassungswidrigkeit und zur Datenschutzfrage in Europa vgl. Petri, DuD 2011, 607 ff.

77 EGMR v. 27.03.1996, MR 1996, 123 ff.; zum Schutz des Vertrauensverhältnisses von Informanten vgl. BVerfG v. 27.02.2007, BVerfGE 117, 244 ff.

78 Dingledine, The Free Haven Project (2000), S. 11.

79 Pfitzmann/Hansen, Anonymity, Unlikability. Undetectability, Unobservability, Pseudonymity, and Identity Management – A consolidated proposal for Terminology (2008).

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Präsidenten Nixon führten.[80] Die Zuordnung des Pseudonyms zum „realen" Namen des Agenten William Mark Felt wurde 30 Jahre lang geheim gehalten.[81] Mit dem Skandal verbunden ist gleichzeitig ein Plädoyer zugunsten einer allgemeinen Zugänglichkeit von Regierungsunterlagen (freedom of information).[82]

Pseudonymität ermöglicht es den interagierenden Parteien, dass sie untereinander erkennbar bleiben (z. B. im rechtsgeschäftlichen Verkehr bei Karten einer Payback-Gruppe oder in Mobiltelefonen mit SIM- und E-Mail-Nummer). Sicherheitsbehörden decken nicht nur Pseudonyme auf, sondern nutzen sie ihrerseits, um etwa im Rahmen von Zeugenschutzprogrammen Informanten eine Tarnidentität zu geben[83] oder verdeckte Ermittlungsaufgaben durchzuführen.[84] Denkbar ist auch, dass Anbieter eine Reihe von Interessensdaten beobachten, ohne die Betroffenen zu identifizieren (Datensammlung unter Pseudonym). Das kann dazu führen, dass Nutzer Angebote erhalten, die für sie nicht transparent sind.[85]

Anonymität und Pseudonymität betreffen die Identität der Partner. Dagegen bezieht sich der Begriff **Vertraulichkeit** auf den Inhalt einer übertragenen Information, der nur für Befugte zugänglich sein soll. Im Hinblick auf die digitale Kommunikation bedeutet dies, dass Sender und Empfänger Informationen austauschen können, zu denen eine dritte Partei keinen Zugang hat.

Beispiel: Anonymisierungsdienste haben die Aufgabe, den Nutzer gegenüber einem Anbieter unkenntlich zu machen. Wenn zusätzlich der Datenverkehr zwischen Nutzer und Anonymisierungsdienst verschlüsselt wird, kann auch ein externer Beobachter nicht erkennen, welche Inhalte zwischen Nutzer und Anbieter vertraulich ausgetauscht werden.

Der Vertraulichkeitsschutz steht im Zentrum des grundrechtlich verankerten Post- und Fernmeldegeheimnisses. Exemplarisch hat der EGMR auf die *„Bedeutung einer richterlichen Kontrolle auf einem Gebiet [hingewiesen], in dem Missbräuche in Einzelfällen so leicht möglich sind und derart schädliche Folgen für die demokratische Gesellschaft insgesamt haben können"*.[86]

80 Detaillierter Überblick bei Bernstein/Woodward, All The President's Men (1974).

81 Day, Credit Management 04/2006, 38 f.

82 Vgl. etwa den novellierten Freedom of Information Act von 1974, der US-Behörden dazu verpflichtet, den Bürgern größtmögliche Akteneinsicht zu gewähren. Abrufbar unter: http://www.loc.gov/rr/frd/Military_Law/pdf/FOIA-1974.pdf (letzter Abruf 22.03.2012).

83 § 5 ZSHG.

84 § 110a Abs. 1 StPO.

85 Vgl. europäische Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy) in der Fassung der Richtlinie 2009/136/EG v. 25.11.2009.

86 EGMR v. 06.09.1978, EGMR-E 1, 320 ff.; vgl. auch EGMR v. 25.03.1998, StV 1998, 683 ff.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

stützt,[31] im anderen Fall dagegen auf den Verstoß gegen das AGB-rechtliche Transparenzgebot des § 307 Abs. 1 S. 2 BGB.[32] Im praktischen Ergebnis spielt es jedoch auch keine Rolle, ob eine Einwilligungsklausel bereits aufgrund der spezifisch AGB-rechtlichen Vorgaben der §§ 305 ff. BGB unwirksam ist oder erst aufgrund der Unvereinbarkeit der Klausel mit datenschutzrechtlichen Grundgedanken.

Beispiele aus der Rechtsprechung zur Wirksamkeit formularmäßiger Einwilligungserklärungen:

- BGHZ 95**,** 362 (SCHUFA-Klausel): Eine pauschale Einwilligungsklausel, die sich nicht auf bestimmte Daten beschränkt, ist mit den Grundgedanken des BDSG nicht vereinbar und daher unwirksam.
- BGH NJW 2003, 1237: Eine widersprüchlich oder unklar gefasste Einwilligungsklausel stellt eine unangemessene Benachteiligung nach § 307 Abs. 1 S. 2 BGB dar.
- OLG Köln DuD 2002, 436: Eine in Fettdruck gehaltene Einwilligungsklausel genügt nicht dem Hervorhebungsgebot des § 4a Abs. 1 S. 4 BDSG, wenn daneben auch andere Einwilligungsklauseln im Fettdruck gestaltet sind.
- BGH DuD 2010, 493 (Happy Digits): Eine freiwillige Entscheidung des Verbrauchers i.S.v. § 4a Abs. 1 S. 1 BDSG ist gewahrt, wenn auf die Möglichkeit der Streichung der Einwilligungsklausel hingewiesen wird.

2.2 Wirksamkeit der Einwilligung

Damit eine Einwilligung wirksam ist und eine Datenverarbeitung nach § 4 Abs. 1 BDSG legitimieren kann, müssen verschiedene formale und inhaltliche Voraussetzungen erfüllt sein. Ist dies nicht der Fall, bleibt es beim grundsätzlichen Verbot der Datenverarbeitung nach § 4 Abs. 1 BDSG, insbesondere kann sich die datenverarbeitende Stelle nicht hilfsweise doch wieder auf einen gesetzlichen Erlaubnistatbestand stützen, wenn sie gegenüber dem Betroffenen zum Ausdruck gebracht hat, dass es für die Zulässigkeit der Datenverarbeitung auf seine Entscheidung ankommen soll.[33]

2.2.1 Freiwilligkeit der Einwilligung

Nach § 4a Abs. 1 Satz 1 BDSG muss die Einwilligung insbesondere „auf der freien Entscheidung des Betroffenen“ beruhen. Der Gesetzgeber hat damit Art. 2 lit. h der EG-Datenschutzrichtlinie von 1995 umgesetzt, wonach eine Einwilligung „ohne Zwang“ des Betroffenen abgegeben werden muss.[34] Legitimationsgrundlage für eine Verarbeitung personenbezogener Daten ist die Einwilligung also nur dann, wenn sich der Betroffene bei Abgabe der Einwilligung nicht in einer faktischen Zwangssituation befunden hat.[35]

---

31 BGH v. 19. 09. 1985, BGHZ 95, 362, 367.

32 So BGH v. 23. 01. 2003, NJW 2003, 1237, 1241.

33 Zum Verhältnis zwischen Einwilligung und gesetzlichen Erlaubnistatbeständen s. oben Kap. 2.1.2.

34 Siehe auch Däubler in Däubler/Klebe/Wedde/Weichert, BDSG (3. A. 2010), § 4a Rn. 20; Gola/Schomerus, BDSG (10. A. 2010), § 4a Rn. 6.

35 Simitis in ders. (Hg.), BDSG (7. A. 2011), § 4a Rn. 62.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

Das Problem der faktischen Zwangs

Eben in einer solchen faktischen Zwangssituation befindet sich der Betroffene aber in vielen Fällen, oftmals hat der Einzelne praktisch gar keine andere Wahl als eine Einwilligung in die Verarbeitung seiner personenbezogenen Daten zu erteilen.

Beispiele: Der Einzelne muss die SCHUFA-Klausel der Banken unterschreiben, wenn er ein Konto eröffnen oder einen Kredit in Anspruch nehmen möchte; der Bewerber für einen Arbeitsplatz muss, möchte er einen Arbeitsvertrag bekommen, einer Erfassung seiner Daten zustimmen; der potentielle Versicherungsnehmer muss sich mit einer Verarbeitung seiner gesundheitsbezogenen Daten einverstanden erklären, möchte er eine Lebens- oder Krankenversicherung abschließen.

Die Möglichkeit, sich den Informationsinteressen der verantwortlichen Stellen zu entziehen oder zumindest Einfluss auf deren Art und Weise der Datenverarbeitung auszuüben, ist in all diesen und ähnlichen Fällen tatsächlich nicht gegeben.[36] Zwar ist der Einzelne immer noch „frei", den Vertrag als ganzen abzulehnen und sich damit auch der Datenverarbeitung zu entziehen, gerade in solch Fällen wie dem Abschluss eines Girokonto-, Arbeits- oder Versicherungsvertrags ist diese Freiheit aber nur eine theoretische, weil der Einzelne tatsächlich auf solcherlei Leistungen angewiesen ist.

SCHUFA-Entscheidung des BGH

Der BGH hat das Problem der fehlenden Freiwilligkeit bereits vor mehr als zwanzig Jahren in seiner SCHUFA-Entscheidung kritisiert. Der Gerichtshof betont in dieser Entscheidung, dass in all den Fällen, in denen der Betroffene auf einen Vertragsschluss *angewiesen* ist, dieser Vertragsschluss aber von einer Einwilligung in die Datenverarbeitung abhängig gemacht wird, tatsächlich keine echte Entscheidungsfreiheit besteht, sondern die Einwilligung in solcherlei Konstellationen zu einer **„reinen Formalität absinkt"**.[37]

Grundsätzlich gilt nach der Rechtsprechung des BGH, dass es immer dann an einer Freiwilligkeit der Einwilligung fehlt, „wenn die Einwilligung in einer Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird".[38] Eben dies ist aber in den eben geschilderten Konstellationen regelmäßig der Fall.

Dessen ungeachtet wird jedoch die rechtliche Wirksamkeit solcherlei Einwilligungserklärungen heute praktisch nicht mehr in Frage gestellt, im Fall der SCHUFA-Klausel etwa mit der Begründung, dass es auf Seiten der kreditgebenden Wirtschaft ein „berechtigtes Informationsinteresse" gebe, das Risiko möglicher Kreditausfälle möglichst gering zu halten.[39] Im Versicherungsbereich wird sogar dahingehend argumentiert, dass es „angesichts der millio-

36 Vgl. BVerfG v. 19.10.1993, BVerfGE, 89, 214, 232; BVerfG v. 26.07.2005, BVerfGE 114, 1 34 f.; BVerfG v. 23.10.2006, RDV 2007, 20, 22. Siehe zum Problem des faktischen Zwanges auch Petri, RDV 2007, 153, 154; Buchner, Informationelle Selbstbestimmung (2006), S. 139.

37 BGH v. 19.09.1985, BGHZ 95, 362, 368.

38 BGH v. 16.07.2008, DuD 2008, 818, 820; BGH v. 11.11.2009, DuD 2010, 493, 495.

39 S. etwa Kamlah, MMR 1999, 395, 397; Kloepfer/Kutzschbach, MMR 1998, 650, 652; kritisch dazu Petri, RDV 2007, 153, 156.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

nenfach unterzeichneten Einwilligungserklärungen nur theoretische Bedeutung haben“ kann, ob die Einwilligung in eine Datenverarbeitung zu Versicherungszwecken tatsächlich freiwillig erfolgt ist oder nicht.[40] Sonderlich überzeugen können solcherlei Argumente nicht, gerade letzteres Argument der „Macht des Faktischen“ ist mehr als fragwürdig.

Umso mehr ist es daher zu begrüßen, dass für den Fall der Entbindung von der ärztlichen Schweigepflicht gegenüber einem Versicherungsunternehmen das Bundesverfassungsgericht vor einiger Zeit in aller Deutlichkeit festgehalten hat, dass eine entsprechende Einwilligung unwirksam ist, wenn sie „praktisch nicht verhandelbar“ ist und vom einzelnen Betroffenen in zu weitgehendem Umfang ein Einverständnis in die Weitergabe seiner personenbezogenen Daten abverlangt.

Wirksamkeit einer Schweigepflichtentbindungsklausel (BVerfG)[41]
Im konkreten Fall ging es um die Wirksamkeit einer Schweigepflichtentbindungserklärung, die in einem Antragsformular für Leistungen aus einer Berufsunfähigkeitsversicherung enthalten war und das Versicherungsunternehmen ermächtigte, *„von allen Ärzten, Krankenhäusern und Krankenanstalten, bei denen ich in Behandlung war oder sein werde sowie von meiner Krankenkasse: … und von Versicherungsgesellschaften, Sozialversicherungsträgern, Behörden, derzeitigen und früheren Arbeitgebern sachdienliche Auskünfte einzuholen.“*

Das Bundesverfassungsgericht stellt in seiner Entscheidung klar, dass in Konstellationen, in denen zwischen den Beteiligten ein „erhebliches Verhandlungsungleichgewicht“ besteht, eine Schweigepflichtentbindungserklärung nicht mehr als Ausdruck einer freien und selbstbestimmten Entscheidung des Betroffenen über den Umgang mit seinen personenbezogenen Daten gewertet werden kann. Wenn wie im konkreten Fall der Betroffene auf einen Vertragsschluss angewiesen ist und die Vertragsbedingungen für ihn **„praktisch nicht verhandelbar“** sind, ist es nach Überzeugung des Bundesverfassungsgerichts mit dem Recht auf informationelle Selbstbestimmung nicht mehr vereinbar, wenn sich der Betroffene in nahezu unbeschränktem Umfang mit einer Erhebung von sensiblen Gesundheitsinformationen einverstanden erklären muss, soweit diese nur irgendeinen Bezug zum Versicherungsfall haben. Das Gericht verweist darauf, dass es durchaus datenschutzfreundlichere Alternativen gibt, um auch den Informationsinteressen des Versicherungsunternehmens Rechnung zu tragen, etwa die Einholung von Einzelermächtigungen oder die Einräumung einer Widerspruchsmöglichkeit.

Die Ausführungen des Bundesverfassungsgerichts sind von ganz grundsätzlicher Bedeutung für die Rolle der Einwilligung als datenschutzrechtlicher Erlaubnistatbestand. Das Gericht geht nicht so weit, die Rolle der Einwilligung als Legitimationsgrundlage gänzlich in Frage zu stellen, auch nicht in Konstellationen, in denen zwischen den Beteiligten ein Verhandlungsungleichgewicht besteht. Was das Bundesverfassungsgericht jedoch zu Recht fordert, ist ein **Einsatz von Einwilligungsklauseln mit Augenmaß**. Je weniger frei der einzelne Betroffene in seiner Entscheidung ist, ob er sich mit einer Nutzung seiner Daten einverstanden erklären möchte oder nicht, desto sorgsamer muss bei der Formulierung einer Einwilli-

40 Naujok in Roßnagel (Hg.), Handbuch Datenschutzrecht (2003), Kap. 7.3 Rn. 34.

41 BVerfG v. 23.10.2006, DuD 2006, 817.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

gungserklärung darauf geachtet werden, dass diese nicht zu pauschal ausfällt und so dem Betroffenen jegliche Möglichkeit eines informationellen Selbstschutzes genommen wird.

Art. 7 Abs. 4 DS-GVO-E („erhebliches Ungleichgewicht")
Die Kommission hat in ihrem Vorschlag für eine Datenschutz-Grundverordnung dem Problem des faktischen Zwangs bei Erteilung einer Einwilligung explizit Rechnung getragen. Nach Art. 7 Abs. 4 DS-GVO-E soll die Einwilligung keine Rechtsgrundlage für eine Verarbeitung personenbezogener Daten bieten, „wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein **erhebliches Ungleichgewicht** besteht." Nach den Erwägungsgründen (EG 34) soll dies vor allem dann der Fall sein, wenn sich der Betroffene „in einem Abhängigkeitsverhältnis von dem für die Verarbeitung Verantwortlichen befindet"; beispielhaft wird die Verarbeitung personenbezogener Daten des Arbeitnehmers durch den Arbeitgeber im Rahmen eines Beschäftigungsverhältnisses genannt.

Koppelungsverbot

Eine besondere Ausprägung hat die Freiwilligkeitsmaxime des § 4a Abs. 1 Satz 1 BDSG im so genannten Koppelungsverbot gefunden, wie es in § 28 Abs. 3b BDSG normiert ist. Danach darf die datenverarbeitende Stelle einen Vertragsschluss nicht von einer Einwilligung des Betroffenen abhängig machen, „wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist". § 28 Abs. 3b BDSG zielt damit auf die klassischen Konstellationen eines „take it or leave it" ab, also auf Konstellationen, in denen man sich mit der Datenverarbeitung zwar nicht einverstanden erklären „muss", in denen man aber, wenn man sich nicht einverstanden erklären sollte, dann eben auch keinen Vertrag bekommt. Allerdings ist die Reichweite dieses Koppelungsverbots beschränkt, erfasst werden von diesem Verbot nur solcherlei Einwilligungserklärungen, die eine Datenverarbeitung für Zwecke des Adresshandels oder der Werbung legitimieren sollen; obige Beispielsfälle wie die SCHUFA-Klausel oder die Datenverarbeitungsklauseln in Versicherungsverträgen fallen also gerade nicht unter § 28 Abs. 3b BDSG.

Beispiele: Erfasst werden vom Koppelungsverbot etwa Fälle wie die Mitgliedschaft in einem sozialen Netzwerk, das E-Mail-Konto oder die Kundenkarte, deren Inanspruchnahme jeweils unter die Bedingung gestellt wird, dass sich der Betroffene mit einer Verarbeitung seiner Daten zu Zwecken des Marketings einverstanden erklärt.

All diese und ähnliche Geschäftsmodelle, die jeweils auf der Idee „Leistung gegen Daten" fußen, verstoßen zunächst einmal gegen die datenschutzrechtliche Freiwilligkeitsmaxime im Allgemeinen und das Koppelungsverbot des § 28 Abs. 3b BDSG im Besonderen. Im Einzelnen besteht hier jedoch noch viel Klärungsbedarf: Fraglich ist insbesondere, wann davon auszugehen ist, dass „ein anderer Zugang zu gleichwertigen vertraglichen Leistungen… nicht in zumutbarer Weise möglich ist". Mitunter wird argumentiert, dass eine solche Unzumutbarkeit schon dann vorliegt, wenn ein Alternativangebot teurer, schlechter oder nur mit größerem Zeitaufwand zu erhalten ist. All die Anbieter von kostenlosen Online-Dienstleistungen,

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

die ihr Angebot mit einer Marketing-Klausel verknüpfen, fallen nach dieser Ansicht also schon dann unter das Koppelungsverbot, wenn es zwar vergleichbare Alternativangebote gibt, diese aber nicht kostenlos sind.

Zwingend oder auch sonderlich überzeugend ist dies allerdings nicht: Zumutbar ist die Inanspruchnahme einer Leistung sehr wohl auch dann noch, wenn für sie ein normales Marktentgelt entrichtet werden muss. Ebenso ist etwa im Beispiel der Kundenkarten durchaus ein zumutbares Alternativangebot darin zu sehen, dass die gleichen Waren auch ohne Kundenkarte erworben werden können, wenn auch ohne Prämiengeschenke oder zu einem höheren Preis. Insoweit ist es wenig überzeugend, wenn ein Verstoß gegen das Koppelungsverbot allein damit begründet wird, dass die Kundenkarte selbst ohne eine Einwilligung in die Datenverarbeitung zu Marketingzwecken nicht verfügbar ist.

Schließlich kann man auch am Beispiel der **sozialen Netzwerke** wie studiVZ oder Facebook durchaus diskutieren, ob es bereits einen Verstoß gegen das Koppelungsverbot bedeutet, wenn solche sozialen Netzwerke die Teilnahmemöglichkeit zwingend von der Erteilung einer Einwilligung in die Datenverarbeitung zu Marketingzwecken abhängig machen. Selbst wenn alle sozialen Netzwerke ihr Angebot zwingend an eine solche Einwilligung koppeln sollten, ist immer noch zu fragen, ob ein zumutbares Alternativangebot nicht all die sonst zur Verfügung stehenden Kommunikationsinstrumente sein können – angefangen beim Telefon über SMS und E-Mail bis hin zu Twitter und Ähnlichem. Wie immer man sich entscheidet, wichtig ist jedenfalls festzuhalten, dass die Frage der Zumutbarkeit nicht zu streng beurteilt werden darf.

Opt-in versus Opt-out

Umstritten ist auch, ob die Freiwilligkeit einer Einwilligung möglicherweise daran scheitert, dass sich die datenverarbeitende Stelle die Einwilligung nicht in Form eines Opt-in, sondern in Form eines Opt-out einholt.

- Dass sog. **Opt-in-Modell** zeichnet sich dadurch aus, dass der Einzelne seine Einwilligung in die Datenverarbeitung ***aktiv*** erklären muss, also etwa durch Unterzeichnen einer gesonderten Einwilligungserklärung oder durch Ankreuzen eines für die Erteilung der Einwilligung vorgesehenen Kästchens.
- Beim sog. **Opt-out-Modell** wird dem Betroffenen dagegen im Ausgangspunkt zunächst einmal ein Einverständnis mit der Datenverarbeitung unterstellt, weil sich eine entsprechende Einwilligungsklausel bereits vorformuliert im Vertragswerk befindet. Es ist dann am einzelnen Betroffenen, durch Auskreuzen, Ausklicken, Durchstreichen o.Ä. diese Einwilligung im konkreten Fall wieder hinfällig zu machen.

Im Falle des Opt-out muss der Betroffene also aktiv werden, wenn er eine Datenverarbeitung nicht legitimieren will. Bleibt er hingegen untätig, sei es auch durch Nachlässigkeit, Unkenntnis oder auch aus Scheu, wird seine Einwilligung in die Datenverarbeitung ohne weiteres unterstellt. Eben deshalb ist das Opt-out-Modell bei Datenverarbeitern so beliebt und umgekehrt bei Daten- und Verbraucherschützern so unbeliebt; es bürdet letztlich dem einzelnen Betroffenen die Last zum Tätigwerden auf, wenn er die Verarbeitung seiner personenbezogenen Daten vermeiden will.

Im Falle des Opt-in-Modells ist es genau umgekehrt, Nichtstun auf Seiten des Betroffenen ist datenschutzrechtlich „ungefährlich“. Es ist hier am einzelnen Unternehmen, aktiv zu werden und seine Kunden zu Erteilung einer Einwilligung zu bewegen, wenn es eine Verarbeitung

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

personenbezogener Daten über das gesetzlich zulässige Maß hinaus anstrebt. Die Notwendigkeit einer aktiven Handlung seitens des Betroffenen stellt so betrachtet für Unternehmen eine zusätzliche Hürde dar, wenn diese Daten verarbeiten wollen.

Der BGH hat in seinen beiden Entscheidungen zu den Kundenbindungs- und Rabattsystemen Payback und HappyDigits klargestellt, dass die Wirksamkeit einer datenschutzrechtlichen Einwilligung auch im Falle eines Opt-out-Modells grundsätzlich zu bejahen ist.[42]

Die Payback-Entscheidung des BGH
Gegenstand des Payback-Verfahrens war eine vorformulierte Klausel, mit der sich die Teilnehmer am Payback-Programm damit einverstanden erklären, dass zu Zwecken der Werbung und Marktforschung ihre Daten verarbeitet werden – sowohl die persönlichen Daten (Name, Geburtsdatum, Anschrift) als auch freiwillige Daten (etwa zu Familienstand, Kindern oder Einkommen) sowie die sog. Programmdaten (Art der gekauften Waren und Dienstleistungen, Preis, Rabattbetrag, Ort und Datum des Vorgangs). Die Einwilligungsklausel ist in dem Anmeldeformular enthalten, welches die Teilnehmer vor Ausstellung der Kundenkarte ausfüllen müssen. Die Klausel befindet sich am Schluss des Textes unmittelbar vor der Unterschriftenzeile und ist schwarz umrandet sowie durch Fettdruck hervorgehoben. Rechts neben dem Einwilligungstext befindet sich ein Kästchen mit dem Text: „Hier ankreuzen, falls die Einwilligung nicht erteilt wird."

Die HappyDigits-Entscheidung des BGH
Auch bei HappyDigits ging es um eine vorformulierte Einwilligungsklausel im Anmeldeformular für das HappyDigits-Programm. Unter der Überschrift „Einwilligung in Beratung, Information (Werbung) und Marketing" erklärt sich der Teilnehmer damit einverstanden, dass seine persönlichen und freiwilligen Daten sowie seine Programmdaten zu Zwecken der Werbung und Marktforschung verarbeitet werden. Die Einwilligungsklausel ist zusätzlich umrandet und ergänzt durch den in Fettdruck gehaltenen Zusatz: „Sind Sie nicht einverstanden, streichen Sie die Klausel."

Sowohl im Fall Payback als auch im Fall HappyDigits handelt es sich damit um klassische Beispiele für ein Opt-out-Modell: Den Teilnehmern, die das Anmeldeformular unterschreiben, wird im Ausgangspunkt eine Einwilligung in die Datenverarbeitung unterstellt und es ist an diesen, diese Einwilligung wieder aus der Welt zu schaffen, indem sie sich auskreuzen (Beispiel Payback) oder sie die entsprechende Einwilligungsklausel streichen (Beispiel HappyDigits).

Nach Auffassung des BGH sind solcherlei Opt-out-Modelle datenschutzrechtlich jedoch nicht zu beanstanden. Der BGH sieht in diesem Modell – entgegen anders lautenden Stimmen in Rechtsprechung und Literatur – keinen Verstoß gegen die Freiwilligkeitsmaxime des § 4a BDSG. Freiwillig erfolgt die Einwilligung im Fall von Payback und HappyDigits aus Sicht des Gerichtshofs schon deshalb, weil die Verbraucher bei ihrer Entscheidung über den Beitritt zu diesen Rabattsystemen keinem rechtlichen, wirtschaftlichen oder faktischen Zwang unterliegen. Aus Sicht des BGH stellt es keine „ins Gewicht fallende Hemmschwelle"

42 BGH v. 16.07.2008, DuD 2008, 818, 820; BGH v. 11.11.2009, DuD 2010, 493, 495.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.

dar, wenn von dem einzelnen Verbraucher verlangt wird, dass er, wenn er mit einer Datenverarbeitung zu Marketingzwecken nicht einverstanden ist, die entsprechende Klausel durchstreichen, auskreuzen oder Ähnliches muss. Allein deshalb werde der Verbraucher nicht davon abgehalten, von seiner Entscheidungsmöglichkeit Gebrauch zu machen. Ein solches Aktivwerden sei für den Verbraucher denkbar einfach, allein deshalb gerate er noch nicht in einen schwer lösbaren Konflikt, der ihm eine freie Entscheidung unmöglich macht.[43]

Beachte: Tatsächlich ist das Einholen einer Einwilligung mittels Opt-out kein Freiwilligkeitsproblem, sondern ein **Problem des fehlenden Einwilligungsbewusstseins**. Letzteres ist Wirksamkeitsvoraussetzung jeder Einwilligung, fehlt aber regelmäßig im Falle von Opt-out-Modellen.[44]

„Übermäßige Anreize“

Diskutiert wird die Freiwilligkeit einer Einwilligung auch dann, wenn der einzelne Betroffene etwa durch Werbegeschenke, durch Gewinnmöglichkeiten oder sonstige Arten von Prämien zu einer Preisgabe seiner personenbezogenen Daten motiviert werden soll. Der BGH geht davon aus, dass es an einer freien Entscheidung des Betroffenen jedenfalls dann fehlt, wenn dieser „durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten verleitet wird“.[45] Wann ein solcher übermäßiger Anreiz allerdings anzunehmen ist, fällt schwer zu beurteilen – letztlich wird es auf die Umstände des Einzelfalls ankommen.

Beispiele: Zweifel an einer Freiwilligkeit der Einwilligung hat die Rechtsprechung im Falle einer Auslosung von Preisen in Höhe von insgesamt 22.500 DM und eines Höchstpreises von 10.000 DM geäußert.[46]

Eine die freie Willensbildung beeinträchtigende psychische Drucksituation hat die Rechtsprechung auch dann bejaht, wenn die Teilnahme an einer Verlosung von einer Einwilligung in die Datenverarbeitung zu Marketingzwecken abhängig gemacht wird und der Verbraucher von dieser Koppelung zwischen Gewinnspielteilnahme und Einwilligungserklärung erst erfährt, nachdem er sich bereits für die Teilnahme an der Verlosung entschieden hat.[47]

43 Eine andere Frage, die der BGH in diesem Zusammenhang diskutiert, betrifft die besondere Hervorhebung der Einwilligung, wenn diese zusammen mit anderen Erklärungen schriftlich erteilt werden soll – sog. Hervorhebungsgebot (§ 4a Abs. 1 S. 4 BDSG).

44 Ausführlich dazu sogleich Kap. 2.2.2.

45 BGH v. 16.07.2008, DuD 2008, 818, 820.

46 S. LG Stuttgart v. 30.08.1998, DuD 1999, 294, 295.

47 OLG Köln v. 12.09.2007 DuD 2008, 142, 144.

Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.
ISBN 978-3-486-59656-4. Oldenbourg Wissenschaftsverlag 2012.