

Datenschutzrecht

von Rechtsanwalt Dr. Ivo Geis

Hamburg, Februar 2007

Überblick

Datenschutz ist ein komplexes Rechtsgebiet. Aus dem Verfassungsrecht wird das informationelle Selbstbestimmungsrecht abgeleitet (1.0). Das Bundesdatenschutzgesetz bestimmt allgemeingültige Regeln (2.0). Durch den stetig wachsenden Datenaustausch über Website, E-Mail und Mobilfunk ist ein besonderes Datenschutzrecht entstanden, das durch das Telemediengesetz (3.0) geregelt ist.

Inhalt

1.0	Die verfassungsrechtliche Grundlage.....	5
2.0	Das Bundesdatenschutzgesetz	7
2.1	Europäische Richtlinie und BDSG	7
2.1.1	Rechtsangleichung im Binnenmarkt	7
2.1.2	Grenzüberschreitender Datenaustausch	9
2.2	Anwendbarkeit des BDSG.....	10
2.2.1	Personenbezogene Daten	10
2.2.2	Öffentlicher und nicht öffentlicher Bereich	10
2.2.3	Beteiligte: Verantwortliche Stelle, Empfänger und Dritter	12
2.2.4	Datenerhebung	13
2.2.5	Datenverarbeitung.....	13
2.2.6	Nutzen	14
2.3	Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung.....	14
2.3.1	Verbot mit Erlaubnisvorbehalt.....	14
2.3.2	Gesetzliche Erlaubnis.....	15
2.3.3	Einwilligung.....	16
2.4	Allgemeine Regeln der Erhebung, Verarbeitung, Nutzung	17
2.4.1	Grundsatz der Datenvermeidung und Datensparsamkeit	17
2.4.2	Anonymisieren und Pseudonymisieren	17
2.4.3	Datengeheimnis.....	18
2.5	Rechte des Betroffenen.....	18
2.5.1	Benachrichtigung und Folgerechte	18
2.5.2	Schadensersatzansprüche	19
2.6	Meldepflicht und Datenschutzbeauftragte	20
2.6.1	Meldepflicht.....	21
2.6.2	Der betriebliche Datenschutzbeauftragte	21
2.6.3	Zuständige Aufsichtsbehörde.....	22
2.6.4	Der Bundesbeauftragte für den Datenschutz.....	22
2.7	Datenschutz und Technik	23
2.7.1	Automatisierte Einzelentscheidung.....	23
2.7.2	Videoüberwachung	23
2.7.3	Mobile personenbezogene Speicher und RFID.....	25
2.7.4	Rechtlicher Schutz	27
2.7.5	Automatisierte Abrufverfahren	27
2.7.6	Datensicherung	28
2.7.7	Datenschutzaudit.....	28
2.8	Auftragsdatenverarbeitung	28
2.9	Grenzüberschreitende Datenübermittlung	29
2.9.1	Unternehmen mit Sitz im Inland	29
2.9.2	Unternehmen mit Sitz im Ausland	31
2.9.3	Ergebnis	32
2.10	Bußgeldvorschriften.....	33

3.0	Das neue Telemediengesetz	35
3.1	Geltungsbereich.....	35
3.2	Anbieter-Nutzer-Verhältnis	37
3.3	Gesetzes- und Einwilligungsvorbehalt	37
3.4	Organisatorische Pflichten des Diensteanbieters	37
3.5	Bestandsdaten	38
3.5.1	Definition und der Grundsatz der Erforderlichkeit	38
3.5.2	Das Recht zur Auskunft	38
3.6	Nutzungsdaten	39
3.6.1	Definition	39
3.6.2	Werbung.....	39
3.6.3	Abrechnungsdaten.....	39
3.6.4	Erheben, Verarbeiten und Nutzen von Abrechnungsdaten	40
3.6.5	Übermittlung von Abrechnungsdaten	40
3.6.6	Zusammenführen von Nutzungsdaten zu Abrechnungszwecken.....	41
3.6.7	Inhalt der Abrechnung	41
3.6.8	Löschungsfrist für Einzelnachweise.....	42
3.6.9	Auskunft an die Strafverfolgungsbehörden.....	42
3.6.10	Recht zur Datenverarbeitung bei Missbrauch von Telemediendiensten	42

1.0 Die verfassungsrechtliche Grundlage

Personenbezogene Daten werden nach dem Volkszählungsurteil des Bundesverfassungsgerichts durch das Recht auf informationelle Selbstbestimmung verfassungsrechtlich geschützt: die Befugnis, über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen.¹ Das Bundesverfassungsgericht verdeutlicht im Volkszählungsurteil, dass es das informationelle Selbstbestimmungsrecht nicht in einer sphärenbezogenen Weise interpretiert, sondern dass dieses Recht vor Gefahren schützt, die sich aus der Zusammenfügung mit anderen Datensammlungen zu einem mehr oder weniger vollständigen Persönlichkeitsbild ergeben, dessen Richtigkeit und Verwendung der Betroffene nur unzureichend kontrollieren kann.² Damit entfaltet das Recht auf informationelle Selbstbestimmung einen flexiblen, gegenüber technischen und gesellschaftlichen Entwicklungen reagiblen und an der konkreten Gefährdungssituation ausgerichteten Gewährleistungsgehalt.³ Als absolutes Nutzungs- und Verfügungsrecht analog dem Eigentum ist das informationelle Selbstbestimmungsrecht nicht anerkannt.⁴ Die Konstruktion als absolutes Nutzungs- und Verfügungsrecht gilt als nicht angemessen, da der Betroffene kein Herrschaftsrecht über Informationen beanspruchen kann, die erst der Verwender aus einem Bestand von Daten konstruiert hat.⁵ Schutzwürdig ist aber sein Recht, die Verwendung seiner persönlichen Daten durch Dritte kennen und kontrollieren zu können.⁶ Dies gilt besonders dann, wenn diese Verwendung sich für ihn selbst als folgenreich erweist. Denn nicht allein Art und Umfang der erhobenen Daten sind grundrechtsrelevant, vielmehr kommt es auch auf die denkbaren Verwendungen und das jeweilige Missbrauchspotential an.⁷

Eine aktuelle Interpretation hat das informationelle Selbstbestimmungsrecht durch das Urteil des Bundesverfassungsgerichts vom 2. März 2006 und den Beschluss vom 4. April 2006 erhalten.

¹ BVerfGE 65, 1 (41 ff.).

² BVerfGE 65, 1 (42).

³ Auf die Gefährdungsabhängigkeit stellt *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel (Hrsg.), Handbuch des Datenschutzrechts, 2003, S. 156 ff., Rn. 14, ab.

⁴ So aber *Ladeur*, DuD2000, 12, 18.

⁵ *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel (Hrsg.), Handbuch des Datenschutzrechts, 2003, S. 156 ff., Rn. 21.

⁶ *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel (Hrsg.), Handbuch des Datenschutzrechts, 2003, S. 156 ff., Rn. 19.

⁷ Vgl. BVerfGE 65, 1 (46).

Mit dem Urteil des zweiten Senats vom 2. März 2006⁸ wurde die Grenze zwischen Fernmeldegeheimnis des Art. 10 GG und dem informationellen Selbstbestimmungsrecht nach Art. 1 Abs. 2 i.V.m. Art. 2 Abs. 1 GG gezogen. Der Schutz des Fernmeldegeheimnisses gilt nur die telekommunikative Übermittlungsphase. Die auf TK-Endgeräten gespeicherten Daten werden durch das informationelle Selbstbestimmungsrecht geschützt. Nach diesem Schutzrecht ist den staatlichen Sicherheitsbehörden der Zugriff auf mobile Speichermedien verwehrt, wenn die dort gespeicherten Daten auf andere Weise schon verfügbar waren und der Eingriff damit nicht mehr für die Rechtssicherung notwendig war.

Mit Beschluss vom 4. April 2006⁹ zur Rasterfahndung hat der erste Senat des Bundesverfassungsgerichts eine Grenze für die polizeiliche Rasterfahndung gezogen.¹⁰ Nach Ansicht des Gerichts ist ein derart intensiver Grundrechtseingriff nur verhältnismäßig, wenn die Anforderungen an die Wahrscheinlichkeit des Gefahrenintritts und die Nähe des Betroffenen zur Bedrohung eingegrenzt werden. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die Einbußen an grundrechtlich geschützter Freiheit nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient. Die Maßnahme der Rasterfahndung zur Aufdeckung sog. „Schläfer“ ist nur dann mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar, wenn eine „konkrete“ und somit durch hinreichende Tatsachen zu belegende Gefahr für hochrangige Rechtsgüter, wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Das Vorliegen einer allgemeinen Bedrohungslage, etwa bei Vorliegen von vagen Vermutungen ohne greifbaren auf den Einzelfall bezogenen Anlass, ist hingegen nicht ausreichend.

⁸ CR 2006, 383 = MMR 2006, 217.

⁹ CR 2006, 594 = MMR 2006, 531.

¹⁰ Zur Konsequenz dieser Entscheidung für die Antiterrordatei *Kirchberg*, CR 2007, 10, 14. Rasterfahndung wegen Kinderpornographie soll den Anforderungen dieser Entscheidung entsprechen, da nur nach Straftätern gefahndet wird. Hierzu FAZ 11. Januar 2007, S. 7 und 9.

2.0 Das Bundesdatenschutzgesetz

2.1 Europäische Richtlinie und BDSG

Der Ministerrat und das Europäische Parlament verabschiedeten am 24. Oktober 1995 eine allgemeine Datenschutzrichtlinie, die bis Ende 1998 in das Recht der Mitgliedstaaten umgesetzt werden musste.¹¹ Dies ist inzwischen bis auf Frankreich und Irland geschehen. Hierdurch sind einheitliche Strukturen für den Datenschutz entstanden. Diese Harmonisierung des Datenschutzrechts in der europäischen Union war bereits durch das “Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ (Europäische Datenschutzkonvention) vom 28. Januar 1981¹² vorgezeichnet. Die Konvention verpflichtete die Unterzeichnerstaaten, die niedergelegten Grundsätze als gemeinsames datenschutzrechtliches Minimum zu verwirklichen. Eine Pflicht der Mitgliedstaaten zur Umsetzung in nationales Recht war hiermit nicht verbunden. Eine solche Verpflichtung ist erst mit der allgemeinen Datenschutzrichtlinie entstanden.

2.1.1 Rechtsangleichung im Binnenmarkt

Rechtsgrundlage für diese Richtlinien ist die Notwendigkeit der Rechtsangleichung im Binnenmarkt (Artikel 100 a EGV). Nach dem Subsidiaritätsprinzip (Artikel 3 lit.b Abs.2 EGV) dürfen die EG-Organen dann tätig werden, wenn ein Ziel besser auf der Gemeinschaftsebene als auf derjenigen der einzelnen Mitgliedstaaten erreicht werden kann. Aus ökonomischer Sicht erfordert der Warenverkehr oder die Anbahnung und Abwicklung von Dienstleistungen eine europäische Regelung für die Verarbeitung von personenbezogenen Daten, da die Übermittlung personenbezogener Daten wesentlicher Bestandteil des Geschäftsverkehrs ist. Datenschutz ist zugleich auch die Gewährleistung eines elementaren Menschenrechts. Der Gerichtshof hat das in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) verankerte Recht auf Achtung des Privatlebens in seiner Entscheidung vom 5.10.1994 als “ein von der Gemeinschaftsordnung geschütztes Grundrecht” bezeichnet und damit auch den Wert des Grundrechts auf Privatheit/Datenschutz für die Gemeinschaftsordnung betont.

¹¹ Richtlinie 95/46/EG des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Text in: *Geis/Helfrich*, Datenschutzrecht/Textausgabe, S. 68 ff.

¹² Text in: *Geis/Helfrich*, Datenschutzrecht/Textausgabe, S. 58 ff.; hierzu näher *Burkert in Roßnagel*, Handbuch des Datenschutzrechts, 2.3 Internationale Grundlagen, Rdnr. 35.

- Strukturen des Datenschutzes

Zweck der Richtlinie ist es, nach Erwägungsgrund 10 ein möglichst hohes und gleichwertiges Datenschutzniveau für den Binnenmarkt herzustellen. Die Richtlinie regelt für öffentliche und nicht öffentliche Stellen die manuelle und die automatisierte bzw. teilweise automatisierte Verarbeitung von personenbezogenen Daten in Dateien. Die Definition "dateimäßige Verarbeitung" (Artikel 2) geht weiter als im BDSG und erfasst "jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, gleichgültig, ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird".¹³

Die Richtlinie sieht unabhängige Kontrollinstanzen vor (Artikel 28), die eine Regelkontrolle vornehmen müssen. Den Verantwortlichen für die Datenverarbeitung gibt die Richtlinie ein Wahlrecht zwischen der generellen Meldepflicht automatisierter Datenverarbeitung an ein öffentliches Register und der Bestellung eines betrieblichen/behördlichen Beauftragten für den Datenschutz.

Ein prinzipielles Verbot besteht für sensitive Daten: Angaben über die rassische und ethnische Herkunft, die politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.

Verboten sind negative Einzelentscheidungen, die ausschließlich aufgrund einer automatisierten Verarbeitung ergehen, wie z.B. die Beurteilung der Leistungen und des Verhaltens von Bewerbern, der Abgleich von Daten für Sozialpläne und die Kreditvergabe.

Die Haftungsklausel (Artikel 23) sieht Schadensersatzansprüche bei rechtswidriger Datenverarbeitung in unbegrenzter Höhe vor.

Das öffentliche Interesse, wie das Sicherheits- und Verteidigungsinteresse, kann pauschale Einschränkungen und Ausnahmen im öffentlichen Bereich begründen: Entsprechende Dateien fallen nicht unter den Anwendungsbereich der Richtlinie. Dadurch entstehen Probleme hinsichtlich eines einheitlichen Datenschutzes in der EU wie durch Europol.

¹³ *Brühmann in Roßnagel*, Handbuch des Datenschutzrechts, 2.4 Europarechtliche Grundlagen, Rdnr. 17-56.

2.1.2 Grenzüberschreitender Datenaustausch

Die Richtlinie erklärt den Ort der Niederlassung (Artikel 4 Abs. 1 lit.a und lit.c) zum Anknüpfungspunkt des Datenschutzes. Die jeweiligen nationalen Datenschutzbestimmungen greifen also dort, wo die datenverarbeitende Stelle ihren Sitz hat. Bei einem Sitz des Verantwortlichen außerhalb der EU mit Zugriffsmöglichkeiten auf personenbezogene Daten in einem EU-Mitgliedstaat gilt das Recht dieses Staates.¹⁴ Der Datenexport in Drittstaaten ist nur im Rahmen der Richtlinie zulässig. Sie erlauben den Datentransfer grundsätzlich nur dann, wenn im Land des Datenempfängers ein im Verhältnis zur Datenschutzrichtlinie angemessenes Datenschutzniveau vorliegt (Artikel 25 Abs. 1). Alternativ kann in Ausnahmefällen der Transfer (Artikel 26 Abs. 2) vertraglich zwischen Datenübermittler, Betroffenen und Datenempfänger vereinbart werden (Vertragslösung), wenn auf diese Weise die datenschutzrechtlichen Interessen des Betroffenen sichergestellt werden. Für die Beurteilung des Schutzniveaus in der Gemeinschaft und in Drittstaaten spielt die Datenschutzgruppe (Artikel 29 i.V.m. Artikel 30 Abs. 1 lit.d, Abs. 3) eine wichtige Rolle. Sie nimmt hierzu auf Anfrage gegenüber der Kommission Stellung, hat aber auch die Möglichkeit von sich aus präventiv Empfehlungen abzugeben.¹⁵

Die Richtlinie ist mit dem am 23. Mai 2001 in Kraft getretenen “Gesetz zur Änderung des Bundesdatenschutzgesetzes” in geltendes Recht umgesetzt worden.¹⁶ Mit der Umsetzung der Datenschutzrichtlinie ist das bisherige Bundesdatenschutzgesetz (BDSG) aus dem Jahre 1990 zum BDSG 2001 entwickelt worden. Das BDSG 2001 ist durch Regeln gekennzeichnet, die der technischen Entwicklung und der Internationalisierung des Datenaustausches entsprechen.¹⁷ Das Bundesdatenschutzgesetz hat nach dem im Volkszählungsurteil¹⁸ für den Datenschutz entwickelten Begriff des Persönlichkeitsrechtes „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (§ 1 Abs. 1 BDSG). Die Anknüpfung des Bundesdatenschutzgesetzes an den im Volkszählungsurteil entwickelten Begriff des Persönlichkeitsrechtes bedeutet, dass der Einzelne sein Persönlichkeitsrecht nicht ohne Rücksicht auf Interessen Dritter durchsetzen kann, sondern dieses Persönlichkeitsrecht nach

¹⁴ Zur Frage des anwendbaren Rechts eingehend *Kuner*, European Data Privacy Law and Online Business, 85-116.

¹⁵ *Brühann* in *Roßnagel*, Handbuch des Datenschutzrechts, 2.4 Europarechtliche Grundlagen, Rdnr. 50-55.

¹⁶ Zum Stand der Umsetzung in den Mitgliedstaaten: *Brühann* in *Roßnagel*, Handbuch des Datenschutzrechts, 2.4 Europarechtliche Grundlagen, Rdnr. 64-78.

¹⁷ Text in *Geis/Helfrich*, Datenschutzrecht/Textausgabe, S. 213 ff.; Als Überblick zum BDSG 2001: *Gerhold/Heil*, DuD 2001, 377 ff.

¹⁸ BVerfGE 65, 1.

einer entsprechenden Abwägung zu Gunsten vorrangiger Gegeninteressen zurücktreten muss. Datenschutz wird damit von dem Prinzip der Angemessenheit bestimmt.

2.2 Anwendbarkeit des BDSG

2.2.1 Personenbezogene Daten

Personenbezogene Daten sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmaren natürlichen Person (Betroffener)“, § 3 Abs. 1 BDSG. Damit ist für die Definition der personenbezogenen Daten ein weiter Begriff gewählt. Dieser reicht von Name und Alter bis zu Daten über Gesundheit, charakterliche Eigenschaften, Qualifikation und bestimmte Tätigkeitszeiten.¹⁹ Datenschutz ist nicht davon abhängig, ob es sich um besonders empfindliche Daten, sensitive Daten, handelt. Denn auch vermeintlich „triviale Daten“, wie Name und Anschrift, sind unter den Verknüpfungsmöglichkeiten der modernen Datenverarbeitung keine belanglosen Daten.

Das BDSG hat entsprechend der Vorgabe durch die EG-Datenschutzrichtlinie gemäß § 3 Abs. 9 Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben als besondere Art personenbezogener Daten bestimmt. Dies ist eine Abkehr von dem bisher tragenden Grundsatz des deutschen Datenschutzrechts, personenbezogene Daten nicht zu klassifizieren.²⁰ Die Verarbeitungsanforderungen sind in § 13 Abs. 2 BDSG für das Erheben durch öffentliche Stellen, in § 28 Abs. 6 bis 9 BDSG für die Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke nicht öffentlicher Stellen und gleichlautend in § 29 Abs. 5 BDSG für die geschäftsmäßige Datenerhebung und –speicherung zum Zweck der Übermittlung durch nicht öffentliche Stellen näher umschrieben. Für diese Regelungen ist die Datenverarbeitung des für die Praxis wichtigsten Typs besonderer personenbezogener Daten, der Gesundheitsdaten, charakteristisch.

2.2.2 Öffentlicher und nicht öffentlicher Bereich

Das BDSG hält auch nach der Umsetzung der EG-Datenschutzrichtlinie die grundsätzliche Trennung zwischen öffentlichem und nicht öffentlichem Bereich aufrecht. Die Umsetzung der EG-Richtlinie führt im Ergebnis jedoch dazu, dass die nach früherem Recht bestehenden

¹⁹ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 3-59.

²⁰ *Simitis u.a.*, BDSG/ *Simitis*, § 3 Rdnr. 257.

wesentlichen Unterschiede zwischen öffentlichem und nicht-öffentlichem Bereich aufgeweicht sind.

Durch die weitgefasste Regelung des § 2 Abs. 1 BDSG soll sichergestellt werden, dass alle Stellen des Verwaltungsträgers „Bundesrepublik Deutschland“ dem BDSG unterfallen. Der Begriff der „öffentlich-rechtlich organisierten Einrichtungen“ des Bundes umfasst Behörden, Organe der Rechtspflege und durch die Auffangklausel „andere öffentlich-rechtlich organisierte Einrichtungen“ Einrichtungen des Bundes, die weder Behörden noch Organe der Rechtspflege sind. Für öffentliche Stellen der Länder (§ 2 Abs. 2 BDSG) gelten die jeweiligen Landesdatenschutzgesetze. Für Mischvereinigungen des privaten Rechts aus Stellen des Bundes und der Länder regelt § 2 Abs. 3 BDSG die Anwendbarkeit von Bundesdatenschutzgesetz oder Landesdatenschutzgesetzen. Dem öffentlichen Bereich ordnet das Bundesdatenschutzgesetz auch öffentlich-rechtliche Wettbewerbsunternehmen des Bundes (§ 27 Abs. 1 Nr. 2 a BDSG) oder der Länder (§ 27 Abs. 1 Nr. 2 b BDSG) zu, die als Unternehmen am Wettbewerb teilnehmen.

Als „nicht-öffentliche Stelle“ qualifiziert das Gesetz natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des Privatrechts, soweit sie nicht zu den öffentlichen Stellen zählen, § 2 Abs. 4 BDSG. Diese unterliegen dem BDSG, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Das novellierte BDSG stellt im Gegensatz zur früher geltenden Rechtslage nicht mehr auf die Unterscheidung zwischen „Datei“ und „Akte“ ab, sondern auf die „automatisierte Verarbeitung“ im Sinne von § 3 Abs. 2 Satz 1 BDSG. Dies entspricht den Vorgaben der EG-Datenschutzrichtlinie. Ein verbleibender regelungstechnischer Restbezug auf die „Datei“ ist in § 3 Abs. 2 Satz 2 BDSG zu finden. Danach ist eine „nicht automatisierte Datei“ jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich ist sowie ausgewertet werden kann. Die Sammlung ist auch eine ungeordnete oder nur sequentielle Ansammlung personenbezogener Daten, wenn die generelle Möglichkeit der automatisierten Auswertung nach bestimmten Merkmalen gegeben ist. Ausreichend sind dafür mindestens zwei Merkmale. Als automatisierte Datei gelten damit auch Textdateien mit personenbezogenen Daten, die durch spezielle Suchprogramme nach verschiedenen Kriterien ausgewertet werden können.²¹ Die Anwendbarkeit des BDSG ist nach § 1 Abs. 2 Nr. 3 nur

²¹ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 60-105.

dann im nicht-öffentlichen Bereich ausgeschlossen, wenn die dort genannten Tatbestände ausschließlich für persönliche oder familiäre Tätigkeiten erfüllt sind. Von den Anforderungen des Bundesdatenschutzgesetzes wird damit nur die im privaten Bereich verbleibende Datenverarbeitung nicht erfasst. Für alle anderen Formen der Datenverarbeitung durch natürliche und juristische Personen sowie Personenvereinigungen gilt das BDSG: für natürliche Personen wie Gewerbetreibende, Freiberufler, Forst- und Landwirte, Personenvereinigungen, wie Vereine, Gewerkschaften, Arbeitgeberverbände oder sonstige Berufsverbände und für Kapitalgesellschaften. Auf die früher wichtige Frage, ob die Daten geschäftsmäßig oder für berufliche oder gewerbliche Zwecke erhoben, verarbeitet oder genutzt werden, kommt es nach dem novellierten Recht nicht mehr an.

2.2.3 Beteiligte: Verantwortliche Stelle, Empfänger und Dritter

Vor der Novellierung stellte das BDSG auf den Begriff der „speichernden Stelle“ ab. Dies entsprach nicht mehr der Terminologie, wie sie von der EG-Datenschutzrichtlinie aufgezeigt wird. Folgerichtig wird der frühere Begriff nun in § 3 Abs. 7 BDSG durch den Begriff der verantwortlichen Stelle ersetzt. Verantwortliche Stelle ist nun jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Im öffentlichen Bereich wird die speichernde Stelle durch den Behördenbegriff der Landesdatenschutzgesetze definiert. Im nicht öffentlichen Bereich ist jede juristische Einheit und damit jede natürliche und juristische Person sowie Gesellschaft oder andere Personenvereinigung verantwortliche Stelle, § 3 Abs. 7 i.V.m. § 1 Abs. 2 Nr. 3, § 2 Abs. 4 und § 27 Abs. 1 BDSG. Das BDSG geht von einer juristischen Betrachtungsweise aus. Damit sind verantwortliche Stelle die Firma und ihre Niederlassungen und Zweigstellen. Aufgrund dieser juristischen Betrachtungsweise sind auch die rechtlich selbständigen Unternehmen im Konzernverbund jeweils eigene speichernde Stelle.²² Die wesentliche Ergänzung des § 3 Abs. 7 BDSG besteht in der Festlegung, dass auch derjenige, der als Auftraggeber die Datenverarbeitung durch andere vornehmen lässt, verantwortliche Stelle ist.

Empfänger ist jede Person oder Stelle, die Daten erhält, § 3 Abs. 8, S. 1 BDSG. So Arbeitnehmer, die Aufgaben im Rahmen der verantwortlichen Stelle wahrnehmen oder in deren Auftrag tätig werden.²³

²² *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 231.

²³ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 241.

Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, § 3 Abs. 8 S. 2 BDSG. So ist im öffentlichen Bereich eine andere Behörde Dritter. Im nicht-öffentlichen Bereich ist jede natürliche oder juristische Person und jede Gesellschaft oder sonstige Personenvereinigung des Privatrechts eine verantwortliche Stelle. Auch verbundene Unternehmen bleiben zueinander Dritte solange sie rechtlich selbständig sind.²⁴

2.2.4 Datenerhebung

„Erheben“ von Daten bedeutet das Beschaffen von Daten über den Betroffenen, § 3 Abs. 3 BDSG. Das Erheben der Daten muss gezielt erfolgen. Das Erheben reicht von dem Erfragen besonderer Angaben bis zu dem Fotografieren bestimmbarer Personen.²⁵ Das zufällige Wahrnehmen von Daten löst folglich nicht den Schutz des Bundesdatenschutzgesetzes aus.

2.2.5 Datenverarbeitung

Die Speicherung ist die häufigste Form der Verarbeitung. Sie umfasst das Erfassen, Aufnehmen und Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung, § 3 Abs. 4 Nr. 1 BDSG. Datenträger ist ein weiter Begriff, der jedes Medium umfasst, auf dem personenbezogene Daten festgehalten werden können.²⁶

Verändern ist „das inhaltliche Umgestalten gespeicherter personenbezogener Daten“, § 3 Abs. 4 Nr. 2 BDSG. Inhaltliches Umgestalten ist jede Maßnahme, durch die der Informationsgehalt einer Nachricht geändert wird, so dass ein neuer Aussagewert entsteht. Eine Veränderung ist damit gegeben, wenn neue Aussagen durch die Berichtigung oder Verfälschung von Daten, das Herausnehmen von Daten aus dem Zusammenhang und das Einfügen von Daten in andere Zusammenhänge gewonnen werden.²⁷

Das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an eine andere Person als den Betroffenen, einem Dritten, wird als Übermitteln definiert, wenn die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder der Empfänger von der speichernden Stelle zur Einsicht oder zum

²⁴ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 238-239.

²⁵ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 115.

²⁶ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 124.

²⁷ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 135.

Abruf bereitgehaltene Daten einsieht oder abrufen, § 3 Abs. 4 Nr. 3 BDSG. Übermittlung ist damit nicht das Bereithalten von personenbezogenen Daten zur Einsicht oder zum Abruf, sondern die konkrete Einsichtnahme bzw. der konkrete Abruf.²⁸

Sperren, das „Kennzeichnen personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken“ (§ 3 Abs. 4 Nr. 4 BDSG) kommt vor allem in Frage, wenn die Daten aufgrund von gesetzlichen Vorschriften aufbewahrt werden müssen oder die Richtigkeit der Daten vom Betroffenen bestritten wird. Die Sperrung kann für Dateien durch Zusatzinformationen oder durch Codierungen erfolgen, für Akten am sichersten durch Auslagerung.²⁹

Löschen, das Unkenntlichmachen gespeicherter personenbezogener Daten (§ 3 Abs. 4 Nr. 5 BDSG) geschieht durch Vernichten von Informationen und Datenträgern oder durch Unkenntlichmachen der Informationen auf dem Datenträger, indem die Daten physikalisch gelöscht werden und damit die Kenntnisnahme ihres Informationsgehalts der verantwortlichen Stelle unmöglich ist.³⁰

2.2.6 Nutzen

Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um deren Verarbeitung handelt (§ 3 Abs. 5 BDSG). Danach ist Nutzen die Auswertung von verarbeiteten Daten, die Verwendung des Informationsgehalts verarbeiteter Daten und die Weitergabe der Daten innerhalb der speichernden Stelle. Nutzen reicht damit von der Verwendung von Daten zur Korrespondenz mit dem Betroffenen bis zur Übersendung der Daten zur Auftragsdatenverarbeitung.³¹

2.3 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

2.3.1 Verbot mit Erlaubnisvorbehalt

Datenerhebung, Datenverarbeitung und Datennutzung sind nach dem Grundsatz des Bundesdatenschutzgesetzes verboten, wenn dies ausnahmsweise nicht erlaubt ist. Erlaubt wird

²⁸ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 151-161.

²⁹ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 172.

³⁰ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 189.

³¹ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 201.

die Datenverarbeitung und Datennutzung durch Rechtsvorschriften des BDSG, andere Rechtsvorschriften und die Einwilligung des Betroffenen, § 4 Abs. 1 BDSG.

2.3.2 Gesetzliche Erlaubnis

- Allgemeine Anforderungen an die Erhebung

Nach dem Grundsatz der Direkterhebung sind personenbezogene Daten beim Betroffenen zu erheben, 4 Abs. 2 S 2 BDSG. Werden personenbezogene Daten beim Betroffenen erhoben, so ist er von der verantwortlichen Stelle über deren Identität, die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung und die Kategorien von Empfängern zu unterrichten, § 4 Abs. 3 BDSG. Ohne Mitwirkung des Betroffenen dürfen nach § 4 Abs. 2 S 2 BDSG seine personenbezogenen Daten nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

- die Erhebung bei anderen erforderlich ist, um die Verwaltungsaufgabe/den Geschäftszweck zu erfüllen oder
- die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde
- und keine überwiegenden schutzwürdigen Interessen des Betroffenen beeinträchtigt werden.

Spezielle Anforderungen an die Datenerhebung im öffentlichen Bereich

Datenerhebung im öffentlichen Bereich ist gesetzlich erlaubt, wenn die Kenntnis der Daten für öffentliche Stellen zur Erfüllung ihrer Aufgaben erforderlich ist, § 13 Abs. 1 BDSG.

Hierdurch wird der Grundsatz der Direkterhebung beim Betroffenen begründet, von dem nur ganz bestimmte Ausnahmen zugelassen sind: Werden die Daten nicht beim Betroffenen selbst sondern bei einer nicht öffentlichen Stelle erhoben, ist diese über den Erhebungszweck zu informieren und darüber, ob und aufgrund welcher Vorschrift sie zur Auskunft verpflichtet ist, § 13 Abs. 1a BDSG. Hierdurch wird verhindert, dass Informationen durch Einschaltung von Dritten oder durch heimliches Observieren gewonnen werden. Die Voraussetzungen zur Erhebung besonderer Arten personenbezogener Daten, die in § 3 Abs. 9 BDSG legaldefiniert sind, ist nur unter engen Voraussetzungen zulässig. Diese sind im Katalog des § 13 Abs. 2 BDSG abschließend aufgeführt.

Speichern, Verändern, Nutzen im öffentlichen Bereich

Während die Datenerhebung im nicht öffentlichen Bereich in § 28 Abs. 1 Satz 2 BDSG a.F. lediglich an den Grundsatz von Treu und Glauben sowie an das Kriterium der Rechtsmäßigkeit gekoppelt war, enthält der neugefasste § 28 Abs. 1 BDSG einen umfassenden Katalog der Kriterien zulässiger Datenerhebung nicht öffentlicher Stellen.

Spezielle Anforderungen im nicht-öffentlichen Bereich

Im nicht öffentlichen Bereich erlaubt das Bundesdatenschutzgesetz die Datenerhebung, Datenverarbeitung und Datennutzung aus unterschiedlichen Gründen: im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen, zur Wahrung berechtigter Interessen der verantwortlichen Stelle, wenn das schutzwürdige Interesse des Betroffenen nicht überwiegt, die Entnahme der Daten aus allgemein zugänglichen Quellen und zur Durchführung wissenschaftlicher Forschung, § 28 Abs. 1 BDSG. Andere Rechtsvorschriften sind Spezialgesetze zum BDSG wie die Spezialgesetze des Bundes und der Länder, z.B. die Ländermeldegesetze oder die Datenschutzgesetze der Länder. Zu diesen Erlaubnisvorschriften gehören auch Verordnungen und Satzungen, nicht aber Verwaltungsvorschriften. Erlaubnisvorschriften des Arbeitsrechtes sind Tarifverträge, Betriebs- und Dienstvereinbarungen, weil die Verarbeitung von Personaldaten im Betrieb sinnvoll nur nach einheitlichen Gesichtspunkten erfolgen kann.³²

2.3.3 Einwilligung

Im neu geschaffenen § 4a BDSG werden die Wirksamkeitsvoraussetzungen für die Einwilligung aufgestellt:

Die Einwilligung muss auf der „freien Entscheidung des Betroffenen“ beruhen, § 4a Abs. 1 S. 1 BDSG. Deshalb ist der Betroffene nach § 4a Abs. 1 S. 2 BDSG auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen einer Einwillungsverweigerung hinzuweisen.

Für die Einwilligung ist grundsätzlich Schriftform erforderlich, § 4a Abs. 1 S. 3 BDSG. Wird die Einwilligung in Formularverträgen als Bestandteil der Allgemeinen Geschäftsbedingungen erteilt, so ist sie im äußeren Erscheinungsbild der Erklärung hervorzuheben, § 4a Abs. 1 S. 4 BDSG. In dieser Form unterliegt die Einwilligung der AGB-

³² Gola/Schomerus, BDSG, § 4 Rdnr. 10.

rechtlichen Inhaltskontrolle. Damit darf sie den Vertragspartner nach den Geboten von Treu und Glauben nicht unangemessen benachteiligen. Dieses Benachteiligungsverbot verlangt eine Konkretisierung der Einwilligung auf den Geschäftszweck, auf die Datenverarbeitungsphasen und auf die Art der Daten.³³

Ausnahmsweise ist eine ausdrückliche mündliche Einwilligung oder eine stillschweigende Einwilligung ausreichend. Dies wird bei einer Geschäftsbeziehung von langer Dauer angenommen, in der sich der Betroffene mit der Datenverarbeitung einverstanden erklärt hat und die Verhältnisse sich nicht geändert haben.³⁴

Die datenschutzrechtliche Einwilligung ist an dem Begriff der vorherigen Zustimmung gemäß §§ 182, 183 BGB orientiert. Damit ist die nachträgliche Zustimmung zur Datenverarbeitung ausgeschlossen.³⁵

2.4 Allgemeine Regeln der Erhebung, Verarbeitung, Nutzung

2.4.1 Grundsatz der Datenvermeidung und Datensparsamkeit

Das Teledienstedatenschutzgesetz nahm erstmals den Grundsatz der Datenvermeidung und der Datensparsamkeit auf (§ 3 Abs. 4 TDDSG). Mit der BDSG-Novelle findet sich dieser nun auch in § 3a S 1 BDSG wieder. Nach dem Willen des Gesetzgebers soll durch die Einführung des Grundsatzes bereits durch die Gestaltung der Systemstrukturen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten soweit wie möglich vermieden und dadurch Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein minimiert werden. Es handelt sich um einen gesetzgeberischen Programmsatz, aus dem nicht unmittelbar Rechtsfolgen abgeleitet werden können. Der Grundsatz wird jedoch im Rahmen der Auslegung anderer Vorschriften heranzuziehen sein und so – mittelbar – die Ausgestaltung der Datenverarbeitungssysteme und –strukturen beeinflussen.

2.4.2 Anonymisieren und Pseudonymisieren

Durch die BDSG-Novelle ist in § 3a S 2 BDSG der vorrangige Einsatz anonymisierter und pseudonymisierter Formen der Datenerhebung gesetzlich vorgesehen. Deshalb musste die terminologische Fixierung des Begriffes der Pseudonymisierung – in Abgrenzung zum

³³ Gola/Schomerus, BDSG, § 4a Rdnr. 14.

³⁴ Gola/Schomerus, BDSG, § 4a Rdnr. 13.

³⁵ Gola/Schomerus, BDSG, § 4a Rdnr. 15.

bisherigen Begriff der Anonymisierung – erfolgen. Anonymisieren ist das Verändern personenbezogener Daten (§ 3 Abs. 6 BDSG) und Pseudonymisieren das Ersetzen des Namens (§ 3 Abs. 6a BDSG). Das Gesetz schreibt keine Methoden der Anonymisierung³⁶ und keine Verfahren der Pseudonymisierung³⁷ vor.

2.4.3 Datengeheimnis

Allen bei der Datenverarbeitung beschäftigten Personen im öffentlichen und privaten Bereich ist jede unbefugte Verarbeitung und Nutzung zu untersagen, § 5 BDSG. Unbefugt ist die Verarbeitung immer, wenn weder aus Gesetz, Verordnung, Anordnung, Vertrag oder Einzelanweisung eine Erlaubnis für die Verarbeitung oder Nutzung besteht. Im öffentlichen Bereich entfällt die gesonderte datenschutzrechtliche Verpflichtung, denn die Angehörigen des öffentlichen Dienstes sind bereits aufgrund dienst- oder arbeitsrechtlicher Vorschriften zur Verschwiegenheit verpflichtet. Entweder sind sie als Amtsträger vereidigt oder über ihre Schweigepflicht belehrt bzw. nach dem Verpflichtungsgesetz an die Schweigepflicht gebunden. Personen im nicht öffentlichen Bereich müssen durch ausdrückliche Erklärungen darauf hingewiesen werden, dass sie personenbezogene Daten in und aus Dateien nur befugt verarbeiten und nutzen dürfen, § 5 Satz 2 BDSG. Zu diesem Personenkreis werden auch Personen gerechnet, die Kenntnis von geschützten personenbezogenen Daten erhalten wie z.B. als Angehörige von Fachabteilungen, Botendienste, Wartungspersonal. Nicht erfasst werden Personen, die lediglich in der Nähe von Datenverarbeitungsanlagen tätig sind wie das Reinigungspersonal.³⁸

2.5 Rechte des Betroffenen

2.5.1 Benachrichtigung und Folgerechte

Durch den Grundsatz der Direkterhebung (§ 4 Abs. 2 BDSG) erhält der Betroffene Kenntnis von der Erhebung, Speicherung und Nutzung. Hat er mangels Direkterhebung keine Kenntnis von der Erhebung, Speicherung oder Übermittlung der Daten, so ist er im öffentlichen und nicht-öffentlichen Bereich über die Erhebung, Verarbeitung und Nutzung zu benachrichtigen.

Im öffentlichen Bereich ist der Betroffene nach § 19a BDSG zu unterrichten. Auf Antrag ist dem Betroffenen nach § 19 BDSG Auskunft über die zu seiner Person gespeicherten Daten,

³⁶ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 211.

³⁷ *Simitis u.a.*, BDSG/Dammann, § 3 Rdnr. 225.

³⁸ *Gola/Schomerus*, BDSG, § 5 Rdnr. 9.

die Empfänger der Daten und den Zweck der Speicherung zu erteilen. Der Betroffene hat gemäß § 20 BDSG ein Recht auf Berichtigung der Daten, wenn sie unrichtig sind, ein Recht auf Löschung, wenn die Speicherung unzulässig ist und ein Recht auf Sperrung, wenn einer Löschung Aufbewahrungspflichten entgegenstehen. Auf die Erteilung der Auskunft, der Berichtigung, der Löschung und der Sperrung hat der Betroffene ein subjektives öffentliches Recht, das er gerichtlich durchsetzen kann. Zuständig ist, je nachdem welche Behörde oder Stelle die Daten speichert das Verwaltungsgericht, das Sozialgericht oder das Finanzgericht. Die Ablehnung der geltend gemachten Rechte ist ein Verwaltungsakt. Die richtige Klageart ist deshalb im Allgemeinen die Verpflichtungsklage (§ 42 Abs. 1 VwGO).³⁹ Die Rechte auf Auskunft, Berichtigung, Löschung und Sperrung sind für den Betroffenen unverzichtbar, § 6 Abs. 1 BDSG.

Im nicht-öffentlichen Bereich haben die verantwortlichen Stellen die Pflicht, den Betroffenen von der erstmaligen Speicherung (§ 33 Abs. 1 Satz 1 BDSG) oder von der erstmaligen Übermittlung (§ 33 Abs. 1 Satz 2 BDSG) seiner Daten zu benachrichtigen. Damit hat der Betroffene die Möglichkeit, sein Recht auf Auskunft (§ 34 BDSG) und die Folgerechte auf Berichtigung, Löschung oder Sperrung unrichtiger Daten (§ 35 BDSG) wahrzunehmen. Wie im öffentlichen Bereich so sind auch im nicht-öffentlichen Bereich die Rechte auf Auskunft, Berichtigung, Löschung und Sperrung für den Betroffenen unverzichtbar, § 6 Abs. 1 BDSG.

2.5.2 Schadensersatzansprüche

Für den öffentlichen Bereich und den nicht öffentlichen Bereich sind die Schadensersatzansprüche gesondert geregelt.

Für den öffentlichen Bereich besteht eine Schadensersatzvorschrift in Form der Gefährdungshaftung, § 8 Abs. 1 BDSG. Hiernach haftet eine öffentliche Stelle, wenn die automatisierte Verarbeitung personenbezogener Daten nach dem BDSG oder einer anderen Datenschutzvorschrift unzulässig oder unrichtig war und dem Betroffenen ein Schaden zugefügt worden ist. In diesem Fall ist dem Betroffenen der materielle Schaden zu ersetzen und ein Schmerzensgeld zu zahlen, wenn eine schwere Verletzung seines Persönlichkeitsrechts vorliegt, § 8 Abs. 2 BDSG. Maßgeblich hierfür ist der objektive Umfang der Beeinträchtigung durch die unrichtige oder unzulässige Verarbeitung. Je nachhaltiger die durch eine Verwendung falscher Daten bewirkte Benachteiligung des Betroffenen ist, je schärfer sich in seinem privaten oder beruflichen Bereich und in der

³⁹ *Simitis u.a.*, BDSG/*Mallmann*, § 19 Rdnr. 124.

Öffentlichkeit ein Bild seiner Person abzeichnet, das ihn in seiner Handlungs- und Entscheidungsfreiheit beschränkt, desto zwingender erscheint der Ausgleich. Dies wird bei einer diskriminierenden Veröffentlichung von Personaldaten anzunehmen sein.⁴⁰ Der Anspruch aus § 8 verjährt gemäß § 8 Abs. 6 BDSG drei Jahre nachdem der Betroffene Kenntnis vom Schaden erhalten und erfahren hat, welche öffentliche Stelle dafür verantwortlich ist, spätestens dreißig Jahre nach der schadenstiftenden Handlung.

Während das BDSG alter Fassung für den nicht-öffentlichen Bereich lediglich eine Beweislastregel enthielt, findet sich nun in § 7 Satz 1 BDSG eine Anspruchsgrundlage, die dem Betroffenen einen Schadensersatzanspruch gewährt. Die verantwortliche Stelle kann sich jedoch nach § 7 Satz 2 BDSG exkulpieren, wenn sie nachweist, dass sie „die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.“ Die verantwortliche Stelle muss damit den Beweis erbringen, dass der Schaden eingetreten ist, obgleich sie alle im konkreten Fall erforderlichen Maßnahmen getroffen hat, um eine gesetzeskonforme Verwendung personenbezogener Daten zu gewährleisten. Eine Ersatzpflicht ist unter diesen Umständen nicht gegeben, wenn das Verhalten der verantwortlichen Stelle zwar den gesetzlichen Anforderungen entsprach, der Schaden aber trotzdem nicht verhindert werden konnte.⁴¹ Für die Verjährung bleibt es bei den Regeln, die generell auf deliktsrechtliche Ansprüche anzuwenden sind: Der Schadensersatzanspruch verjährt damit grundsätzlich drei Jahre nachdem der Geschädigte den Schaden festgestellt und erfahren hat, wen die Ersatzpflicht trifft, spätestens aber dreißig Jahre nach der Begehung der schadensstiftenden Handlung.⁴² Streitigkeiten über Schadensersatzansprüche sind grundsätzlich vor den Zivilgerichten geltend zu machen. Dies gilt auch dann, wenn sich die Ersatzansprüche gegen öffentliche Stellen richten. Sofern sich die Ansprüche auf eine unrichtige oder unzulässige Verarbeitung von Arbeitnehmerdaten beziehen und sich gegen den Arbeitgeber richten, müssen sie bei den Arbeitsgerichten geltend gemacht werden (§ 2 Abs. 1 Nr. 3 ArbGG).⁴³

2.6 Meldepflicht und Datenschutzbeauftragte

Das datenschutzrechtliche Kontrollsystem besteht aus der Meldepflicht, den Datenschutzbeauftragten, der Aufsichtsbehörde und dem Bundesdatenschutzbeauftragten.

⁴⁰ *Simitis u.a.*, BDSG/*Simitis*, § 8 Rdnr. 18.

⁴¹ *Simitis u.a.*, BDSG/*Simitis*, § 7 Rdnr. 24-25.

⁴² *Simitis u.a.*, BDSG/*Simitis*, § 7 Rdnr. 46.

⁴³ *Simitis u.a.*, BDSG/*Simitis*, § 7 Rdnr. 74-75.

2.6.1 Meldepflicht

Verfahren automatisierter Verarbeitungen sind nach § 4d Abs. 1 BDSG vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde nach Maßgabe von §4e zu melden. Die Meldepflicht umfasst nach § 4e BDSG die nähere Bezeichnung der verantwortlichen Stelle, die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, der Empfänger, die geplante Löschung, die geplante Übermittlung in Drittstaaten eine Beschreibung, ob die Maßnahmen nach § 9 BDSG angemessen sind. Die Meldepflicht entfällt nach § 4d Abs. 2 BDSG, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat. Die Meldepflicht entfällt nach § 4d Abs. 3 BDSG auch, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.

2.6.2 Der betriebliche Datenschutzbeauftragte

Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert erheben, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen, § 4f Abs. 1 S. 1 BDSG. Im nicht-öffentlichen Bereich ist ein betrieblicher Datenschutzbeauftragter zu bestellen, wenn eine verantwortliche Stelle mehr als vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt, § 4f Abs. 1 S. 1 und S. 4 BDSG, oder wenn sie einer Vorabkontrolle unterliegt oder wenn sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt, § 4f Abs. 1 S. 6 BDSG. Der Datenschutzbeauftragte muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit erfüllen, § 4f Abs. 2 S 1 BDSG. Er ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen, § 4f Abs. 3 S 1 BDSG. In Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes ist er weisungsfrei, § 4f Abs. 3 S. 2 BDSG. Wegen der Erfüllung seiner Aufgaben darf er nicht benachteiligt werden, § 4f Abs. 3 S. 3 BDSG. Für den Datenschutzbeauftragten gilt ein umfassendes Verschwiegenheitsgebot, § 4f Abs. 4 BDSG. Bei der Erfüllung seiner Aufgaben haben die öffentlichen und nicht-öffentlichen Stellen den Datenschutzbeauftragten zu unterstützen, § 4f Abs. 5 S. 1 BDSG. Betroffene können sich jederzeit an ihn wenden, § 4f Abs. 5 S. 2 BDSG. Der behördliche und der betriebliche Beauftragte für den Datenschutz ist

verpflichtet, auf die Einhaltung der datenschutzrechtlichen Vorschriften hinzuwirken, § 4g Abs. 1 S. 1 BDSG.⁴⁴ Er hat die ordnungsgemäße Anwendung der Datenverarbeitungsanlagen zu überwachen (§4g Abs. 1 S. 3 Nr. 1 BDSG) und die bei der Verarbeitung tätigen Personen mit den datenschutzrechtlichen Vorschriften vertraut zu machen, § 4g Abs. 1 S. 3 Nr. 2 BDSG.

2.6.3 Zuständige Aufsichtsbehörde

Die durch Landesrecht zuständige Aufsichtsbehörde kontrolliert die Ausführung der datenschutzrechtlichen Anforderungen, § 38 Abs. 1 S. 1 BDSG. Zur Gewährleistung des Datenschutzes kann die Aufsichtsbehörde nach § 38 Abs. 5 S 1 BDSG anordnen, dass nach § 9 BDSG festgestellte technische oder organisatorische Mängel beseitigt werden. Bei schwerwiegenden Mängeln kann sie nach § 38 Abs. 5 S 2 BDSG den Einsatz einzelner Verfahren untersagen. Dies gilt insbesondere dann, wenn die Mängel entgegen ihrer Anordnung und trotz Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann nach § 38 Abs. 5 S 3 BDSG die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

2.6.4 Der Bundesbeauftragte für den Datenschutz

Der Bundesbeauftragte für den Datenschutz (BfD) kontrolliert, ob die öffentlichen Stellen des Bundes die Vorschriften über den Datenschutz einhalten, § 24 Abs. 1 BDSG. Jedermann kann sich nach § 21 BDSG an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Eine bestimmte Form ist für die Anrufung nicht vorgeschrieben, an irgendetwelche Fristen ist die Anrufung nicht gebunden.⁴⁵ Der Betroffene kann seinen Anspruch auf Entgegennahme, Prüfung und Bescheidung durch Leistungsklage unter entsprechender Anwendung der Grundsätze zur Untätigkeitsklage vor dem Verwaltungsgericht durchsetzen. Der Bescheid des BfD ist nicht mit Rechtsmitteln angreifbar. Klagen sind gegen die Bundesrepublik Deutschland, vertreten durch den BfD, zu richten.⁴⁶

⁴⁴ Zum behördlichen Datenschutzbeauftragten: *Schild*, DuD 2001, 31 ff.

⁴⁵ *Simitis u.a.*, BDSG/Dammann, § 21 Rdnr. 13-15.

⁴⁶ *Simitis u.a.*, BDSG/Dammann, § 21 Rdnr. 28.

2.7 Datenschutz und Technik

2.7.1 Automatisierte Einzelentscheidung

Die Regelung des § 6a BDSG soll belastende Entscheidungen beschränken, die ausschließlich auf eine automatisierte Verarbeitung wertender personenbezogener Daten gestützt wird. Damit soll der Betroffene vor belastenden Wertungsentscheidungen geschützt werden.

Eine Belastung ist nach der ersten Alternative des § 6a Abs. 1 BDSG bereits gegeben, wenn die Entscheidung eine rechtlich Folge erst „nach sich zieht“. Im öffentlichen Bereich haben in der Regel Verwaltungsakte rechtliche Folgen, wie die Verweigerung, die Rücknahme oder der Widerruf einer Leistung. Im nicht öffentlichen Bereich haben vor allem Willenserklärungen rechtliche Folgen, wie die Kündigung eines Vertrages. Nach der zweiten Alternative des § 6a Abs. 1 BDSG sind automatisierte Entscheidungen untersagt, die den Betroffenen „erheblich beeinträchtigen“. Ein typisches Beispiel sind Scoringverfahren, die in der Kreditwirtschaft zur Bewertung der Kreditwürdigkeit eingesetzt werden und zur Ablehnung des Kreditantrags führen.⁴⁷

Von dem Verbot automatisierter Einzelentscheidungen sieht § 6a Abs. 2 BDSG zwei Ausnahmen vor: wenn dem Begehren des Betroffenen stattgegeben wird und wenn die berechtigten Interessen des Betroffenen gewährleistet werden, insbesondere ihm die Möglichkeit gegeben wird, seinen Standpunkt geltend zu machen.

Der Auskunftsanspruch des Betroffenen auf die zu seiner Person gespeicherten Daten, den Empfänger und den Zweck der Speicherung soll gemäß § 6a Abs. 3 BDSG Transparenz schaffen, indem der Anspruch auch „den logischen Aufbau“ der Daten umfasst.

2.7.2 Videoüberwachung

Mit der Vorschrift des § 6b BDSG wollte der Gesetzgeber die durch öffentliche und nicht öffentliche Stellen bereits durchgeführte Videoüberwachung auf eine gesetzliche Grundlage stellen. So sehen schon Landesgesetzgeber in Polizeigesetzen Befugnisnormen zur Videoüberwachung vor.⁴⁸ Adressat der Regelung sind öffentliche Stellen des Bundes und nicht öffentliche Stellen.

⁴⁷ *Simitis u.a.*, BDSG/ *Bizer*, § 6a Rdnr. 13-31.

⁴⁸ Art. 32 Abs. 2 BayPAG; § 14 Abs. 4 HSOG; § 32 Abs. 3 NdsGefAG; .

Die Beobachtung ohne eine Speicherung der Bilder (Kamera-Monitor-Prinzip) genügt für die Anwendung des § 6b BDSG.⁴⁹ Gegenstand der Beobachtung sind öffentlich zugängliche Räume, wie Bahnsteige, Ausstellungsräume und Schalterhallen.⁵⁰ Die Videoüberwachung öffentlicher Räume ist nach § 6b Abs. 1 BDSG nur zulässig, wenn sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Diese sich inhaltlich überschneidenden Anforderungen werden durch die Gebäudesicherheit, die Zugangskontrolle und den Schutz des Eigentums erfüllt.⁵¹ Die Videoüberwachung muss für diese Zwecke erforderlich sein. Können diese Zwecke durch andere Mittel erreicht werden, so ist auf die Videoüberwachung zu verzichten. Die Videoüberwachung muss durch geeignete Maßnahmen erkennbar gemacht werden, § 6b Abs. 2 BDSG. Dies wird durch optische Hinweise im Blickfeld des Betroffenen und akustische Hinweise erreicht, die sich wiederholen. Dies ermöglicht dem Betroffenen, entweder sein Verhalten unter dem Blick der Kamera einzurichten oder der Kamera auszuweichen.⁵²

Von der Zulässigkeit der Beobachtung kann nicht auf die Verarbeitung oder Nutzung der erhobenen personenbezogenen Daten geschlossen werden. Vielmehr muss nach § 6b Abs. 3 BDSG in einem eigenen Prüfschritt die Erforderlichkeit der weiteren Verarbeitung oder Nutzung festgestellt werden. So ist eine längere Speicherung zur Abwehr konkreter Gefahren nicht erforderlich, wohl aber zur Beweissicherung für ein späteres Gerichtsverfahren.⁵³ Die Verarbeitung und Nutzung ist grundsätzlich auf den Beobachtungszweck beschränkt. Dieser Grundsatz wird zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung durchbrochen, § 6b Abs. 3 S. 2 BDSG.

Der Betroffene muss nach § 6b Abs. 4 BDSG über eine Verarbeitung oder Nutzung seiner Daten benachrichtigt werden, wenn durch die Videoüberwachung erhobene Daten seiner Person zugeordnet werden. Die Zuordnung zu einer durch weitere Informationen lediglich bestimmbar Person löst die Benachrichtigungspflicht nicht aus. Erforderlich ist die Kenntnis der Identität des Betroffenen, insbesondere durch seinen Namen.

⁴⁹ *Simitis u.a.*, BDSG/ Bizer, § 6b Rdnr. 37.

⁵⁰ Zur Videoüberwachung öffentlicher Plätze: *Achelpöhler/Niehaus*, DuD 2002, 731 ff.

⁵¹ *Simitis u.a.*, BDSG/ Bizer, § 6b Rdnr. 46 und 52..

⁵² *Simitis u.a.*, BDSG/ Bizer, § 6b Rdnr. 66.

⁵³ *Simitis u.a.*, BDSG/ Bizer, § 6b Rdnr. 78.

Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie nicht mehr erforderlich sind, um den Zweck zu erreichen oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Gelöscht sind die Daten, wenn sie unkenntlich gemacht sind, § 3 Abs. 4 Nr. 5 BDSG. Welches Verfahren anzuwenden ist, lässt die Regelung offen.

2.7.3 Mobile personenbezogene Speicher und RFID

Intelligente Chipkarten in der Hand des Betroffenen wie die elektronische Kundenkarte, die elektronische Krankenversichertenkarte oder der elektronische Dienstaussweis sind der Gegenstand des § 6c BDSG.⁵⁴

Diese Medien definiert § 3 Abs. 10 BDSG: Sie werden an den Betroffenen ausgegeben (§ 3 Abs. 10 Nr. 1 BDSG), von der ausgebenden Stelle können personenbezogene Daten über die Speicherung hinaus automatisiert verarbeitet werden (§ 3 Abs. 10 Nr. 2 BDSG) und der Betroffene kann die Verarbeitung nur durch den Gebrauch des Mediums beeinflussen (§ 3 Abs. 10 Nr. 3 BDSG). Die Regelung setzt nach Nr. 1 eine Stelle voraus, die den mobilen Datenträger an denjenigen ausgibt, dessen personenbezogene Daten auf dem Medium gespeichert und verarbeitet werden. Nach § 3 Abs. 10 Nr. 2 BDSG müssen auf dem mobilen Medium über die Speicherung hinaus personenbezogene Daten „automatisiert verarbeitet werden können“. Technisch muss das Medium also mit einem Prozessorchip ausgestattet sein, der über das Speichern hinaus auch eine Verarbeitung personenbezogener Daten ermöglicht. Schließlich darf der Betroffene nach § 3 Abs. 10 Nr. 3 BDSG die Datenverarbeitung auf dem Medium nur durch den Gebrauch des Mediums beeinflussen. Gebrauch liegt vor, wenn das Medium in ein Lesegerät eingeführt oder im Fall einer kontaktlosen Karte an ihm vorbeigeführt wird. Der Gegenbegriff zum Gebrauch ist das eigenständige Steuern von Verarbeitungsprozessen durch die Eingabe von Befehlen beispielsweise an einer Tastatur oder über eine Sprachsteuerung. Dies ist beispielsweise der Fall bei Mobiltelefon, Laptop, Notebook, Palm, PDA.⁵⁵ Somit sind dies Datenverarbeitungsanlagen im Sinne von § 3 Abs. 2 BDSG.

§ 6c Abs. 1 BDSG enthält eine Verpflichtung zur Unterrichtung des Betroffenen über den für die Ausgabe des Mediums bzw. für das automatisierte Verfahren Verantwortlichen (Nr. 1), die Funktionsweise des Mediums und der zu verarbeitenden Daten (Nr. 2), der Ausübung der

⁵⁴ *Simitis u.a.*, BDSG/ *Bizer*, § 6c Rdnr. 7.

⁵⁵ *Simitis u.a.*, BDSG/ *Bizer*, § 3 Rdnr. 278, § 6c Rdnr. 2.

Rechte des Betroffenen (Nr. 3) sowie die bei Verlust oder Zerstörung zu treffenden Maßnahmen (Nr. 4).

Nach § 6c Abs. 2 BDSG müssen die nach Absatz 1 verpflichteten Stellen dafür Sorge tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

Nach § 6c Abs. 3 BDSG müssen Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, für den Betroffenen eindeutig erkennbar sein. Diese Signalisierung soll sicherstellen, dass Verarbeitungen nicht unbemerkt, z.B. beim Vorbeigehen an einem Terminal ausgelöst werden.⁵⁶

Eine besondere Art mobiler Speichermedien sind RFID-Chips. Radio Frequency Identification (RFID) dient dem kontaktlosen Speichern und Auslesen von Daten. Die Daten werden auf RFID-Tags gespeichert, die überall befestigt werden können. Diese Systeme sollen die üblichen Barcodes ablösen. Barcodes sind zwar maschinenlesbar, benötigen aber eine Sichtverbindung. RFID-Tags können dagegen Distanzen von bis zu 30 Metern überbrücken. Ein Barcode identifiziert ein Objekt als zu einer bestimmten Kategorie gehörend. RFID-Tags können jedes Objekt mit einer eindeutigen Kennung versehen, durch die sich Informationen zu diesem Gegenstand mit einer Datenbank abgleichen lassen. Hierdurch entstehen zahlreiche Anwendungsmöglichkeiten, so für die Lagerverwaltung, für Zugangskontrollen, für Wegfahrsperrern, für die Tierkennzeichnung oder Mautsysteme. In Verbindung mit Informationen aus anderen Datenbanken können Einkaufs- und Nutzungsprofile personalisiert werden.⁵⁷ Dieses Datenerhebungs- und Datenübermittlungssystem der RFID-Tags wird perfektioniert. Smart Dusts sind Chips, die sich miteinander vernetzen, ihre Umgebung überwachen und die dabei anfallenden Daten an eine Basisstation übersenden. Ambient Intelligent Landscape ist eine Welt, in der Gegenstände miteinander kommunizieren und auf die Anwesenheit von bestimmten Personen mit spezifischen Verhaltensweisen reagieren. Funkchips werden in Alltagsgegenstände integriert, etwa in Medikamente implantiert.

⁵⁶ BT-Drs 14/5793, S. 64.

⁵⁷ Hierzu *Westerholt/Döring*, CR 2004, 710, 711-713.

5.3.2 Rechtlicher Schutz

RFID-Tags ermöglichen die versteckte Datenerhebung und übermitteln die Daten. Hierauf kann der Betroffene nicht Einfluss nehmen. Rechtlicher Schutz soll durch das Prinzip der Transparenz gewährt werden. Dies ist ein internationales datenschutzrechtliches Verständnis mit unterschiedlicher Ausprägung. Nach deutschem Recht gelten RFID-Funktionen als „Mobile personenbezogene Speicher- und Verarbeitungsmedien“ im Sinne von § 6c BDSG, wenn die gespeicherten Daten ohne Beeinflussung durch den Betroffenen übermittelt werden.⁵⁸ Damit muss die Stelle, die den RFID-Tag ausgibt, den Betroffenen über ihre Identität und darüber unterrichten, wie er seine Rechte auf Auskunft, Berichtigung, Löschung und Sperrung wahrnehmen kann.⁵⁹ Die Internationale Konferenz der Datenschutzbeauftragten hielt 2003 in einer Resolution fest, dass personenbezogene Daten aus RFID-Tags nur in einer offenen und transparenten Weise erhoben werden dürfen, um einen ungerechtfertigten Eingriff in die Privatsphäre zu verhindern. Das US-amerikanische Auto-ID Center des MIT verlangt ein Recht „to know whether a product contains an EPC-Tag (Electronic Product Code)“. Nach dem Kalifornischen Gesetz zum Konsumentenschutz können personenbezogene Daten, die anhand von RFID-Tags ermittelt werden, nur nach schriftlicher Einwilligung des Betroffenen auf dem RFID-Tag oder beim Händler gespeichert werden.⁶⁰

2.7.4 Automatisierte Abrufverfahren

Der automatisierte Abruf von Daten ist Bestandteil der Telekommunikationsgesellschaft. So kann in der Organisation des Telebanking die Telebank auf die Konten der Kunden bei der Mutterbank zugreifen. Personenbezogene Daten, die eine verarbeitende Stelle zum automatisierten Abruf bereithält, unterliegen besonderen Zulässigkeitsanforderungen, § 10 BDSG. Voraussetzung für die Zulässigkeit ist nach § 10 Abs. 1 BDSG eine Abwägung der Angemessenheit der schutzwürdigen Interessen der Betroffenen mit den Aufgaben und dem Geschäftszweck der verarbeitenden Stellen. Die Angemessenheit kann bei einem Bedürfnis nach besonders schneller Auskunft ebenso gegeben sein wie bei einem sehr großen Umfang von Übermittlungen, sogenannten Massenübermittlungen.⁶¹ Die Zulässigkeit des Abrufverfahrens muss nach § 10 Abs. 2 BDSG kontrolliert werden können. Deshalb sind die Anforderungen des Abrufverfahrens schriftlich festzulegen. Gegenstand dieser Vereinbarung

⁵⁸ *Gola/Schomerus*, § 6c Rz. 2.

⁵⁹ Hierzu *Bizer, Simitis u.a.*, 3 6c Rz. 50 f.

⁶⁰ www.datenschutz.de „Kalifornischer Gesetzesentwurf zum Schutz der Verbraucher vor RFID im Einzelhandel.“

⁶¹ *Gola/Schomerus*, Bundesdatenschutzgesetz, § 10 Rdnr. 11.

sind Anlass und Zweck des Abrufverfahrens, Datenempfänger, Art der zu übermittelnden Daten und die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen. Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt nach § 10 Abs. 4 BDSG die abrufende Stelle. Damit obliegt dem Empfänger beim automatisierten Abrufverfahren die Einhaltung sämtlicher Zulässigkeitsvoraussetzungen für die Datenübermittlung.

2.7.5 Datensicherung

Im öffentlichen und privaten Bereich hat der Anwender unter dem Schlagwort „Datensicherheit“ für eine angemessene, technische und organisatorische Realisierung des Datenschutzes zu sorgen § 9 BDSG. Bei der automatisierten Datenverarbeitung gelten die präzisierten Anforderungen in der Anlage zu § 9 BDSG für 8 Kontrollbereiche: den Zutritt, den Zugang, den Zugriff, die Weitergabe, die Eingabe, die Auftragsverarbeitung, die Datenverfügbarkeit und die getrennte Datenverarbeitung. Nach einer Verhältnismäßigkeitsklausel sind Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht, § 9 Satz 2 BDSG. Damit ist eine der Sensibilität der personenbezogenen Daten angemessene Datensicherung zu organisieren.

2.7.6 Datenschutzaudit

Anbieter von Datenverarbeitungssystemen und –programmen sowie datenverarbeitende Stellen können gemäß § 9a BDSG „zur Verbesserung des Datenschutzes und der Datensicherheit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen“.⁶² Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter bleibt einem Ausführungsgesetz überlassen, denn die Anforderungen haben Berufs beschränkenden Charakter. Die Vorlage des Ausführungsgesetzes ist für die 15. Legislaturperiode angekündigt.⁶³

2.8 Auftragsdatenverarbeitung

Für die Datenverarbeitung im Auftrag gemäß § 11 BDSG ist die wichtigste Voraussetzung, dass die Erhebung, Verarbeitung und Nutzung lediglich in ihrer Hilfsfunktion für die Erfüllung der Aufgaben und Geschäftszwecke der verantwortlichen Stelle ausgelagert wird.

⁶² Zu Audits und Gütesiegeln im Datenschutz: *Bäumler*, CR 2001, 795-800; zum bisherigen Stand der Umsetzung: *Schaar/Stutz*, DuD 2002, 330 ff.

⁶³ *Simitis u.a.*, BDSG/ *Bizer*, § 9a Rdnr. 76.

Der Auftragnehmer darf nach § 11 Abs. 3 Satz 1 BDSG die Daten nur „im Rahmen der Weisungen des Auftraggebers“ erheben, verarbeiten und nutzen. Unter „Weisungen“ sind alle vom Auftragnehmer vertraglich übernommenen Pflichten in Bezug auf Art und Gegenstand der Erhebung, Verarbeitung oder Nutzung sowie die technisch-organisatorische Datensicherung zu verstehen. Werden die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecke teilweise abgegeben oder erbringt der externe Datenverarbeiter über die technische Verarbeitung hinaus materielle vertragliche Leistungen mit Hilfe der überlassenen Daten, dann ist er nicht mehr bloßer Auftragnehmer, sondern wird selbst zur verantwortlichen Stelle. Die Datenweitergabe im Rahmen einer solchen „Funktionsübertragung“ ist konsequenterweise als Übermittlung zu klassifizieren.⁶⁴ § 11 Abs. 2 Satz 2 BDSG verlangt, dass der Auftrag schriftlich zu erteilen ist. In dem schriftlichen Vertrag sind die „Datenerhebung, -verarbeitung oder -nutzung“ festzulegen. Damit sind die Phasen der Datenverarbeitung angesprochen. Zu fixieren sind ferner die „technischen und organisatorischen Maßnahmen“ der Datensicherung. Sie müssen den Zeitraum von dem Eingang der Daten beim Auftragnehmer bis zu Ablieferung beim Auftraggeber umfassen.⁶⁵

2.9 Grenzüberschreitende Datenübermittlung

Entsprechend den Vorgaben der EG-Datenschutzrichtlinie gelten für Unternehmen mit Sitz im Inland und für Unternehmen mit Sitz im Ausland die folgenden Regeln.

2.9.1 Unternehmen mit Sitz im Inland

Für Unternehmen mit Sitz im Inland regelt das BDSG die Datenübermittlung in ein anderes EU-Mitgliedsland und in ein EU-Drittland unterschiedlich.

- Datenübermittlung von der BRD in ein anderes EU-Mitgliedsland

Durch die Umsetzung der EG-Datenschutzrichtlinie (EG-DatSchRL) in den einzelnen Mitgliedsländern ist in dem EU-Raum ein einheitliches Datenschutzniveau entstanden. Deshalb ist für Unternehmen mit Sitz im Inland die grenzüberschreitende Datenübermittlung innerhalb des EU-Raums unter den Voraussetzungen, wie sie auch für die Übermittlung im Inland gelten, mit § 4b Abs. 1 BDSG als zulässig erklärt. Ein Unternehmen mit Sitz im Inland

⁶⁴ *Simitis u.a.*, BDSG/ *Walz*, § 11 Rdnr. 18.

⁶⁵ *Simitis u.a.*, BDSG/ *Walz*, § 11 Rdnr. 50.

ist also berechtigt, personenbezogene Daten EU-weit zu übermitteln, wenn dieses Recht nach § 28 BDSG besteht.⁶⁶

- Datenübermittlung von der BRD in Drittländer

Übermittlungen in Drittländer müssen, wie die Übermittlungen nach § 4 b Abs. 1 BDSG im EU-Raum, den Anforderungen der BDSG-Vorschriften entsprechen, § 4 b Abs. 2 S. 1 BDSG. Die Übermittlung muss unterbleiben, wenn der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn ein angemessener Datenschutz im Drittland nicht gewährleistet ist, § 4b Abs. 2 S. 2 BDSG. Die Angemessenheit des Schutzniveaus wird nach § 4b Abs. 3 BDSG unter Berücksichtigung aller Umstände beurteilt, die bei der Datenübermittlung von Bedeutung sind. Hierzu zählen die Art der Daten, die Zweckbestimmung, die Dauer der Verarbeitung, die für den Empfänger geltenden Rechtsnormen, Standesregeln und Sicherheitsmaßnahmen.⁶⁷ Die Angemessenheit des Schutzniveaus ist von der EU-Kommission nach Art. 25 DSchRL für die Schweiz und Kanada festgestellt worden.⁶⁸ Eine weitere Entscheidung zu Art. 25 DSchRL hat die EU-Kommission zu Datenübermittlungen in die USA getroffen. Danach gewährleistet das mit dem USA-Handelsministerium ausgehandelte Safe-Harbor-Verfahren einen angemessenen Datenschutz. Hierzu muss sich der Empfänger in den USA durch Erklärungen gegenüber der zuständigen US-Behörde zur Einhaltung bestimmter Datenschutzprinzipien verpflichten. Für andere Drittländer ist es wegen der komplexen Kriterien kaum möglich, das angemessene Schutzniveau zu bestimmen.⁶⁹ Deshalb sind die in § 4c Abs. 1 und Abs. 2 BDSG bestimmten Ausnahmen wichtig, nach denen eine Datenübermittlung in Drittstaaten zulässig ist, auch wenn ein angemessenes Datenschutzniveau nicht gewährleistet ist.

Nach § 4c Abs. 1 BDSG ermöglichen die Einwilligung des Betroffenen und die Übermittlung zur Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle die grenzüberschreitende Datenübermittlung. So bilden die Einwilligung und der Vertragszweck die Rechtsgrundlage für die Übermittlung von Daten im Reiseverkehr.⁷⁰

In allen anderen Fällen ermöglicht es die „genehmigungspflichtige Vertragslösung“ des § 4c Abs. 2 BDSG der verarbeitenden Stelle, Datenübermittlungen in Empfängerländer

⁶⁶ *Gola/Schomerus*, Bundesdatenschutzgesetz, § 4b Rdnr. 2-3.

⁶⁷ Zum angemessenen Schutzniveau: *Räther/Seitz*, MMR 2002, 425, 426 f.

⁶⁸ *Simitis u.a.*, BDSG/*Simitis*, § 4b Rdnr. 65.

⁶⁹ *Simitis u.a.*, BDSG/*Simitis*, § 4b Rdnr. 52-64.

⁷⁰ Zu den Anwendungsfällen: *Simitis u.a.*, BDSG/*Simitis*, § 4c Rdnr. 7-24.

vorzunehmen, in denen ein angemessenes Datenschutzniveau nicht sichergestellt ist.⁷¹ Die Vertragsklauseln oder „verbindlichen Unternehmensregelungen“ müssen ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechtes bieten und vorab durch die zuständige Aufsichtsbehörde genehmigt werden, § 4c Abs. 2 Satz 1 BDSG. Für internationale Konzerne ist es empfehlenswert zur Vereinfachung von Genehmigungsverfahren auf Standardvertragsklauseln zurückzugreifen, wie sie in einer gemeinsamen Studie des Europarats, der Europäischen Kommission und der Internationalen Handelskammer entwickelt worden sind.⁷² Auch Selbstverpflichtungen in Unternehmensrichtlinien können den Datenfluss innerhalb internationaler Konzerne ermöglichen. Diese sog. Codes of Conduct müssen den Betroffenen ebenso rechtlich garantierte Rechtspositionen einräumen, wie es bei der Vertragslösung der Fall ist.⁷³

2.9.2 Unternehmen mit Sitz im Ausland

Unternehmen mit Sitz in einem EU-Mitgliedsland, die in der BRD Daten erheben, verarbeiten und nutzen, unterliegen anderen datenschutzrechtlichen Anforderungen als Unternehmen, die mit Sitz im EU-Ausland, in der BRD Daten erheben, verarbeiten und nutzen.

- Erhebung, Verarbeitung und Nutzung von Daten in der BRD durch ein Unternehmen mit Sitz in einem anderen EU-Mitgliedsland.

Auf Unternehmen mit Sitz in einem anderen EU-Mitgliedsstaat findet das BDSG nach § 1 Abs. 5 Satz 1 BDSG keine Anwendung. Wenn diese im deutschen Inland Daten erheben, verarbeiten oder nutzen, so gilt nach dem Sitzprinzip das Datenschutzrecht des Mitgliedstaates, in dem die Stellen ihren Sitz haben. Nur wenn diese Stellen eine Niederlassung im deutschen Inland haben, gilt nach dem Territorialprinzip deutsches Datenschutzrecht,⁷⁴

- Erhebung, Verarbeitung und Nutzung von Daten in der BRD durch Unternehmen mit Sitz in Drittländern.

Für Stellen mit Sitz in Drittländern gilt nach dem Territorialprinzip bei der Erhebung, Verarbeitung oder Nutzung von Daten in der BRD das BDSG, § 1 Abs. 5 S 2 BDSG.⁷⁵

⁷¹ Zur Vertragslösung: *Räther/Seitz*, MMR 2002, 520-528 und *Büllesbach/Höss-Löw*, DuD 2001, 135 ff.

⁷² *Simitis u.a.*, BDSG/*Simitis*, § 4c Rdnr. 42-50.

⁷³ *Gola/Schomerus*, BDSG-Kommentar, 8. Aufl. 2005, § 4c Rz. 9.

⁷⁴ *Gola/Schomerus*, Bundesdatenschutzgesetz, § 1 Rdnr. 27-28.

⁷⁵ *Gola/Schomerus*, Bundesdatenschutzgesetz, § 1 Rdnr. 29.

2.9.3 Ergebnis

Im EU-Raum gilt das Datenschutzrecht des Staates, in dem das datenverarbeitende Unternehmen seinen Sitz hat:

- Für Unternehmen mit Sitz im Inland gilt das BDSG, § 4b Abs. 1 BDSG.
- Für Unternehmen mit Sitz in einem anderen EU-Mitgliedsland gilt das Datenschutzrecht des Sitzlandes, § 1 Abs. 5 S. 1 BDSG.

Die datenschutzrechtlichen Beziehungen zwischen der BRD und EU-Drittstaaten werden durch folgende Regeln bestimmt:

- Datenübermittlung vom Inland in ein EU-Drittland erfordert angemessenes Datenschutzniveau im Drittland (§ 4b Abs. 2 und 3 BDSG) oder eine Ausnahmeregel für die Angemessenheit nach § 4c BDSG.
- Für Unternehmen mit Sitz in einem EU-Drittland, die im Inland Daten erheben, verarbeiten und nutzen, gilt das BDSG, § 1 Abs. 5 S 2 BDSG.

2.10 Bußgeldvorschriften

§ 43 Abs. 1

§ 4d

eine Meldung unterbleibt (Abs. 1 Nr. 1)

§ 4f

der Beauftragte für den Datenschutz wird nicht bestellt (Abs. 1 Nr.2)

§ 28

den Betroffenen nicht rechtzeitig unterrichtet (Abs. 1 Nr. 3) die Daten unbefugt übermittelt oder nutzt (Abs. 1 Nr. 4).

§ 29

Gründe nicht aufzeichnet (Abs. 1 Nr. 5), Daten in Verzeichnisse aufnimmt (Abs. 1 Nr. 6), die Übernahme von Kennzeichnungen nicht sicherstellt (Abs. 1 Nr. 7).

§ 33

den Betroffenen nicht benachrichtigt (Abs. 1 Nr. 8)

§ 35

Daten ohne Gegendarstellung übernimmt Abs. 1 Nr. 9)

§ 38

Dem Betroffenen nicht eine Auskunft erteilt (Abs. 1 Nr. 10) und einer Anordnung zuwiderhandelt (Abs. 1 Nr. 11.)

§ 43 Abs. 2

§ 1 Abs. 2

unbefugtes Erheben oder Verarbeiten (Abs. 2 Nr.1) unbefugt zum Abruf mittels

§ 10

automatisierte Verfahren bereithalten (Abs. 2 Nr. 2) oder abrufen (Abs. 2 Nr. 3)

§ 16 Abs. 4 Satz 1,

§ 28 Abs. 5 Satz 1

die Übermittlung erschleicht (Abs. 2 Nr. 4) die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt (Abs. 2 Nr. 5)

§ 30 Abs. 1 Satz 2,

§ 40 Abs. 2 Satz 3

Merkmale über persönliche und sachliche Verhältnisse mit Einzelangaben zusammenführt (Abs. 2 Nr. 6).

§ 44

Antragsdelikt, das bei vorsätzlicher Handlung gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht mit Freiheitsstrafe bestraft oder mit Geldstrafe bestraft wird.

3.0 Das neue Telemediengesetz

Das Telemediengesetz hat eine lange Geschichte. Im Jahre 1997 wurden mit dem Informations- und Kommunikationsdienstegesetz (IuKDG) rechtliche Rahmenbedingungen für die neuen Dienste in der Informationsgesellschaft, die Teledienste, geschaffen. Durch das Teledienstegesetz (TDG) entstanden Regeln für die Zulassungsfreiheit, die Informationspflichten und die Verantwortlichkeit für Inhalte. Durch das Teledienstedatenschutzgesetz (TDDSG) entstanden Regeln für den Datenschutz. Mit der europäischen „Richtlinie über den elektronischen Geschäftsverkehr“ traten neue Regeln in Kraft, die in Deutschland mit dem „Elektronischen-Geschäftsverkehr-Gesetz“ (EGG) im TDG umgesetzt wurden. Zugleich erfolgte eine Novellierung des TDDSG auf Grund der Erfahrungen und Entwicklungen seit Inkrafttreten des IuKDG. Bund und Länder haben sich Ende 2004 auf weitere Schritte verständigt, die Medienordnung zu entwickeln und am 19.4.2005 den „Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer – Geschäftsverkehr – Vereinheitlichungsgesetz – ElGVG)“ vorgelegt. Das Bundeskabinett hat am 16. Juni 2006 den Entwurf für dieses Gesetz beschlossen. Am 18.1.2007 ist das Gesetz in dritter Lesung von dem Bundestag verabschiedet worden. Mit Artikel 1 dieses Gesetzes werden die rechtlichen Anforderungen für Tele- und Mediendienste in einem Telemediengesetz zusammengefasst. Für das Thema des Datenschutzes sind der Geltungsbereich des Gesetzes (3.1), die Anbieter-Nutzerbeziehung und die bereichsspezifischen datenschutzrechtlichen Vorschriften (3.3) relevant.

3.1 Geltungsbereich

Das Gesetz gilt nach § 1 Abs. 1 Satz 1 TMG für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht ausschließlich Telekommunikation nach § 3 Nr. 22 TKG oder Rundfunk im Sinne von § 2 des Rundfunkstaatsvertrages sind.

Die bisher in § 2 TDG und MDSStV enthaltenen Regelbeispiele werden zwar nicht aufgenommen, sind nach der Gesetzesbegründung aber weiterhin charakteristisch für Telemediendienste, wie

- Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit,

- Video auf Abruf, soweit es sich nicht nach Form und Inhalt um einen Fernsehdienst handelt,
- Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen,
- die kommerzielle Verbreitung von Informationen über Waren/Dienstleistungsangebote mit elektronischer Post.⁷⁶

Eine komplizierte Stellung zwischen TMG und TKG haben Telekommunikationsdienste, die neben der Übertragungsdienstleistung noch eine inhaltliche Dienstleistung anbieten, wie den Internetzugang und die E-Mail-Übertragung. Sie gelten wegen der Übertragungsdienstleistung als Telekommunikationsdienste und wegen der inhaltlichen Dienstleistung als Telemediendienste. Für sie gelten die Regeln des TMG zum Herkunftslandprinzip, zur Zugangsfreiheit und zur Haftungsprivilegierung. Der Datenschutz regelt sich nach dem TKG. Dies hat wesentliche Folgen für die E-Mail-Kommunikation: Die TK-Diensteanbieter müssen das Fernmeldegeheimnis nach § 88 TKG beachten, Bestandsdaten (§ 95 TKG) und Verkehrsdaten (§ 96 TKG) speichern und die Sicherheitsbehörden können unter den gegebenen gesetzlichen Voraussetzung auf diese Daten zugreifen (§§ 110 ff. TKG).⁷⁷

Für die Anwendung des TMG spielt es nach § 1 Abs. 1 Satz 2 keine Rolle, ob ein Diensteanbieter die Nutzung seiner Angebote ganz oder teilweise unentgeltlich oder gegen Entgelt ermöglicht. Dies entspricht der bisherigen Regelung des § 2 Abs. 3 TDG. In § 1 Abs. 1 Satz 2 TMG wird auch klargestellt, dass das Gesetz für private Anbieter und öffentliche Stellen gleichermaßen gilt. Denn es besteht kein Anlass, die öffentlichen Stellen aus dem Geltungsbereich des Gesetzes herauszunehmen, insbesondere nicht im Hinblick auf die Informationspflichten und die Haftungsprivilegierung.

Als Datenschutzbestimmungen für Telemediendienste (§§ 11 – 15 TMG) sind bis auf geringe redaktionelle Änderungen die Vorschriften des TDDSG übernommen worden. Sie regeln das Anbieter-Nutzerverhältnis (3.2), den Gesetzes- und Einwilligungsvorbehalt (3.3), die organisatorischen Pflichten des Diensteanbieters (3.4), den Schutz der Bestands- (3.5) und der Nutzungsdaten (3.6).

⁷⁶ Begründung zum EIGVG S. 18.

⁷⁷ Begründung zum EIGVG S. 17.

3.2 Anbieter-Nutzer-Verhältnis

§ 1 Abs. 1 TMG enthält eine sehr weit gefasste Begriffsbestimmung für Teledienste: alle elektronischen Informations- und Kommunikationsdienste soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG sind. Diese Begriffsbestimmung erfordert für das Datenschutzrecht des TMG eine Klarstellung: Nach § 11 Abs. 1 TMG gelten die datenschutzrechtlichen Vorschriften nicht in Bereichen, in denen eine Anwendung der speziellen datenschutzrechtlichen Grundsätze des TMG als Schutzrecht für Endverbraucher nicht sachgerecht ist. Dies ist die Nutzung von Informations- und Kommunikationssystemen zu ausschließlich beruflichen oder dienstlichen Zwecken und zur ausschließlichen Steuerung von Arbeits- oder Geschäftsprozessen.⁷⁸ Auch der Nutzerbegriff wurde durch § 11 Abs. 2 TMG anders als in § 2 Nr. 3 TMG geregelt, indem die juristischen Personen aus dem Nutzerbegriff herausgenommen wurden, da diese nicht Inhaber personenbezogener Daten sein können.⁷⁹

3.3 Gesetzes- und Einwilligungsvorbehalt

§ 12 TMG regelt entsprechend dem früheren § 3 TDDSG den Gesetzes- und Einwilligungsvorbehalt für das Erheben und Verwenden personenbezogener Daten (§ 12 Abs. 1 und Abs. 2 TMG), das Verbot, die Bereitstellung von Telemedien von einer Einwilligung des Nutzers in eine bestimmte Verwendung seiner Daten abhängig zu machen (§ 12 Abs. 3 TMG) und die Anwendung der Schutzvorschriften, wenn die Daten nicht automatisiert verarbeitet werden (§ 12 Abs. 4 TMG).

3.4 Organisatorische Pflichten des Diensteanbieters

Mit § 13 TMG werden die Pflichten des Diensteanbieters entsprechend § 4 TDDSG mit lediglich redaktionellen Änderungen übernommen. Es handelt sich um die Informationspflichten über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten (Abs. 1), um die Regelung zur elektronischen Einwilligung (Abs. 2 und 3), um die technischen und organisatorischen Vorkehrungen (Abs. 4), um die Anzeige der Weitervermittlung zu einem anderen Diensteanbieter (Abs. 5), die anonyme oder pseudonyme Zahlung (Abs. 6) und das Recht des Nutzers auf Auskunft (Abs. 7).

⁷⁸ BT Drucks. 14/6098, S. 27.

⁷⁹ *Schaar*, Datenschutz im Internet, S. 234 ff.

3.5 Bestandsdaten

3.5.1 Definition und der Grundsatz der Erforderlichkeit

Der Datenschutz der Bestandsdaten ist entsprechend § 5 TDDSG in § 14 TMG geregelt. Der Gesetzgeber hat in § 14 Abs. 1 TMG, wie schon in § 5 TDDSG, von einer katalogartigen Aufzählung möglicher Bestandsdaten abgesehen, weil die Vielfältigkeit möglicher Teledienste eine kasuistische Aufzählung ausschließt. Als typische Arten von personenbezogenen Daten, die zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Telemediendienste-Vertrages geeignet sind, gelten Name, Vorname, Anschrift, Rufnummer, Teilnehmer- oder Anschlusskennung, persönliches Kennwort, Passwort, E-mail-Adresse, Geburtsdatum, Kreditkartennummer, Bankverbindung.⁸⁰ Bestandsdaten können nach § 14 Abs. 1 TMG nur erhoben, verarbeitet und genutzt werden, wenn dies erforderlich ist. Das Kriterium der „Erforderlichkeit“ ist für die Frage von erheblicher Bedeutung, ob ein Diensteanbieter im Vorfeld des Vertragsabschlusses Bestandsdaten über den Nutzer erheben darf. So verlangen Diensteanbieter häufig von Nutzern die Angabe personenbezogener Informationen, wenn der Nutzer das Angebot kostenlos sichten und Informationen auf seinen Rechner herunterladen will. Das TMG erlaubt durch § 14 Abs. 1 die Erhebung von Bestandsdaten nur zur Begründung, zur inhaltlichen Ausgestaltung oder Änderung eines Telemediendienste-Vertrages. Die Datenverarbeitung im Rahmen eines vorvertraglichen Vertrauensverhältnisses ist damit nicht erlaubt.⁸¹ Die Pflicht zur Löschung von Bestandsdaten ist in § 14 TMG nicht ausdrücklich geregelt. Diese Pflicht ergibt sich aus dem Grundsatz der Erforderlichkeit. Nach diesem Grundsatz sind die Bestandsdaten zu löschen, wenn sie nicht mehr zur Begründung, Ausgestaltung und Änderung des Telemediendienste-Vertrages erforderlich sind, etwa weil das Vertragsverhältnis beendet ist und nachträgliche Ansprüche nicht mehr bestehen.

3.5.2 Das Recht zur Auskunft

§ 14 Abs. 2 TMG ergänzt die bisher in § 5 Satz 2 TDDSG geregelt Befugnis zur Auskunftserteilung für Zwecke der Strafverfolgung, indem die Verfassungsschutzbehörden des Bundes und der Länder, der Bundesnachrichtendienst und der Militärische Abschirmdienst aufgenommen worden sind. Auf diese Weise wird der Kreis der Behörden, an die Bestandsdaten übermittelt werden dürfen, erweitert. Die Vorschrift konstituiert weder eine eigene Übermittlungsverpflichtung gegenüber den genannten Stellen, noch gibt sie diesen das

⁸⁰ Dix in *Roßnagel*, Recht der Multimedia-Dienste, § 5 Rz. 27-28.

⁸¹ Dix in *Roßnagel*, Recht der Multimedia-Dienste, § 5 Rz. 37-38.

Recht auf automatisierten Zugriff zu Kundendateien. Die Regelung soll lediglich klarstellen, dass die Anbieter von Telemediendiensten berechtigt sind, den genannten Stellen die Daten zu übermitteln, die diese berechtigt erheben und dass das Datenschutzrecht dies nicht verhindert. Damit wird klargestellt, dass Bestandsdaten aufgrund § 94 StPO beschlagnahmt werden dürfen und dass der Diensteanbieter die Daten gemäß § 95 StPO herauszugeben hat.⁸²

3.6 Nutzungsdaten

Die Regelung der Nutzungsdaten nach § 6 TDDSG ist in § 15 TMG übernommen worden.

3.6.1 Definition

Nach der beispielhaften Auflistung in § 15 Abs. 1 TMG sind Nutzungsdaten insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemediendienste. Hierzu gehören Steuerungsinformationen und Informationen zur Bestimmung der Interaktionspartner. Typische Steuerungsinformationen sind die Beschreibung des technischen Dienstes, der genutzt werden soll wie das File Transfer Protocol, die Bezeichnung einer Seite im WorldWideWeb als URL, die Anfragen bei einer Suchmaschine, Angaben über den eingesetzten Browsertyp, der mit Identifikationsdaten verbunden ist. Informationen zur Bestimmung des Interaktionspartners sind E-Mail-Adressen, Nutzerkennungen einschließlich persönlicher Identifikationsnummern (PIN) und Transaktionsnummern (TAN), IP-Adressen, die eine Identifikation des Nutzers, wie durch die statische Zuordnung, zulassen.⁸³

3.6.2 Werbung

§ 15 Abs. 3 TMG enthält in Satz 1 die gesetzliche Erlaubnis des Diensteanbieters für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile unter Verwendung von Pseudonymen zu erstellen.

3.6.3 Abrechnungsdaten

Nach § 15 Abs. 4 TMG ist der Diensteanbieter berechtigt, Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus zu verarbeiten und zu nutzen, soweit sie für Zwecke der

⁸² *Schaar*, Datenschutz im Internet, S. 257.

⁸³ *Dix/Schaar in Roßnagel*, Recht der Multimedia-Dienste, § 6 Rz. 82-86.

Abrechnung erforderlich sind. Sind Nutzungsdaten hierfür nicht erforderlich, so sind sie zu löschen. Zeitlicher Anknüpfungspunkt für die Löschung ist das Ende der jeweiligen Nutzung. Ist eine sofortige Löschung nicht oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so reicht die Löschung im Rahmen der täglichen Reorganisation des Datenbestandes aus.⁸⁴ Nach § 15 Abs. 4 S. 2 TMG ist es möglich, entsprechend § 3 Nr. 4 BDSG Daten zu sperren. Damit wird besonderen Aufbewahrungsfristen Rechnung getragen. So sind beispielsweise Bestands- und Abrechnungsdaten im Rahmen der kaufmännischen Buchführung nach Handelsrecht (§ 257 HGB) und Steuerrecht (§ 147 AO) 10 Jahre aufzubewahren, wenn sie Bestandteil kaufmännischer Belege sind.⁸⁵

3.6.4 Erheben, Verarbeiten und Nutzen von Abrechnungsdaten

Sieht der Diensteanbieter ein Verfahren zur personenbezogenen Bezahlung von Telemediendiensten vor, so darf er nach § 15 Abs. 4 TMG als Abrechnungsdaten personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies für die Abwicklung des Abrechnungsverfahrens erforderlich ist. Wird ein Telemediendienst nach der Nutzungszeit abgerechnet, so rechtfertigt dies eine Speicherung der Zeiten, in denen der Nutzer den Dienst in Anspruch genommen hat. Bei einer mengenmäßigen Tarifierung sind ausschließlich die übertragenen Datenmengen zu speichern.⁸⁶

3.6.5 Übermittlung von Abrechnungsdaten

§ 15 Abs. 5 TMG regelt die Befugnisse des Diensteanbieters zur Übermittlung von Abrechnungsdaten an andere Diensteanbieter oder Dritte. Nach § 15 Abs. 5 S. 1 TMG können Abrechnungsdaten an andere Diensteanbieter oder Dritte für Zwecke der Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer übermittelt werden. Nach § 15 Abs. 5 S. 2 TMG darf der Diensteanbieter einem Dritten Abrechnungsdaten übermitteln, mit dem er einen Vertrag über den Einzug des Entgelts geschlossen hat und soweit es für diesen Zweck erforderlich ist. Damit ist das Outsourcing der Abrechnung von Telediensten erlaubt. Dieses Outsourcing ist mit einer ausdrücklichen Zweckbindung auf die Abrechnung beschränkt. Deshalb sind in dem Outsourcingvertrag die gesetzlichen Vorgaben möglichst konkret abzubilden.

⁸⁴ *Schaar/Schulz in Roßnagel*, Recht der Multimedia-Dienste, § 4 Rz. 81.

⁸⁵ BT Drucks. 14/6098, S. 28.

⁸⁶ *Dix/Schaar in Roßnagel*, Recht der Multimedia-Dienste, § 6 Rz. 119.

3.6.6 Zusammenführen von Nutzungsdaten zu Abrechnungszwecken

§ 15 Absatz 2 TMG stellt als Erlaubnistatbestand klar, dass Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemediendienste zusammengeführt werden dürfen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist. Die Vorschrift ist für die Anbieter von Online-Diensten von praktischer Relevanz, die den Zugang zu vielfältigen Telemediendiensten ermöglichen und für Access-Provider, die die technische Basis für den Zugang zum Internet bereitstellen. Nur wenn ein Anbieter die Abrechnung für verschiedene Telemediendienste übernimmt und für diesen Zweck die Zusammenführung von Nutzungsdaten verschiedener Anbieter erforderlich ist, dürfen diese Daten gemeinsam verarbeitet werden.⁸⁷ Außerhalb dieser Zweckbestimmung ist eine Zusammenführung nur unter den Voraussetzungen des § 12 Abs. 2 TMG zulässig. Danach darf der Diensteanbieter für die Durchführung von Telemediendiensten erhobene personenbezogene Daten für andere Zwecke nur verarbeiten und nutzen, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.⁸⁸

3.6.7 Inhalt der Abrechnung

§ 15 Abs. 6 TMG regelt den Detaillierungsgrad der Abrechnung von Telemediendiensten. Die Abrechnung darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit von einem Nutzer in Anspruch genommener Dienste nur erkennen lassen, wenn der Nutzer dies verlangt. Die Vorschrift ist eine Konkretisierung des in § 3a BDSG verankerten Grundsatzes zur Datenvermeidung und Datenminimierung. Welche Angaben im Regelfall in einer Abrechnung erscheinen dürfen, richtet sich nach dem Abrechnungsmodus. Erscheint die Abrechnung als pauschaler nutzungsunabhängiger Betrag, als sogenannte Flatrate, so sind auf der Abrechnung keine Detailangaben zu vermerken. Nur wenn ein Nutzer einen Einzelnachweis verlangt, darf die Abrechnung auch Detailangaben über die in Anspruch genommenen Telemediendienste enthalten. Die Vorschrift bindet die Erstellung eines Einzelnachweises daran, dass der Kunde einen solchen Nachweis verlangt. Der Begriff „Verlangen“ ist für das Datenschutzrecht ungewöhnlich. Sinnvoll ist die Deutung, dass es sich um eine ausdrückliche Einwilligung handeln muss.⁸⁹

⁸⁷ *Schaar/Schulz in Roßnagel*, Recht der Multimedia-Dienste, § 4 Rz. 99.

⁸⁸ BT Drucks. 14/6098, S. 29.

⁸⁹ *Dix/Schaar in Roßnagel*, Recht der Multimedia-Dienste, § 6 Rz. 182-187.

3.6.8 Löschungsfrist für Einzelnachweise

§ 15 Abs. 7 TMG passt die Löschungsfrist für Einzelnachweise an die 6-Monatsfrist bezüglich der Einzelnachweise in § 97 Abs. 3 TKG an. Abrechnungsdaten, für die ein Einzelnachweis verlangt wird, dürfen nach § 15 Abs. 7 S. 1 TMG höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung gespeichert werden. Zu diesem Zeitpunkt sind die Abrechnungsdaten, für die ein Einzelnachweis verlangt wird, zu löschen. Über diesen Zeitpunkt hinaus dürfen sie nach § 15 Abs. 7 S. 2 TMG nur im Ausnahmefall aufbewahrt werden, wenn innerhalb der 6-Monatsfrist Einwendungen gegen die Entgeltforderung erhoben worden sind oder diese trotz Zahlungsaufforderung nicht beglichen wurde.

3.6.9 Auskunft an die Strafverfolgungsbehörden

Nach § 15 Abs. 5 Satz 4 TMG hat der Diensteanbieter wie im Falle der Abrechnungsdaten (§ 14 Abs. 2 TMG) das Recht, den berechtigten Stellen Auskunft über die Nutzungsdaten zu erteilen, wenn die rechtlichen Voraussetzungen gegeben sind.

3.6.10 Recht zur Datenverarbeitung bei Missbrauch von Telemediendiensten

§ 15 Abs. 8 TMG enthält einen Erlaubnistatbestand, der es einem Diensteanbieter ermöglicht, im Falle des Missbrauchs seiner Telemediendienste durch Nutzer deren Daten für Zwecke der Rechtsverfolgung zu verarbeiten, zu nutzen und an Dritte zu übermitteln. Die Regelung ist sachgerecht: Wie bei den Telekommunikationsanbietern dürfen die Datenschutzbestimmungen dem Diensteanbieter nicht die Möglichkeit nehmen, sich gegen schädigende Handlungen durch Nutzer zu wehren. Die Vorschrift ist eng gehalten. Insbesondere kann der Diensteanbieter nicht beliebig vorgehen. Er muss Anhaltspunkte, die die Annahme eines Missbrauchs durch einen Nutzer nahe legen, dokumentieren, damit diese gegebenenfalls von der Aufsichtsbehörde überprüft werden können.⁹⁰

⁹⁰ BT Drucks. 14/6098, S. 30.