§ 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. **die an den Betroffenen ausgegeben werden,**
2. **auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und**
3. **bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.**

(11) Beschäftigte sind:

1. **Arbeitnehmerinnen und Arbeitnehmer,**
2. **zu ihrer Berufsausbildung Beschäftigte,**
3. **Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),**
4. **in anerkannten Werkstätten für behinderte Menschen Beschäftigte,**
5. **nach dem Jugendfreiwilligendienstegesetz Beschäftigte,**
6. **Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,**
7. **Bewerberinnen und Bewerber für ein Beschäftigtenverhältnis sowie Personen, deren Beschäftigtenverhältnis beendet ist,**
8. **Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.**

Literatur: *Abel*, Rechtsfragen von Scoring und Rating, RDV 2006, S. 108; Art. 29-Datenschutzgruppe, Arbeitspapier. Privatsphäre im Internet – Ein integrierter EU-Ansatz zum Online-Datenschutz vom 21.11.2000 (WP 37); Art. 29-Datenschutzgruppe, Arbeitspapier. Datenschutzfragen im Zusammenhang mit der RFID-Technik vom 19.1.2005 (WP 105); Art. 29-Datenschutzgruppe, Stellungnahme zum Begriff „personenbezogene Daten" vom 20.6.2007 (WP 136); *Bizer*, Der Datentreuhänder, DuD 1999, S. 392; *Dammann*, Der EuGH im Internet – Ende des internationalen Datenschutzes?, RDV 2004, S. 19; *Kamlah*, Das SCHUFA-Verfahren und seine datenschutzrechtliche Zulässigkeit, MMR 1999, S. 395; *Kloepfer/Kutzschbach*, Schufa und Daten-

schutzrecht, MMR 1998, S. 650; *Koch*, Scoring-Systeme in der Kreditwirtschaft. Einsatz unter datenschutzrechtlichen Aspekten, MMR 1998, S. 458; *Mackenthun*, Datenschutzrechtliche Voraussetzungen der Verarbeitung von Kundendaten beim zentralen Rating und Scoring im Bank-Konzern, WM 2004, S. 1713; *Möller/Florax*, Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken?, NJW 2003, S. 2724; *Petri*, Das Scoringverfahren der Schufa, DuD 2001, S. 290; *Petri*, Sind Scorewerte rechtswidrig?, DuD 2003, S. 631; *Roßnagel*, Anmerkung zu EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist/Schweden*), MMR 2004, S. 99; *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, S. 721; *Taeger*, Datenschutz bei Direktmarketing und Bonitätsprüfung, in: Brunner/Seeger/Turturica (Hrsg.), Fremdfinanzierung von Gebrauchsgütern, Wiesbaden 2010, S. 51; *ULD*, Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für den Verbraucher, Schlussbericht Kiel 2006; *Weichert*, Der Schutz genetischer Informationen, DuD 2002, S. 133; *Wente*, Ist die Veröffentlichung von Daten (k-)eine Übermittlung im Sinne von § 2 Abs. 2 Nr. 2 BDSG?, RDV 1986, S. 256; *Westerholt/Döring*, Datenschutzrechtliche Aspekte der Radio Frequency Identifikation, CR 2004, S. 710; *Wuermeling*, Scoring von Kreditrisiken, NJW 2002, S. 3508.

Übersicht

I. Allgemeines

1. Gesetzeszweck

1 § 3 BDSG ist die zentrale Definitionsnorm des BDSG. Bis auf die Begriffe der öffentlichen und der nicht-öffentlichen Stelle, die in § 2 BDSG definiert sind, finden sich die für die Anwendung des BDSG wichtigsten Begriffsbestimmungen in der Vorschrift des § 3 BDSG aufgezählt. Eine weitere Definitionsnorm ist schließlich § 46 BDSG, der allerdings für die Anwendung des BDSG selbst ohne Bedeutung ist.[1]

2. Europarechtliche Grundlagen

2 Ebenso wie das BDSG mit § 3 BDSG enthält auch die EG-DSRl mit Art. 2 eine Norm mit den wichtigsten in der Richtlinie bestimmten Begriffen. Der deutsche Gesetzgeber hat mit der Novellierung des BDSG 2001 die Datenschutzrichtlinie zwar umgesetzt, zu einer vollständigen Vereinheitlichung der Terminologie in BDSG und EG-DSRl hat diese Umsetzung jedoch nicht geführt. Teilweise wurden die Begriffsbestimmungen des BDSG denen der Richtlinie zwar angepasst (so in Abs. 2, Abs. 7 und Abs. 8).[2] Insbesondere beim zentralen Begriff des „Verarbeitens" personenbezogener Daten gelten jedoch weiterhin unterschiedliche Definitionen: Während der Begriff der Verarbeitung in der Richtlinie umfassend ist und auch das Erheben und Nutzen von Daten mit einbezieht, gilt im BDSG noch immer ein enger Begriff des Verarbeitens.

II. Begriffsbestimmungen im Einzelnen

1. Personenbezogene Daten; Betroffener (Abs. 1)

a) Weites Verständnis

3 Der Begriff der personenbezogenen Daten ist von zentraler Bedeutung für die Anwendung der Bestimmungen des BDSG. Nur wenn „personenbezogene Daten" betroffen sind, ist der Anwendungsbereich des BDSG überhaupt eröffnet. Entgegen dem Wortlaut („personenbezogene Daten") reicht jedoch auch der Umgang mit einer Einzelinformation (d.h. mit einem „personenbezogenen Datum") aus, um den Anwendungsbereich des BDSG zu eröffnen.[3] Der Begriff ist grundsätzlich umfassend zu verstehen. Dies ist insbesondere auch durch die EG-DSRl vorgegeben, da es die Absicht des europäischen Gesetzgebers war, den Begriff „personenbezogene Daten" möglichst weit zu fassen. Dem ist durch eine richtlinienkonforme Auslegung auch auf nationaler Ebene Rechnung zu tragen.[4]

---

1 Näher dazu unten § 46 BDSG.

2 Siehe im Einzelnen dazu bei den jeweiligen Kommentierungen.

3 *Dammann*, in: Simitis, BDSG, § 3 Rn. 3.

4 Zur Auslegung des Begriffs der personenbezogenen Daten im Sinne der Richtlinie siehe die Stellungnahme der Art. 29-Datenschutzgruppe (Stellungnahme zum Begriff „perso-

Personenbezogene Daten sind sämtliche Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Zu den persönlichen und sachlichen Verhältnissen einer Person zählen so verschiedene Aspekte wie deren körperliche und geistige Eigenschaften (Aussehen, Gesundheit, Einstellungen, Vorlieben), ihre Verhaltensweisen und Beziehungen (beruflich, wirtschaftlich, sozial, privat) oder identifizierende Angaben (Name, Personenkennzeichen, IP-Adressen,[5] biometrische Daten[6]).[7] Unerheblich ist es für die Einordnung einer Information als personenbezogenes Datum, wie sensibel die Information ist oder in welchem Maße sie den höchstpersönlichen Bereich einer Person betrifft. Der Grad der Sensibilität personenbezogener Daten ist lediglich insofern von Bedeutung, als das BDSG – dem Vorbild der EG-DSRl folgend – innerhalb der Kategorie der personenbezogenen Daten nochmals nach personenbezogenen Daten im Allgemeinen und einer speziellen Kategorie der „besonderen Arten" personenbezogener Daten differenziert[8] und für letztere Kategorie teils strengere Anforderungen an die Zulässigkeit einer Verarbeitung stellt.[9] Inwieweit eine solche Differenzierung möglich und sinnvoll ist, ist umstritten.[10] 4

Personenbezogene Daten sind nicht nur objektive Informationen über eine Person, sondern auch Werturteile wie etwa die Einordnung als zuverlässig, kreditwürdig oder ehrlich. Die Einordnung einer Information als personenbezogenes Datum setzt nicht voraus, dass diese Information zutreffend oder bewiesen ist. Dass das BDSG auch unrichtige Informationen als personenbezogene Daten einstuft, ergibt sich bereits aus der Normierung der Betroffenenrechte auf Berichtigung, Löschung und Sperrung (§§ 20, 35 BDSG), die gerade voraussetzen, dass personenbezogene Daten unrichtig sind oder zumindest ihre Richtigkeit sich nicht feststellen lässt. 5

Auch Wahrscheinlichkeitsaussagen zu einer Person sind personenbezogene Daten.[11] Dies gilt insbesondere auch für das sog. Scoring, das durch die letzte Novellierung des BDSG erstmals in § 28b BDSG vom Gesetzgeber aufgegriffen worden ist. Charakteristisch für Scoring ist, dass auf der Grundlage mathematisch-statistischer Analysen von Erfahrungswerten aus der Vergangenheit Prognosen über das zukünftige Verhalten von Personen erstellt werden.[12] Unterschiedliche Auffassungen bestehen, inwieweit Planungsdaten (insb. die Personalpla- 6

nenbezogene Daten" vom 20.6.2007 (WP 136)). Ziel der Stellungnahme ist es, eine „gemeinsame Verständnisgrundlage" in den Mitgliedstaaten für den Begriff der personenbezogenen Daten zu schaffen.

5 Näher dazu unten Rn. 17.

6 Näher dazu unten Rn. 15.

7 *Dammann*, in: Simitis, BDSG, § 3 Rn. 10.

8 Definiert sind diese „besonderen Arten personenbezogener Daten" in § 3 Abs. 9 BDSG; siehe unten Rn. 57.

9 Siehe etwa §§ 13 Abs. 2, 14 Abs. 5 und 6, 28 Abs. 6 bis 9, 29 Abs. 5 BDSG.

10 Näher dazu unten Rn. 58.

11 *Weichert*, DuD 2002, S. 133 (134); zu den sog. Scores siehe unter Rn. 16.

12 Näher dazu unten Rn. 16 („Credit Scores").

nungsdaten von Unternehmen) personenbezogene Daten sein können. Bejaht wird dies mit dem Hinweis darauf, dass die Planungen eines Arbeitgebers über die berufliche Zukunft seiner Arbeitnehmer bereits deren gegenwärtige „Verhältnisse" nachhaltig berühren könnten.[13] Jedoch ist es für eine Qualifizierung als personenbezogene Daten nicht allein ausreichend, dass Planungsdaten Auswirkungen auf die Verhältnisse einer Person haben können. Entscheidend muss vielmehr sein, ob sich aus diesen Planungsdaten auch konkrete Informationen über die gegenwärtigen persönlichen Verhältnisse einer Person ableiten lassen. Bei abstrakten Planungsdaten eines Unternehmens ist dies nicht der Fall, diese zählen daher auch nicht zum Kreis der personenbezogenen Daten.[14]

7 Personenbezogene Daten können in beliebigen Formaten (alphabetisch, numerisch, grafisch, fotografisch, akustisch) und auf beliebigen Trägern (Papier, CD, Festplatte, Videoband) gespeichert sein.[15] Auch Proben von menschlichem Gewebe kommen als Datenträger (z. B. von genetischen Daten) in Betracht.[16]

b) Natürliche Person

8 Geschützt sind nur die personenbezogenen Daten natürlicher Personen. Von einer Einbeziehung juristischer Personen und anderer Personenmehrheiten (Personengesellschaften, Vereine, Gruppen) hat der Gesetzgeber bewusst abgesehen.[17] Im Falle einer Ein-Mann-GmbH sind jedoch die Angaben über die finanzielle Situation der GmbH, die als Teil der Angaben über die Person des alleinigen Gesellschafters und Geschäftsführers der GmbH für Kreditauskünfte gespeichert sind, zugleich personenbezogene Daten dieses Gesellschafters und Geschäftsführers.[18]

9 Im Sinne einer Vorwirkung wird auch die Einbeziehung des ungeborenen Lebens in den Schutzbereich des BDSG bejaht.[19] Daher sind etwa die vor Geburt mittels Genomanalyse gewonnen Daten über die Erbanlagen eines Nasciturus ebenfalls als personenbezogene Daten einzuordnen.[20] Ein Schutz von Verstorbenen durch das BDSG wird dagegen ganz überwiegend abgelehnt.[21]

---

13 Siehe *Gola/Schomerus*, BDSG, § 3 Rn. 9, mit dem Beispiel, dass ein hoch qualifizierter Fachmann aufgrund der Planungen seines Unternehmens in diesem keinerlei Entwicklungsmöglichkeiten mehr sieht und sich daher entscheidet, den Arbeitgeber zu wechseln.

14 Vgl. *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 34.

15 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 8; zu Bildern als personenbezogenen Daten siehe VG Wiesbaden DVBl 1981, 790.

16 *Weichert*, DuD 2002, S. 133 (134).

17 OLG Karlsruhe RDV 1987, 142; *Dammann*, in: Simitis, BDSG, § 3 Rn. 17.

18 BGH NJW 1986, 2505.

19 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 10; *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 5 und 10; *Schaffland/Wiltfang*, BDSG, § 3 Rn. 4.

20 *Weichert*, DuD 2002, S. 133 (137).

21 *Dammann*, in: Simitis, BDSG, § 3 Rn. 17; *Schaffland/Wiltfang*, BDSG, § 3 Rn. 4; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 11; für einen Schutz auch Verstorbener jedoch *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 5 ff.

c) Personenbezogenheit

Eine Personenbezogenheit von Daten ist unproblematisch immer dann anzunehmen, wenn sich ihr Informationsgehalt unmittelbar auf die persönlichen oder sachlichen Verhältnisse einer Person bezieht. Eine Krankenakte enthält unstreitig personenbezogene Daten über den Patienten, eine Beschäftigtenakte unstreitig personenbezogene Daten über den Arbeitnehmer und eine Kundendatei unstreitig personenbezogene Daten über den Kunden. Personenbezogene Daten können aber auch dann vorliegen, wenn sich Daten primär auf die Eigenschaften eines bestimmten Gegenstands, eines Prozesses oder eines Ereignisses beziehen, die Daten zugleich aber auch mit einer Person in Verbindung gebracht werden können und nicht auszuschließen ist, dass sich die Kenntnis dieser Daten auf die Rechte oder Interessen dieser Person auswirkt.[22] Daher ist beispielsweise auch der Wert einer Immobilie ein personenbezogenes Datum, wenn dieser gegenüber dem Eigentümer zur Steuerfestsetzung herangezogen wird, oder das Kundendienst-Scheckheft für ein Fahrzeug, wenn auf dessen Grundlage die Produktivität des für die Kundendienstmaßnahme zuständigen Mechanikers beurteilt wird.[23] **10**

d) Bestimmte oder bestimmbare Person

Gemäß Abs. 1 liegen personenbezogene Daten dann vor, wenn sie sich auf die Verhältnisse einer „bestimmten oder bestimmbaren" natürlichen Person beziehen. „Bestimmt" ist eine Person immer dann, wenn sie sich in einer Personengruppe von allen anderen Mitgliedern dieser Gruppe unterscheiden lässt; in erster Linie geschieht dies anhand ihres Namens. Nachdem das Gesetz zwischen Bestimmtheit und Bestimmbarkeit keinen Unterschied macht, ist letzteres Kriterium der Bestimmbarkeit das entscheidende – und klärungsbedürftige – Abgrenzungskriterium. Die „Bestimmbarkeit" einer Person setzt voraus, dass grundsätzlich die Möglichkeit besteht, ihre Identität festzustellen. Mögliche Identifizierungsmerkmale können wiederum der Name sein, ebenso aber auch alle anderen Arten von Daten wie etwa Telefonnummer, Autokennzeichen, Reisepassnummer oder eine Kombination verschiedener Kriterien (Alter, Beruf, Wohnort), die im konkreten Kontext die Wiedererkennung einer Person ermöglichen.[24] Nach der Entscheidung des EuGH in der Rechtssache *Lindqvist/Schweden* ist ein Hinweis auf einer Internetseite auf verschiedene Personen dann eine Verarbeitung personenbezogener Daten, wenn dieser Hinweis geeignet ist, die Personen „entweder durch ihren Namen oder auf andere Weise, etwa durch Angabe ihrer Telefonnummer oder durch Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigung, erkennbar zu machen".[25] Welche Informationen eine Person bestimmbar machen, lässt sich nicht abstrakt-generell beurteilen, sondern ist stets im Hinblick auf die konkreten Umstände des Einzelfalls zu beurteilen. Mitunter kann ein einzelnes **11**

22 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 10 ff.
23 Beispiele bei Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 10 ff.
24 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 15.
25 EuGH MMR 2004, S. 95 (96).

Merkmal ausreichend sein, um Daten einer bestimmten Person zuordnen zu können, mitunter kann es hierfür einer ganzen Reihe von Einzelbeschreibungen bedürfen.

12 Die Bestimmbarkeit einer Person hängt auch davon ab, wie einfach oder schwierig es ist, die für eine Identifizierbarkeit notwendigen Kenntnisse zu erlangen. Gemäß Erwägungsgrund 26 der EG-DSRl sollen bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die „vernünftigerweise" von dem verantwortlichen Datenverarbeiter oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die rein hypothetische Möglichkeit, eine Person zu bestimmen, soll daher nicht ausreichen, um diese Person als „bestimmbar" anzusehen.[26] Entscheidend ist vielmehr, ob es im Rahmen eines realistischen Aufwands an Zeit, Kosten und Arbeitskraft möglich ist, Informationen einer bestimmten Person zuzuordnen.

13 Diskutiert wird, ob das Kriterium der Bestimmbarkeit nach relativen oder objektiven Maßstäben zu beurteilen ist. Nach *Gola/Schomerus* soll es für die Bestimmbarkeit auf die Kenntnisse und Möglichkeiten der datenverarbeitenden Stelle ankommen; diese müsse den Bezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchführen können.[27] Nach *Weichert* sollen für die Bestimmbarkeit hingegen objektive Maßstäbe gelten und die Bestimmbarkeit gerade nicht nur ausschließlich nach den Kenntnissen und Möglichkeiten der datenverarbeitenden Stelle zu beurteilen sein; Daten seien daher etwa auch dann personenbezogen, wenn im Falle einer Pseudonymisierung zwar nicht die datenverarbeitende Stelle über die Zuordnungsmöglichkeiten zu einem Pseudonym verfüge, wohl aber eine andere Stelle.[28] Wie so oft dürfte die Wahrheit irgendwo in der Mitte liegen; ohnehin sollte die Entscheidung nicht an den Begrifflichkeiten relativ und objektiv aufgehängt werden. Der Sache nach geht es einerseits sicherlich zu weit, Daten immer schon dann als personenbezogen einzuordnen, wenn irgendjemand diese Daten einer bestimmten Person zuordnen kann. Andererseits darf für die Frage der Bestimmbarkeit auch nicht ausschließlich auf den Kenntnisstand allein der datenverarbeitenden Stelle selbst abgestellt werden, sondern es muss auch jedes für diese Stelle verfügbare Zusatzwissen berücksichtigt werden, egal wo dieses Zusatzwissen verortet ist. Letztlich sind daher sowohl objektive als auch relative Kriterien maßgeblich: Die Bestimmbarkeit ist zunächst einmal relativ aus der Perspektive der datenverarbeitenden Stelle zu bestimmen, wobei jedoch die Frage, welches Wissen für diese „verfügbar" ist, nach objektiven Kriterien zu bestimmen ist.

e) Betroffener

14 Im Zusammenhang mit der Legaldefinition der personenbezogenen Daten definiert Abs. 1 auch den Begriff des Betroffenen. „Betroffener" ist besagte „bestimmte oder

26 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 17.
27 *Gola/Schomerus*, BDSG, § 3 Rn. 10.
28 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 3.

bestimmbare natürliche Person", deren personenbezogene Daten erhoben, verarbeitet oder sonst wie genutzt werden. Dieser Betroffene steht im Zentrum des Regelungsgefüges des BDSG. So bedarf es insbesondere seiner Einwilligung in die Datenverarbeitung, wenn kein gesetzlicher Erlaubnistatbestand einschlägig ist,[29] es sind grundsätzlich bei ihm die personenbezogenen Daten zu erheben[30] und ihm stehen die – teils unabdingbaren – sog. Betroffenenrechte zu (Recht auf Auskunft und Benachrichtigung; Recht auf Berichtigung, Löschung und Sperrung; Widerspruchsrecht).[31]

f) Einzelne Anwendungsfälle (in alphabetischer Reihenfolge)

Biometrische Merkmale: Biometrische Merkmale sind biologische Eigenschaften, physiologische Merkmale, Gesichtszüge oder reproduzierbare Handlungen, die für eine bestimmte Person spezifisch und messbar sind. Zu den biometrischen Merkmalen zählen nicht nur die klassischen Beispiele wie Fingerabdrücke, Augennetzhaut, Gesichtsform oder Stimme, sondern auch spezielle Fähigkeiten oder sonstige Verhaltensmerkmale (z. B. Unterschrift, Tastenanschlag, charakteristische Gangart oder Sprechweise).[32] Biometrische Merkmale sind personenbezogene Daten im Sinne des § 2 Abs. 1 und zwar auch dann, wenn der Träger zunächst nicht namentlich bekannt ist. Ausreichend ist, dass er – wenn auch nur mit geringer Wahrscheinlichkeit – durch einen Vergleich ermittelt werden kann.[33] **15**

Credit Scores: Mittels Credit Scores liefern Kreditauskunfteien ihren Partnerunternehmen eine Prognose darüber, mit welcher Wahrscheinlichkeit ein potenzieller Kunde ordnungsgemäß zahlen wird oder nicht. Zu diesem Zweck ordnen Kreditauskunfteien die Daten dieses Kunden der Risikowahrscheinlichkeit einer Gruppe mit gleichartigen Merkmalen und damit einer bestimmten Risikoklasse zu. Die so erfolgte Risikoklassifizierung wird in Form eines Punktewerts („score") ausgedrückt, der umso höher ist, desto besser in der Vergangenheit die Erfahrungen mit der entsprechenden Vergleichsgruppe waren und desto positiver damit auch die Risikoprognose für den konkret angefragten Kunden ausfällt. Die datenschutzrechtliche Relevanz von Scorewerten ist früher vereinzelt noch bestritten worden.[34] Schon vor der Aufnahme von § 28b in das BDSG sind Scorewerte jedoch von der ganz h. M. als personenbezogene Daten eingeordnet und daher grundsätzlich unter die datenschutzrechtlichen Vorgaben des BDSG gefasst worden.[35] Die Verarbeitung von Scorewerten musste daher auch schon vor der letzten **16**

29 § 4 Abs. 1 BDSG.

30 § 4 Abs. 2 BDSG (Grundsatz der Direkterhebung); siehe dazu unten § 4 Rn. 56.

31 Siehe §§ 6, 19 ff., 33 ff. BDSG.

32 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 9.

33 *Dammann*, in: Simitis, BDSG, § 3 Rn. 73.

34 *Kamlah*, MMR 1999, S. 395 (400); *Wuermeling*, NJW 2002, S. 3508 (3509).

35 *Dammann*, in: Simitis, BDSG, § 3 Rn. 71; *Gola/Schomerus*, BDSG, § 3 Rn. 3a; *Abel*, RDV 2006, S. 108 (110f.); *Kloepfer/Kutzschbach*, MMR 1998, S. 650 (657); *Koch*, MMR 1998, S. 458; *Möller/Florax*, NJW 2003, S. 2724; *Petri*, DuD 2001, S. 290 (291); *Petri*, DuD 2003, S. 631 (633); *Mackenthun*, WM 2004, S. 1713 (1715).

Novellierung des BDSG insbesondere von einem gesetzlichen Erlaubnistatbestand gedeckt sein. Mit § 28b BDSG ist dieser Streit nunmehr endgültig im Sinne der h. M. entschieden.

17 IP-Adressen: IP-Adressen sind die technische Grundlage der Internet-Kommunikation; als Absender- und Zieladressen identifizieren sie die an das Internet angeschlossenen Rechner und ermöglichen so den Austausch von Datenpaketen zwischen diesen.[36] Unterschieden wird zwischen statischen und dynamischen IP-Adressen. Statische IP-Adressen sind einem bestimmten Rechner fest zugeordnet; ist der Inhaber dieses Rechners eine natürliche Person, ist ein Personenbezug im Sinne des Abs. 1 regelmäßig zu bejahen.[37] Dynamischen IP-Adressen fehlt diese feste Zuordnung, sie werden Internet-Nutzern von ihren Access-Providern vielmehr bei jedem Einwählvorgang neu zugeordnet. Gleichwohl wird auch bei dynamischen Adressen ein Personenbezug angenommen, da Access-Provider regelmäßig Datum, Zeitpunkt und Dauer der Internetverbindung und die dem Internet-Nutzer zugeteilte dynamische IP-Adresse festhalten.[38]

18 RFID-Technologie:[39] Die RFID-Technologie („Radio Frequency Identification") ist das bekannteste und datenschutzrechtlich am häufigsten diskutierte Beispiel für das Phänomen, dass infolge technologischer Miniaturisierung und Vernetzung die Datenverarbeitung zunehmend in den Alltag integriert wird und dort omnipräsent ist (sog. Ubiquitous Computing – „allgegenwärtige Datenverarbeitung"). Bei der RFID-Technologie werden sog. RFID-Tags (kleinste, an Gegenstände angeheftete Transponder) von einem Lesegerät („Reader") in einer bestimmten Frequenz bestrahlt, um dann ihre gespeicherten Daten als Antwortnachricht an diesen Reader zurückzusenden. Wurde die RFID-Technologie ursprünglich im Wesentlichen für „datenschutzneutrale" Zwecke eingesetzt (Wegfahrsperren, Lagerverwaltung, Tierkennzeichnung), bringt die aktuelle und zukünftige Entwicklung der Technologie zunehmend auch eine Gefährdung des Rechts auf informationelle Selbstbestimmung mit sich (RFID-Tags in Ausweisdokumenten, Kundenkarten etc.). Ob mittels RFID-Technologie personenbezogene Daten verarbeitet werden, hängt – wie sonst auch – davon ab, ob diese Daten im Sinne des Abs. 1 als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" zu qualifizieren sind. Zu bejahen ist dies immer dann, wenn die Informationen auf einem RFID-Tag mit den Identifizierungsdaten einer Person (Foto, Name, Anschrift, wiederkehrende Kennnummer) verknüpft werden (können).[40] Sind daher beispielsweise im Einzelhandel nicht nur die einzelnen Produkte, sondern auch die Kundenkarten mit RFID-Tags ausgestattet und ist es daher technisch möglich, einen bestimmten Artikel seinem jeweiligen Käufer zuzuordnen, so handelt es sich bei den Informationen, die das RFID-

36 *Bäumler/Breinlinger/Schrader*, Datenschutz von A-Z, I 670, S. 1.
37 *Dammann*, in: Simitis, BDSG, § 3 Rn. 63.
38 Art. 29-Datenschutzgruppe, Privatsphäre im Internet, S. 17.
39 Vgl. dazu auch *Westerholt/Döring*, CR 2004, S. 710, sowie *Schmitz/Eckhardt*, CR 2007, S. 171.
40 Art. 29-Datenschutzgruppe, RFID, S. 9.

Tag eines bestimmten Produkts übermittelt, nicht mehr nur um warenbezogene Daten dieses Produkts, sondern auch um personenbezogene Daten des Kunden.

Videoüberwachung: Grundsätzlich können auch Bildaufnahmen personenbezogene Daten im Sinne des Abs. 1 sein.[41] Der Personenbezogenheit von Videoaufnahmen steht auch nicht entgegen, dass im Falle der Überwachung öffentlich zugänglicher Räume regelmäßig nur ein ganz geringer Prozentsatz des Bildmaterials tatsächlich zur Identifizierung von Personen genutzt wird. Entscheidend ist vielmehr, dass der Zweck der Videoüberwachung gerade darin besteht, die auf den Videobildern festgehaltenen Personen zu identifizieren, wenn die für die Verarbeitung Verantwortlichen dies für notwendig halten.[42] Der Gesetzgeber hat der zunehmenden Bedeutung der Videoüberwachung durch die Aufnahme einer eigenen Sondervorschrift in das BDSG (§ 6b) Rechnung getragen. 19

2. Automatisierte Verarbeitung; nicht automatisierte Datei (Abs. 2)

Abs. 2 knüpft an Art. 3 Abs. 1 EG-DSRI an, der den Geltungsbereich der Richtlinie auf die automatisierte Verarbeitung personenbezogener Daten erstreckt sowie auf die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. In Umsetzung dieser Kategorisierung definiert das BDSG 2001 nun in Abs. 2 die Begriffe der automatisierten Verarbeitung und der nicht automatisierten Datei. 20

a) Automatisierte Verarbeitung (Abs. 2 Satz 1)

Die Hilfestellung, die die Legaldefinition der automatisierten Verarbeitung in Abs. 2 Satz 1 für die Auslegung und Anwendung des BDSG leistet, hält sich in Grenzen. Dort, wo es auf den Begriff der automatisierten Verarbeitung ankommt, nämlich bei der Bestimmung des Anwendungsbereichs des BDSG in § 1 Abs. 2 Nr. 3 BDSG und § 27 Abs. 1 BDSG, verwendet das Gesetz ohnehin nicht diesen Begriff selbst, sondern ebenfalls dessen Definition.[43] Unglücklich gewählt ist auch die Definition als solche. Letztlich ist das Kriterium, das für die Frage der Anwendbarkeit des BDSG auf die Datenverarbeitung durch nicht-öffentliche Stellen entscheidend ist, das Kriterium der „automatisierten" Datenverarbeitung; eben dieses Kriterium wird aber durch die Definition („unter Einsatz von Datenverarbeitungsanlagen") eher verallgemeinert als konkretisiert. 21

Der Begriff der automatisierten Verarbeitung ist weit auszulegen. Zu den Datenverarbeitungsanlagen im Sinne des Abs. 2 Satz 1 zählen Netzwerke und autonome PC, Groß- und Kleinstcomputer, Bürokommunikationssysteme, Aktenerschließungssysteme, digitale Bildverarbeitungssysteme (soweit eine Verknüpfung der Bilder mit personenbezogenen Daten stattfindet[44]) usw. Auf die Größe und Leis- 22

41 Siehe bereits oben Rn. 7.
42 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 19.
43 *Dammann*, in: Simitis, BDSG, § 3 Rn. 78.
44 Ausführlich *Dammann*, in: Simitis, BDSG, § 3 Rn. 79.

tungsfähigkeit der Datenverarbeitungsanlage kommt es nicht an.[45] Entscheidend ist, ob die automatisierte Verarbeitung zur leichteren Zugänglichkeit einer Datensammlung beiträgt und die Möglichkeit eröffnet, die Datensammlung nach Merkmalen auszuwerten; denn eben diese Auswertung ist das eigentliche Ziel einer automatisierten Verarbeitung.[46]

b) Nicht automatisierte Datei (Abs. 2 Satz 2)

23 Liegt keine automatisierte Datenverarbeitung vor, ist der Anwendungsbereich des BDSG bei einer Datenverarbeitung durch nicht-öffentliche Stellen gemäß §§ 1 Abs. 2 Nr. 3, 27 Abs. 1 BDSG nur dann eröffnet, wenn die Daten „in oder aus nicht automatisierten Dateien" verarbeitet, genutzt oder dafür erhoben werden. Eine nicht automatisierte Datei wird gemäß Abs. 2 Satz 1 durch vier Kriterien definiert: Es muss sich um eine nicht automatisierte Sammlung personenbezogener Daten handeln, diese muss gleichartig aufgebaut sein, nach bestimmten Merkmalen zugänglich sein und schließlich die Möglichkeit einer Auswertung eröffnen.

24 Eine Datensammlung ist bei jeder planmäßigen Zusammenstellung von Daten anzunehmen, wenn diese in einem inneren Zusammenhang zueinander stehen. Solch ein innerer Zusammenhang ist beispielsweise anzunehmen, wenn sich die Daten inhaltlich auf eine gemeinsame Personengruppe (Kunden, Arbeitnehmer) beziehen. Keine Voraussetzung für eine Sammlung ist, dass diese die Daten von mehreren Personen enthält; auch über eine Einzelperson kann eine Datensammlung angelegt werden. Die Datensammlung muss gleichartig aufgebaut sein, was dann der Fall ist, wenn alle Merkmale in einer einheitlichen Ordnung gespeichert werden. Ein solcher gleichartiger Aufbau ist zugleich auch Voraussetzung für die Zugänglichkeit der Datensammlung nach bestimmten Merkmalen (drittes Kriterium des Abs. 2 Satz 2). Erforderlich hierfür ist, dass eine Datei nach einzelnen, festgelegten Merkmalen strukturiert ist, so dass sie auch nach solchen Merkmalen durchsucht werden kann.[47] Sind diese Voraussetzungen gegeben, ist grundsätzlich auch von einer Auswertbarkeit nach bestimmten Merkmalen (viertes Kriterium) auszugehen.

3. Erheben (Abs. 3)

25 Abweichend von der EG-DSRl fällt nach dem BDSG das Erheben von Daten nicht unter den umfassenden Begriff der Datenverarbeitung, sondern steht eigenständig neben diesem. Erheben ist gemäß Abs. 3 das Beschaffen von Daten über den Betroffenen. Ein Erheben personenbezogener Daten setzt nicht zwingend voraus, dass die Daten nach dem Beschaffen auch gespeichert werden.[48] Durch die Datenerhebung erlangt die betreffende Stelle Kenntnis von den Daten und be-

45 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 45.
46 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 47; *Dammann*, in: Simitis, BDSG, § 3 Rn. 79; *Schaffland/Wiltfang*, BDSG, § 3 Rn. 96.
47 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 57.
48 OVG Münster RDV 2002, 127.

gründet ihre Verfügungsmacht über diese.[49] Auf welche Weise dies geschieht – mündliche Befragung, heimliche Beobachtung, Untersuchungen, schriftliche Anforderung von Informationen, automatischer Abruf von Daten – ist unerheblich. Auch das Extrahieren von Informationen aus Proben von menschlichem Gewebe kann eine Datenerhebung sein.[50]

Das Erheben von Daten setzt ein aktives Handeln der erhebenden Stelle voraus. Hierfür reicht es nicht aus, wenn einer Stelle infolge einer unaufgefordert eingereichten Antragstellung, Bewerbung oder Nachricht personenbezogene Daten zugehen. Auch die Datenübermittlung aufgrund einer gesetzlichen Mitteilungspflicht begründet auf Seiten der Empfangsstelle noch keine Datenerhebung. Voraussetzung ist vielmehr stets, dass die betreffende Stelle die zugegangenen Daten gezielt für einen Zweck entgegennimmt.[51] 26

4. Verarbeiten (Abs. 4)

Zum Verarbeiten von Daten gehört nach der Terminologie des BDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Die Tätigkeit des Erhebens und des Nutzens von Daten fällt demgegenüber – anders als nach der EG-DSRl – nicht unter den Begriff des Verarbeitens, sondern findet in den Bestimmungen des BDSG jeweils eine eigenständige Erwähnung und wird dementsprechend auch eigenständig im Rahmen des § 3 in den Absätzen 3 und 5 definiert. Ein stichhaltiger Grund für diese unnötige Kompliziertheit lässt sich nicht ausmachen.[52] Durch den Zusatz „ungeachtet der dabei angewendeten Verfahren" wird nochmals klargestellt, dass zur Datenverarbeitung im Sinne des BDSG die manuelle Datenverarbeitung grundsätzlich ebenso zählt wie die automatisierte Datenverarbeitung. 27

a) Speichern (Abs. 4 Satz 2 Nr. 1)

Speichern ist das „Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung". Als Datenträger kommen alle denkbaren Speichermedien in Betracht, angefangen bei der traditionellen Karteikarte bis hin zu mobilen Speicherchips. „Gespeichert" sind auch zwischengespeicherte Daten, Daten in Sicherungskopien oder in Archivbeständen.[53] Kein tauglicher Datenträger ist hingegen das menschliche Gedächtnis. Das Notieren auf einem Hand- oder Telefonzettel ist zwar grundsätzlich auch ein „Speichern"; zumindest im nicht-öffentlichen Bereich wird dieses Speichern aber regelmäßig ohne datenschutzrechtliche Relevanz sein, weil eine solche Datenspeicherung weder automatisiert noch dateigebunden ist. 28

49 *Dammann*, in: Simitis, BDSG, § 3 Rn. 102.
50 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 10.
51 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 62; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 23.
52 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 26.
53 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 78 ff.

29 Die Definition des Abs. 4 Satz 2 Nr. 1 setzt für ein „Speichern" weiterhin voraus, dass die Daten „zum Zwecke ihrer weiteren Verarbeitung oder Nutzung" gespeichert werden. Die praktische Bedeutung dieser Voraussetzung wird als gering eingeschätzt, da in der Praxis das Speichern von Daten kein Selbstzweck ist, sondern regelmäßig nur dann stattfindet, wenn die Daten auch genutzt werden sollen – sei es auch nur in der Form, dass sie für die Zukunft verfügbar gehalten werden sollen.[54]

b) Verändern (Abs. 4 Satz 2 Nr. 2)

30 Verändern ist das „inhaltliche Umgestalten gespeicherter personenbezogener Daten". Eine Veränderung liegt dann vor, wenn bereits gespeicherte Daten durch eine Aufbereitung oder Verknüpfung mit anderen Daten einen neuen Informationsgehalt bekommen. Eine bloße äußerliche Umgestaltung personenbezogener Daten, die aber deren Informationsgehalt nicht verändert, fällt nicht unter Abs. 4 Satz 2 Nr. 2.

31 An sich führt auch eine Berichtigung von Daten zu einem neuen Informationsgehalt dieser Daten; jedoch bestehen hier unterschiedliche Auffassungen, ob die Berichtigung von Daten als ein Unterfall des Veränderns anzusehen ist[55] oder ob dieser Tatbestand als ein Löschen alter und ein Speichern neuer Daten einzuordnen ist.[56] Im praktischen Ergebnis dürfte die Unterscheidung kaum eine Rolle spielen, da für das Speichern und das Verändern personenbezogener Daten jeweils die gleichen Zulässigkeitsvoraussetzungen gelten.[57]

32 Eine Datenveränderung im Sinne des Abs. 4 Satz 2 Nr. 2 ist auch das sog. Scoring. Mittels Scoring werden auf der Grundlage von bereits existierenden Daten zu einer Person Prognosen über deren zukünftiges Verhalten erstellt. Daten mit einem bestimmten Informationsgehalt (Verhalten in der Vergangenheit) wird also ein neuer Informationsgehalt (Verhalten in der Zukunft) beigemessen.[58] Damit handelt es sich beim Scoring um ein typisches Beispiel der Veränderung von Daten, das bereits unter Abs. 4 Nr. 2 fällt und nicht erst unter den Auffangtatbestand des Abs. 5 (Datennutzung).[59] Bereits vor der letzten Novellierung des BDSG musste sich daher das Scoring an der Regelung des § 29 BDSG messen lassen, der zwar nicht die Zulässigkeit des Nutzens, wohl aber die des Veränderns von Daten regelte. Mittlerweile kommt es auf diese Unterscheidung ohnehin nicht

54 Vgl. *Dammann*, in: Simitis, BDSG, § 3 Rn. 120; im selben Sinne *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 80; *Gola/Schomerus*, BDSG, § 3 Rn. 28.

55 In diesem Sinne *Gola/Schomerus*, BDSG, § 3 Rn. 31.

56 Im letzteren Sinne *Schaffland/Wiltfang*, BDSG, § 3 Rn. 66.

57 Vgl. § 14 BDSG für den öffentlichen und §§ 28, 29 BDSG für den nicht-öffentlichen Bereich.

58 Vgl. schon oben Rn. 6 und Rn. 16; siehe zu den ökonomischen Hintergründen und rechtlichen Anforderungen an Bonitätsprüfungen *Taeger*, in: Brunner/Seeger/Turturica, Fremdfinanzierung von Gebrauchsgütern, S. 51.

59 *ULD*, Scoringsysteme, S. 79; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 30; a. A. *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 125 (Datennutzung); *Petri*, DuD 2003, S. 631 (636).

mehr an, da der neue § 29 BDSG sowohl die Veränderung von Daten als auch die Datennutzung erfasst.[60]

Auch für das Anonymisieren und Pseudonymisieren von Daten wird vertreten, dass es sich hierbei um ein Verändern im Sinne des Abs. 4 Satz 2 Nr. 2 BDSG handelt.[61] Dafür spricht zunächst, dass der Gesetzgeber selbst in Abs. 6 das Anonymisieren als ein „Verändern" personenbezogener Daten definiert. Andererseits zielt ein Anonymisieren oder Pseudonymisieren darauf ab, die Zuordnung von Daten zu einer bestimmten Person aufzuheben oder zumindest wesentlich zu erschweren. Nicht aber führt ein Anonymisieren oder Pseudonymisieren zu einem neuen Informationsgehalt der betreffenden Daten und stellt daher auch kein Verändern im Sinne des Abs. 4 Satz 2 Nr. 2 dar.[62] 33

c) Übermitteln (Abs. 4 Satz 2 Nr. 3)

Übermitteln ist das „Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten". Dritter ist gemäß Abs. 8 Satz 2 jede Person oder Stelle außerhalb der verantwortlichen Stelle, nicht aber der Betroffene selbst sowie diejenigen, die Daten im Auftrag erheben, verarbeiten oder nutzen.[63] Keine Übermittlung liegt daher vor, wenn Daten an den Betroffenen oder an einen Auftragnehmer weitergegeben werden oder wenn Daten innerhalb einer datenverarbeitenden Stelle ausgetauscht werden. Im letzteren Fall kann es sich allerdings um eine Nutzung von Daten im Sinne des Abs. 5 handeln. 34

Das Übermitteln von Daten kann gemäß Abs. 4 Satz 2 Nr. 3 auf zweierlei Weise stattfinden: dadurch, dass die Daten an den Dritten weitergegeben werden, oder dadurch, dass der Dritte Daten, die zur Einsicht oder zum Abruf bereitgehalten werden, einsieht oder abruft. In welcher Form die Übermittlung stattfindet (mündlich, fernmündlich, schriftlich, auf elektronischem Wege), ist unerheblich. Nicht erforderlich ist, dass die Übermittlung gegenüber einem bestimmten Dritten erfolgt.[64] Auch die öffentliche Bekanntmachung personenbezogener Daten ist vielmehr eine Übermittlung im Sinne des BDSG.[65] 35

Auch das Einstellen von Daten in das Internet soll eine Datenübermittlung im Sinne des Abs. 4 Satz 2 Nr. 3 sein.[66] Demgegenüber hat der EuGH in der Rechts- 36

60 Siehe dazu unten § 29 BDSG.

61 Vgl. *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 30.

62 Vgl. *Gola/Schomerus*, BDSG, § 3 Rn. 31.

63 Näher zur Definition des Dritten unten Rn. 56. Zu unterscheiden ist der „Dritte" vom weitergehenden Begriff des sog. Empfängers, wie er in Abs. 8 Satz 1 definiert ist (dazu unten Rn. 55).

64 *Gola/Schomerus*, BDSG, § 3 Rn. 33; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 32.

65 Vgl. BVerfG NVwZ 1990, 1162 (öffentliche Bekanntmachung als die „intensivste Form einer Übermittlung personenbezogener Daten"); *Wente*, RDV 1986, S. 256 (257).

66 In diesem Sinne *Dammann*, RDV 2004, S. 19 (20f.); *Gola/Schomerus*, BDSG, § 3 Rn. 33; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 32.

sache *Lindqvist/Schweden* entschieden, dass das Angebot zum Abruf von Seiten aus dem Internet keine „Übermittlung" im Sinne des Art. 25 EG-DSRI darstellt. Zu berücksichtigen ist allerdings, dass Art. 25 EG-DSRI die Datenübermittlung in Drittländer betrifft und Art. 25 ff. EG-DSRI solch eine Datenübermittlung in Drittländer im Ergebnis nur bei Wahrung eines angemessenen Datenschutzniveaus in diesen Ländern zulassen. Hätte der EuGH auch das Einstellen von Daten in das – weltumspannende – Internet als „Übermittlung" im Sinne des Art. 25 eingeordnet, wäre bei Vollzug des Art. 25 das Internet in Europa weitgehend zum Erliegen gebracht worden, da sich – weltweit – wohl stets ein Land finden lässt, in dem ein angemessenes Datenschutzniveau nicht gewährleistet ist.[67] Vor diesem Hintergrund dürfte die Entscheidung des EuGH für die Auslegung des Abs. 4 Satz 2 Nr. 3 nicht ausschlaggebend sein.

37 Eine Übermittlung von Daten liegt auch bei der Weitergabe kompletter Dateien, etwa im Zuge einer Kanzlei- oder Praxisveräußerung, vor.[68] Die Rechtsprechung sieht hier die Übergabe von Mandanten- oder Patientenakten – unabhängig von der Frage einer Einordnung dieser Übergabe als Datenübermittlung – grundsätzlich nur dann als zulässig an, wenn diese mit Einwilligung der Betroffenen erfolgt.[69] Da in der Praxis diese Einwilligung regelmäßig nur schwer zu erreichen ist, werden alternativ zwei Vorgehensweisen vorgeschlagen: zum einen der Weg über ein Widerspruchsrecht des Betroffenen;[70] zum anderen das sog. Zweischränkemodell,[71] bei dem die Patientenakten in einem verschlossenen Schrank an den Erwerber übergeben werden und dieser sich verpflichtet, auf die Patientendaten nur fallbezogen und nach einem entsprechenden Einverständnis des Betroffenen zuzugreifen. Keine Einwilligung ist schließlich nötig, wenn es sich bei dem Erwerber nicht um einen außenstehenden Dritten handelt, der den betroffenen Patienten völlig unbekannt ist, sondern um jemanden, der vor Erwerb der Praxis bereits einen längeren Zeitraum in dieser mitgearbeitet und freien Zugang zu allen Akten gehabt hat.[72]

d) Sperren (Abs. 4 Satz 2 Nr. 4)

38 Sperren ist das „Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken". Das BDSG sieht in be-

67 Siehe *Roßnagel*, MMR 2004, S. 99.

68 *Gola/Schomerus*, BDSG, § 3 Rn. 35. Zur Übergabe von Patientendaten bei der Veräußerung einer Arztpraxis siehe BGH NJW 1992, 737; zur Übergabe von Mandantenakten im Rahmen einer Kanzleiveräußerung BGH NJW 2001, 2462.

69 BGH NJW 1992, 737; BGH NJW 2001, 2462; siehe auch § 10 Abs. 4 Satz 2 MBO-Ä; „Ärztinnen und Ärzte, denen bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patientinnen und Patienten in Obhut gegeben werden, müssen diese Aufzeichnungen unter Verschluss halten und dürfen sie nur mit Einwilligung der Patientin oder des Patienten einsehen oder weitergeben.".

70 *Gola/Schomerus*, BDSG, § 3 Rn. 35.

71 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 33.

72 Vgl. LG Darmstadt NJW 1994, 2962 (zur Veräußerung einer Rechtsanwaltspraxis).

stimmten Fällen eine Verpflichtung der verantwortlichen Stelle zur Sperrung von Daten vor.[73] Ziel jeder Datensperrung ist es, dass Daten nicht mehr verarbeitet oder genutzt werden, ohne dass diese aber, wie bei der Datenlöschung, unkenntlich gemacht werden. Daten können umfassend zu sperren sein, etwa wenn sich ihre Richtigkeit nicht feststellen lässt;[74] eine Sperrung kann aber auch zweckgebunden erfolgen, etwa wenn Daten „für Zwecke der Werbung oder der Markt- und Meinungsforschung" zu sperren sind.[75]

Der verantwortlichen Stelle steht es grundsätzlich frei, auf welche Weise sie eine Sperrung von Daten kenntlich machen will. Die Form der Kennzeichnung wird insbesondere davon abhängen, ob es sich um eine automatisierte Datenverarbeitung oder um nicht automatisierte Dateien handelt und ob es um die Sperrung von einzelnen Daten, von Datensätzen oder von ganzen Dateien geht. Je nachdem kann eine Kennzeichnung technisch oder textlich erfolgen, sie kann in den Datenbeständen selbst, auf den Datenträgern oder auch auf deren „Verpackung" vorgenommen werden.[76] Auch eine getrennte Aufbewahrung von Daten ist eine Form der Datensperrung. **39**

e) Löschen (Abs. 4 Satz 2 Nr. 5)

Löschen ist das „Unkenntlichmachen gespeicherter personenbezogener Daten". Ein solches Unkenntlichmachen setzt voraus, dass ein Rückgriff auf die gespeicherten Daten nicht mehr möglich ist; dies ist dann nicht der Fall, wenn Daten zwar auf einem Datenträger vollständig gelöscht sind, weiterhin jedoch auf einem anderen Datenträger gespeichert sind. Ein Löschen kann durch Unleserlichmachen, Überschreiben oder sonstige Formen der Datenbeseitigung erfolgen. Auch die Vernichtung des Datenträgers selbst ist eine Datenlöschung. Nicht ausreichend ist es, wenn Daten lediglich als ungültig oder gelöscht gekennzeichnet werden, jedoch weiterhin lesbar sind; ebenso wenig reicht die bloße Auslagerung von Datenbeständen. **40**

5. Nutzen (Abs. 5)

Anders als nach Art. 2 lit. b EG-DSRI ist das Nutzen von Daten nach der Terminologie des BDSG kein Unterfall der Datenverarbeitung, sondern steht als eigenständiger Begriff neben der Datenverarbeitung. Das Nutzen von Daten ist gemäß Abs. 5 jede Verwendung personenbezogener Daten, soweit es sich nicht um eine Verarbeitung handelt. Es handelt sich damit um einen klassischen Auffangtatbestand, der immer dann einschlägig ist, wenn eine bestimmte Art der Datenverwendung keiner Phase der Datenverarbeitung im Sinne des Abs. 4 zugeordnet werden kann. **41**

73 Siehe § 20 Abs. 3 bis 6 BDSG (für den öffentlichen Bereich) und §§ 28 Abs. 4, 29 Abs. 4, 35 Abs. 3 und 4 BDSG (für den nicht-öffentlichen Bereich).

74 Vgl. §§ 20 Abs. 4, 35 Abs. 4 BDSG.

75 Vgl. § 28 Abs. 4 BDSG.

76 *Schaffland/Wiltfang*, BDSG, § 3 Rn. 73a; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 37.

42 Ob ein Umgang mit Daten als Datennutzung im Sinne des Abs. 5 einzuordnen ist, hängt von der Verwendung des Informationsgehaltes dieser Daten ab. Wird dieser Informationsgehalt gerade in seiner Eigenschaft als personenbezogene Information gebraucht, weil sich die Verwendung von Daten auch auf deren Personenbezug erstreckt, liegt eine Datennutzung im Sinne des Abs. 5 vor.[77] Zum Tatbestand der Datennutzung zählen u. a. das Duplizieren von Daten, die Auswertung von Daten, die behördeninterne Bekanntmachung und Mitteilung von Daten oder die Mitteilung an den Betroffenen selbst.[78] Für das Scoring[79] ist der Auffangtatbestand der Datennutzung nicht von Relevanz, da das Scoring als Datenveränderung bereits unter die Kategorie der Datenverarbeitung nach Abs. 4 fällt.[80]

6. Anonymisieren (Abs. 6)

43 Das Anonymisieren personenbezogener Daten zielt darauf ab, die Beziehung zwischen diesen Daten und der Person, auf die sie sich beziehen, aufzulösen. Abs. 6 unterscheidet in seiner Definition zwei Arten des Anonymisierens. Zum einen handelt es sich dann um ein Anonymisieren, wenn personenbezogene Daten dergestalt verändert werden, dass Einzelangaben über persönliche oder sachliche Verhältnisse „nicht mehr" einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (erste Alternative des Abs. 6). Zum anderen handelt es sich auch dann noch um ein Anonymisieren, wenn die Daten so verändert werden, dass sie nur noch „mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" einer Person zugeordnet werden können (zweite Alternative des Abs. 6).

44 Während es in der ersten Alternative unstreitig ist, dass es sich bei dergestalt anonymisierten Daten nicht mehr um „personenbezogene" Daten im Sinne des BDSG handelt, wird in der zweiten Alternative trotz an sich erfolgter Anonymisierung überwiegend davon ausgegangen, dass es sich auch weiterhin um „personenbezogene" Daten handelt, die dem Schutz des BDSG unterfallen.[81] Konsequent ist diese Einordnung dann, wenn auch im Rahmen der Definition des Abs. 1 „personenbezogene Daten" immer schon angenommen werden, wenn nicht völlig auszuschließen ist, dass die Person, auf die sich die Daten beziehen, bestimmbar ist. Nach hier vertretener Auffassung soll jedoch – in Anlehnung an die EG-DSRl und deren Auslegung durch die *Art. 29 Datenschutzgruppe* – die bloß hypothetische Möglichkeit, eine Person zu bestimmen, noch nicht ausreichen, um diese Person als „bestimmbar" anzusehen und damit ein personenbezogenes Datum anzunehmen.[82] Gemäß Erwägungsgrund 26 der Richtlinie sollen vielmehr

77 OLG Köln RDV 2001, 103 (Nutzung personenbezogener Daten zu Zwecken der „Rückwärtssuche" nach Telefonnummern).

78 Weitere Beispiele bei *Dammann*, in: Simitis, BDSG, § 3 Rn. 195.

79 Zum Scoring siehe schon oben Rn. 6.

80 Siehe oben Rn. 32.

81 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 131; *Dammann*, in: Simitis, BDSG, § 3 Rn. 196; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 44.

82 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 17; siehe schon oben Rn. 12.

bei der Entscheidung, ob eine Person bestimmbar ist, alle (aber auch nur diese) Mittel berücksichtigt werden, die „vernünftigerweise" von dem verantwortlichen Datenverarbeiter oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Gleiche Kriterien müssen für die Frage der Personenbezogenheit auch im Rahmen der Anonymisierung gelten, auf die sich Erwägungsgrund 26 ebenfalls bezieht.[83] Eine Personenbezogenheit von anonymisierten Daten ist daher abzulehnen, wenn die Reidentifizierung einer Person nur durch einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft möglich ist.

Für die Frage, ob die Möglichkeit einer Reidentifizierung nach relativen oder objektiven Maßstäben zu beurteilen ist, kann ebenfalls an obige Ausführungen zur Bestimmbarkeit angeknüpft werden.[84] Maßgebend ist nicht, welches Wissen abstrakt-allgemein für eine Reidentifizierung zur Verfügung steht, sondern welches Wissen konkret gerade der datenverarbeitenden Stelle zur Verfügung steht (relativer Maßstab).[85] Hierzu zählt allerdings auch jedes außerhalb der Stelle vorhandene Zusatzwissen, sofern der Zugriff darauf keinen (nach objektiven Kriterien zu bestimmenden) unverhältnismäßigen Aufwand erfordert. 45

7. Pseudonymisieren (Abs. 6a)

Der Begriff des Pseudonymisierens ist mit dem BDSG 2001 neu in den Definitionskatalog des § 3 aufgenommen worden. Datenschutzrechtliche Verwendung hat der Begriff schon vorher in den §§ 4 Abs. 6 und 6 Abs. 3 TDDSG (nunmehr §§ 13 Abs. 6, 15 Abs. 3 TMG) gefunden.[86] Pseudonymisieren wird gemäß Abs. 6a definiert als das „Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." 46

Die Grenze zwischen Anonymisieren und Pseudonymisieren ist fließend. Hier wie dort geht es darum, die Personenbezogenheit von Daten auszuschließen oder zumindest zu erschweren. Während jedoch das Anonymisieren von Daten darauf abzielt, deren Zuordnung zu einer Person möglichst dauerhaft gegenüber jedem auszuschließen, existiert beim Pseudonymisieren eine Zuordnungsregel, die es zumindest dem Kenner dieser Regel ermöglicht, die Pseudonymisierung wieder rückgängig zu machen und den Personenbezug der pseudonymisierten Daten wieder herzustellen.[87] Allerdings kann auch ein Pseudonymisierungsverfahren so ausgestaltet werden, dass von einem Kennzeichen überhaupt nicht mehr auf eine konkrete Person rückgeschlossen werden kann und daher eine Reidentifizierung 47

83 Siehe Satz 3 des Erwägungsgrunds 26 sowie Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 24.

84 Siehe oben Rn. 13.

85 Vgl. *Gola/Schomerus*, BDSG, § 3 Rn. 44; a. A. *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 42.

86 Siehe dazu die Kommentierung bei § 13 TMG, Rn. 40, und § 15 TMG, Rn. 63.

87 *Roßnagel/Scholz*, MMR 2000, S. 721 (724).

für niemand mehr möglich ist, (irreversibles Pseudonymisierungsverfahren). Die dergestalt pseudonymisierten Daten unterfallen dann ebenso wie anonymisierte Daten nicht mehr dem Schutz des BDSG.[88]

48 Ist ein Pseudonymisierungsverfahren reversibel ausgestaltet, ist also ein Rückschluss von einem Kennzeichen auf eine konkrete Person möglich, ist je nach der Art des Pseudonyms zu differenzieren, ob die pseudonymisierten Daten als personenbezogene Daten einzuordnen sind oder nicht:[89]

49 Handelt es sich um ein sog. „selbstgeneriertes Pseudonym", hat also der Betroffene selbst sein Pseudonym ausgewählt und verfügt dieser allein über die Zuordnungsregel, fallen die pseudonymisierten Daten nicht unter den Schutz des BDSG – vorausgesetzt dass Außenstehende die Zuordnungsregel nicht entschlüsseln und auch sonst den Personenbezug der pseudonymisierten Daten nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder herstellen können.

50 Ist umgekehrt die Zuordnungsregel von einer datenverarbeitenden Stelle vergeben und verwaltet diese das Pseudonym, sind die pseudonymisierten Daten jedenfalls gegenüber dieser Stelle als personenbezogene Daten einzuordnen. Viel spricht darüber hinaus dafür, die Daten auch im Verhältnis zu Dritten als personenbezogene Daten einzustufen – zumindest dann, wenn es sich bei der datenverarbeitenden Stelle nicht um eine Stelle handelt, die mit besonderen Vertraulichkeitspflichten und -rechten ausgestattet ist, und daher nicht mit hinreichender Wahrscheinlichkeit für die Zukunft ausgeschlossen werden kann, dass die datenverarbeitende Stelle den Personenbezug der pseudonymisierten Daten gegenüber Dritten wieder herstellt.

51 Schließlich können Pseudonyme auch von einer vertrauenswürdigen Institution vergeben werden, die allein über die Zuordnungsregel verfügt und das Pseudonym nur gegenüber bestimmten datenverarbeitenden Stellen zu fest definierten Zwecken aufdeckt. Ein Beispiel für solch eine Institution ist der Datentreuhänder in der wissenschaftlichen Forschung.[90] Im Verhältnis zu dieser Institution und im Verhältnis zu denjenigen Stellen, denen gegenüber das Pseudonym bestimmungsgemäß wieder aufgedeckt werden soll, handelt es sich bei den so pseudonymisierten Daten um personenbezogene Daten. Fraglich ist, ob darüber hinaus diese Daten auch allgemein gegenüber jedem anderen Dritten als personenbezogene Daten einzuordnen sind. Letztlich kann diese Frage nur je nach Art der Institution, die mit der Zuordnungsregel betraut ist, beantwortet werden. Unterliegt diese Institution Vertraulichkeitspflichten, deren Verletzung ordnungswidrigkeiten- oder strafbewehrt ist, und ist sie überdies auch mit entsprechenden Rechten zur Geheimhaltung, gerade gegenüber staatlichen Stellen, ausgestattet, so kann mit hinreichender Wahrscheinlichkeit davon ausgegangen werden, dass die Anonymität der Da-

88 Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 21.
89 Vgl. hierzu und zum Folgenden *Roßnagel/Scholz*, MMR 2000, S. 721 (725 ff.).
90 Dazu *Bizer*, DuD 1999, S. 392 (394 f.).

ten im Allgemeinen gewahrt bleibt und es sich insoweit daher nicht um personenbezogene Daten handelt, die dem Schutz des BDSG unterfallen würden.

8. Verantwortliche Stelle (Abs. 7)

Mit dem BDSG 2001 wurde der Begriff der speichernden Stelle durch den der verantwortlichen Stelle ersetzt. Abs. 7 entspricht damit der Terminologie der EG-DSRI, die in Art. 2 lit. d Satz 1 den Begriff des „für die Verarbeitung Verantwortlichen" definiert. Definiert wird die verantwortliche Stelle in Abs. 7 als „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt." Dass im letzteren Fall der Auftragsdatenverarbeitung nicht der Auftragnehmer, sondern der Auftraggeber der „Verantwortliche" ist, der für die Einhaltung der datenschutzrechtlichen Vorgaben zu sorgen hat, ergibt sich auch nochmals ausdrücklich aus § 11 Abs. 1 BDSG. 52

Im nicht-öffentlichen Bereich gilt für die Abgrenzung der verantwortlichen Stelle eine rechtliche Betrachtungsweise. „Verantwortliche Stelle" ist die juristische Einheit (die juristische Person, die Gesellschaft oder andere Personenvereinigung), nicht dagegen die einzelne Abteilung oder unselbstständige Zweigstelle eines Unternehmens. Auch ein Konzernprivileg kennt das BDSG nicht.[91] Auch hier kommt es auf die rechtliche Selbstständigkeit an; jede juristisch selbstständige „Konzerntochter" ist – ungeachtet einer wirtschaftlichen Einheit – jeweils auch eine verantwortliche Stelle. 53

Im öffentlichen Bereich sind nicht die juristischen Personen (Bund, Länder, Gemeinden), sondern die in § 2 Abs. 1 und 2 BDSG definierten öffentlichen Stellen die „verantwortlichen Stellen". Für Behörden gilt wiederum nicht der funktionale, sondern der organisatorische Behördenbegriff.[92] Verantwortliche Stellen sind daher niemals die unselbstständigen internen Untergliederungen einer Organisationseinheit (z. B. die einzelnen Abteilungen eines Ministeriums oder die Ämter einer Gemeinde), sondern stets nur die Organisationseinheit im Ganzen (z. B. Ministerium, Gemeinde). 54

9. Empfänger; Dritter (Abs. 8)

a) Empfänger (Abs. 8 Satz 1)

In Umsetzung von Art. 2 lit. g EG-DSRI wurde mit dem BDSG 2001 in Abs. 8 zusätzlich zum „Dritten" der Begriff des „Empfängers" eingeführt. Empfänger ist gemäß Abs. 8 Satz 1 jede Person oder Stelle, die Daten erhält. Relevant ist der Begriff des Empfängers in erster Linie im Rahmen von Informationspflichten der verantwortlichen Stelle und Auskunftsrechten des Betroffenen; der Inhalt dieser Informationspflichten und Auskunftsrechte erstreckt sich auch darauf, wer 55

91 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 51.
92 Siehe dazu oben § 2 BDSG Rn. 7.

die Empfänger personenbezogener Daten sind.[93] Als Adressat eigener Verpflichtungen ist der Empfänger lediglich in einer Vorschrift aufgeführt (§ 29 Abs. 3 Satz 2 BDSG).[94] Teils werden zum Kreis der Empfänger auch die Organisationseinheiten innerhalb einer verantwortlichen Stelle gezählt (z. B. Betriebs- und Personalrat).[95]

b) Dritter (Abs. 8 Satz 2)

56 Dritter ist gemäß Abs. 8 Satz 2 jede Person oder Stelle außerhalb der verantwortlichen Stelle, nicht jedoch der Betroffene selbst oder Auftragsdatenverarbeiter innerhalb der EU bzw. des EWR (Abs. 8 Satz 3). Keine Dritten sind die Untereinheiten (Ämter, Dezernate, Zweigstellen) einer größeren Organisationseinheit (Gemeinde, Ministerium, Unternehmen).[96] Die behörden- oder unternehmensinterne Mitteilung personenbezogener Daten von Amt zu Amt bzw. von Zweigstelle zu Zweigstelle ist daher keine Datenübermittlung an Dritte nach Abs. 4 Nr. 3, sondern eine Datennutzung nach Abs. 5.[97] Auch die Personen innerhalb der verantwortlichen Stelle (z. B. Mitarbeiter) sind regelmäßig keine Dritten, es sei denn, sie erhalten die Daten nicht im Rahmen ihrer dienstlichen Funktion, sondern zu anderen (privaten oder geschäftlichen) Zwecken.[98]

10. Besondere Arten personenbezogener Daten (Abs. 9)

57 Abs. 9 mit seiner Definition der besonderen Arten von personenbezogenen Daten wurde in Umsetzung des Art. 8 EG-DSRI neu in das BDSG 2001 aufgenommen. Zu den besonderen Arten von personenbezogenen Daten gehören gemäß Abs. 9 Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeiten, Gesundheit oder Sexualleben. Vor Umsetzung des Art. 8 EG-DSRI hatte das BDSG nicht explizit nach mehr oder weniger sensitiven Daten differenziert; eine Berücksichtigung der Sensitivität von Daten fand lediglich im Einzelfall im Rahmen der allgemeinen Interessenabwägungsklauseln statt.[99] Fallen nunmehr personenbezogene Daten unter eine der in Abs. 9 aufgeführten Datengruppen, ist der Umgang mit diesen Daten besonderen Restriktionen unterworfen.

58 Der Sinn einer Differenzierung nach mehr oder weniger sensitiven Daten wird überwiegend bezweifelt. Gegen eine solche Differenzierung spricht vor allem,

93 Siehe § 4 Abs. 3 Satz 1 Nr. 3, § 19 Abs. 1 Satz 1 Nr. 2, § 19a Abs. 1 Satz 2, § 33 Abs. 1 Satz 3, § 34 Abs. 1 Satz 1 Nr. 2 und Abs. 2 Satz 2 BDSG.

94 Siehe dazu § 29 BDSG Rn. 62.

95 So *Gola/Schomerus*, BDSG, § 3 Rn. 51; *Schaffland/Wiltfang*, BDSG, § 3 Rn. 86a; a. A. *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 56.

96 *Gola/Schomerus*, BDSG, § 3 Rn. 52; a. A. *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 158 ff.

97 Siehe oben § 2 BDSG Rn. 7 (zur behördeninternen Mitteilung).

98 *Gola/Schomerus*, BDSG, § 3 Rn. 54.

99 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 166.

dass sich die Sensitivität personenbezogener Daten niemals abstrakt, sondern stets nur in Bezug auf den jeweiligen Verwendungszweck beurteilen lässt. Auch vermeintlich harmlose Daten wie Name oder Adresse können im entsprechenden Kontext einen äußerst sensitiven Charakter annehmen.[100] Entsprechend hat bereits das BVerfG im Volkszählungsurteil betont, dass je nach Datenverarbeitungszweck und Datenverarbeitungsmöglichkeiten auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen kann und es daher unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses" Datum mehr gibt.[101]

Die Auflistung der in Abs. 9 erfassten besonderen Gruppen von personenbezogenen Daten ist abschließend. Zu den Angaben über rassische und ethnische Herkunft gehören alle Angaben, die den Betroffenen einer bestimmten Rasse, Hautfarbe, Volksgruppe oder Minderheit zuordnen, nicht jedoch dessen Staatsangehörigkeit oder geographische Herkunft.[102] Angaben über politische Meinungen, religiöse oder philosophische Überzeugungen erfassen nicht nur die Zugehörigkeit (oder Nicht-Zugehörigkeit) zu einer bestimmten Partei, Religions- oder sonstigen Glaubensgemeinschaft, sondern – vorgelagert – auch sämtliche Verhaltensweisen, die auf eine bestimmte politische, religiöse oder philosophische Einstellung schließen lassen. Angaben über die Gesundheit sind alle Angaben, die den körperlichen und geistigen Zustand eines Menschen betreffen (Zustandsbeschreibungen, Befundmitteilungen, Krankheitsgeschichten etc.). Auch genetische Daten und die Schwerbehinderteneigenschaft zählen hierzu.[103] 59

11. Mobile personenbezogene Speicher- und Verarbeitungsmedien (Abs. 10)

Mit § 6c BDSG wurde durch das BDSG 2001 eine besondere Regelung für mobile personenbezogene Speicher- und Verarbeitungsmedien (sog. Chipkarten oder „Smart Cards") in das BDSG aufgenommen. Die Neuregelung des § 6c BDSG machte auch die Einfügung einer Definition der mobilen personenbezogenen Speicher- und Verarbeitungsmedien notwendig, wie sie nunmehr in Abs. 10 normiert ist. 60

Gemäß Abs. 10 handelt es sich bei mobilen personenbezogenen Speicher- oder Verarbeitungsmedien um Datenträger, die an den Betroffenen ausgegeben werden (Nr. 1). Keine Voraussetzung ist, dass bereits bei Ausgabe der Medien irgendwelche Daten auf diesen abgespeichert sind; vielmehr können auch „blanko" ausgegebene Medien unter Abs. 10 fallen.[104] Es muss sich um Speicher- oder Verarbeitungsmedien handeln, auf denen personenbezogene Daten über die Speiche- 61

100 Vgl. *Gola/Schomerus*, BDSG, § 3 Rn. 56, und *Dammann*, in: Simitis, BDSG, § 3 Rn. 251 (mit dem Beispiel der Aufnahme von Namen und Adressen in die Kartei einer Heilanstalt oder Drogenberatungsstelle).

101 BVerfGE 65, 1 (45) – Volkszählungsurteil.

102 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 168.

103 *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 171 f.

104 BT-Drs. 14/5793, S. 60.

rung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können (Nr. 2). Bloße Speichermedien (CDs, Magnetkarten) werden daher nicht erfasst. Darüber hinaus kommt es auf Beschaffenheit und Gestaltung dieser Medien nicht an; es muss sich bei diesen nicht um eine Karte handeln, möglich ist etwa auch ein Armband, eine Kette oder ein anderer Gegenstand.[105] Dritte Voraussetzung ist schließlich, dass der Betroffene die Datenverarbeitung auf diesen Medien nur durch den „Gebrauch" des Mediums beeinflussen kann (Nr. 3). Ein solcher Gebrauch kann etwa das Einführen einer Chipkarte in ein Lesegerät sein oder die Auswahl zwischen einigen wenigen vom Verfahren vorgegebenen Alternativen, etwa das Drücken einer Taste an einem Lesegerät. Kann hingegen der Benutzer die Verarbeitungsvorgänge auf vielfältige Weise steuern wie etwa bei Mobiltelefonen oder Notebooks, handelt es sich nicht mehr um mobile personenbezogene Speicher- und Verarbeitungsmedien im Sinne des Abs. 10.[106]

12. Beschäftigte (Abs. 11)

62 Durch die Aufnahme eines neuen § 32 BDSG zum Datenschutz in Beschäftigtenverhältnissen ist der Begriff des Beschäftigten erstmals im BDSG verankert worden. Diese Neuregelung machte auch die Einführung einer Definition notwendig, die festlegt, wer als Beschäftigter im Sinne des § 32 BDSG zu verstehen ist. Dem trägt § 3 Abs. 11 BDSG Rechnung. Die Regelung stellt klar, dass zum Begriff des Beschäftigten nicht nur Arbeitnehmer im engeren Sinn gehören, sondern auch die zur Berufsausbildung Beschäftigten und Personen, denen eine arbeitnehmerähnliche Stellung zukommt.[107] Auf den Schutzbereich des § 32 BDSG können sich folglich nahezu alle Personen, die in einem Beschäftigtenverhältnis stehen, berufen. Lediglich die Beamtinnen und Beamte sowie die Richterinnen und Richter der Länder sind in § 3 Abs. 11 BDSG nicht erwähnt, da dem Bundesgesetzgeber insoweit die Gesetzgebungskompetenz fehlt.

105 BT-Drs. 14/5793, S. 60.
106 BT-Drs. 14/5793, S. 60
107 Gesetzesbegründung zu BT-Drs.16/13657, S. 27.