

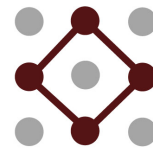


INTARGIA

INTARGIA Managementberatung GmbH

Grundlagen des Datenschutzes in Deutschland

März 2008



IT-SICHERHEITS-
MANAGEMENT



Steffen Weber

Berater IT-Sicherheit und Datenschutz

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1. Zusammenfassung.....	3
2. Geschichtlicher Hintergrund.....	3
3. Rechtliche Aspekte	8
3.1. Datenschutzrechtliche Prinzipien	8
3.2. Allgemeine Datenschutzregeln	9
3.2.1. Betroffenenrechte	10
3.2.2. Datenschutzkontrolle	11
3.2.3. Datensicherheit	12
3.2.4. Regeln für Outsourcing und Konzerne.....	13
3.2.5. Umgang mit besonders riskanten Verfahren	14
3.3. Regelungen zum Mediendatenschutz.....	14
4. Auszug aus dem Bundesdatenschutzgesetz (BDSG).....	15
Literatur- und Quellenverzeichnis.....	17

1. Zusammenfassung

Unser heutiges Verständnis von „Datenschutz“ als Schutz des Einzelnen vor Missbrauch seiner persönlichen Daten wurde entscheidend in den frühen 1980ern geprägt. Im Zusammenhang mit der 1982 von der damaligen Bundesregierung erstmalig als Totalerhebung geplanten Volkszählung entschied das Bundesverfassungsgericht, dass aufgrund von Kritikpunkten wie z. B. der zu umfassenden Datenerhebung oder der fehlenden Anonymisierung eine Volkszählung dieser Art als verfassungswidrig. Das Grundrecht auf informationelle Selbstbestimmung war geboren.

Basierend auf diesem Urteil wurde 1990 das Bundesdatenschutzgesetz novelliert. Diese Fassung bildet, trotz zweier weiteren Anpassungen, immer noch das Grundgerüst für das heutige Datenschutzrecht. Viele Versuchen der jeweiligen Bundesregierung (bekannt geworden sind einige dieser Sachverhalte unter Schlagwörtern wie „Großer Lauschangriff“, „Vorratsdatenspeicherung“, „Bundestrojaner“ oder „Rasterfahndung“), die alle auf eine Aushöhlung und/oder Umgehung der Vorgaben des Volkszählungsurteils ausgerichtet waren, wurden vom Bundesverfassungsgericht mit Hinweis auf das zu den Persönlichkeitsrechten zählende Grundrecht auf informationelle Selbstbestimmung für ganz oder teilweise verfassungswidrig erklärt.

Diese höchstrichterlichen Urteile wurden bis heute in der Fachliteratur als Anlass genommen, einige datenschutzrechtliche Konzepte als Voraussetzung für die Umsetzung des Datenschutzrechts in Deutschland zu sehen. Beispiele sind unter anderem die Prinzipien der Datensparsamkeit, der Datenvermeidung oder allgemeine Regelungen wie die Betroffenenrechte oder Vorgaben zur Datensicherheit mittels technischer und organisatorischer Maßnahmen.

2. Geschichtlicher Hintergrund¹

- **1970: Weltweit erstes Datenschutzgesetz in Hessen**

Hessen verabschiedete das weltweit erste Datenschutzgesetz, in welchem erstmals der Begriff „Datenschutz“ Verwendung fand. Der Aspekt der Datensicherheit, also dem Schutz der gespeicherten Daten vor Beeinträchtigung durch höhere Gewalt, menschliche oder technische Fehler und Missbrauch, stand eindeutig im Vordergrund. Dies lag daran, dass zu dieser Zeit staatliche Datensammlungen als besonders wertvoll und schützenswert angesehen wurden.

¹ Vgl. Witt (2008) und Speichert (2007).

- 1982: Gesetz - **Volkzählung**

Der Bundestag beschließt das Volkzählungsgesetz, welches über die üblicherweise regelmäßigen zum Beginn eines Jahrzehnts stattfindenden, als Mikrozensus durchgeführten inhaltlich begrenzten Zählungen hinausging: Aufgrund des Fortschritts in der Datenverarbeitungstechnik war es nun möglich, die Befragung als Totalerhebung durchzuführen. Diese sollte im Frühjahr 1983 geschehen.

- 1983: Urteil - **Volkzählung**

Der Bundesgerichtshof entschied am 15. Dezember 1983 (Az.: 1 BvR 209, 269, 362, 420, 440, 484/83)², nachdem er aufgrund mehrere Klagen gegen das Volkzählungsgesetz eine einstweilige Verfügung erlassen hatte, die die Durchführung bis auf weiteres untersagte, dass eine Volkzählung auf Basis einer nicht-anonymisierten Totalerhebung, wie sie damals geplant war, nicht durchgeführt werden darf. Datenschutz bzw. das informationelle Selbstbestimmungsrecht wurden durch dieses Urteil ein allgemein anerkanntes Grundrecht, welches als zu den allgemeinen Persönlichkeitsrechten gezählt wird. Es ist definiert als „Grundrecht jedes Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Kritikpunkte waren u.a. der Umfang der abgefragten Daten, der Verzicht auf anonymisierte Befragung und Datenerhebung, die Zusammenfügbarkeit der Daten zu einem umfassenden Persönlichkeitsbild oder der Weitergabe der Daten an viele verschiedene Stellen.

Prüfungsmaßstab für das Recht auf informationelle Selbstbestimmung stellt das allgemeine Persönlichkeitsrecht dar, welches sich aus der Verbindung der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) und der Menschenwürde (Art. 1 Abs. 1 GG) zusammensetzt.

Eingriffsschranken existieren für den Gesetzgeber durch die Anforderungen nach „Normenklarheit“ (es muß klar sein, auf welche Norm sich berufen wird), Verhältnismäßigkeit (der Eingriff muß tatsächlich erforderlich, geeignet und angemessen sein) und „Vorkehrungen“ (hierzu zählen z. B. Anonymisierung, Beschränkung der zu erhebenden Daten auf ein Minimum, Verwendungsbeschränkung oder Gewährleistung der Rechte der Betroffenen).

Die Volkzählung selbst wurde dann unter Berücksichtigung des Volkzählungsurteils des Bundesverfassungsgerichts schließlich 1987 durchgeführt.

² Alle unter www.bundesverfassungsgericht.de, abgefragt am 22.03.2008.

- 1990: Novellierung - **Bundesdatenschutzgesetzes (BDSG)**³

Die ursprüngliche erste Fassung des BDSG vom 27. Januar 1977 wurde, basierend auf dem Urteil des Bundesverfassungsgerichts von 1983 mit Wirkung vom 01. Juni 1991 vom neuen Bundesdatenschutzgesetz ersetzt. Trotz diverser Novellierungen besteht es aber in seinem Grundkonstrukt noch heute. Es bildet die grundlegende und umfassende Rechtsvorschrift zum Persönlichkeitsschutz auf dem Gebiet der Datenverarbeitung im öffentlichen und im nicht-öffentlichen Bereich.

- 1995: Erlass - **EU-Richtlinie zum Datenschutz**

In Deutschland wurde die Richtlinie „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“⁴ im Jahr 2001 durch die Novellierung des Bundesdatenschutzgesetzes mit Wirkung vom 23.05.2001 in nationales Recht umgesetzt. Darin waren generelle Vorgaben zum Datenschutz umzusetzen, wie auch die Regeln für die Übermittlung von personenbezogenen Daten in Drittstaaten, die nicht Mitglied der EU sind: Gemäß Art. 25 ist die Übermittlung nur dann zulässig, wenn der Drittstaat ein „angemessenes Schutzniveau“ gewährleistet. Diese Liste wird regelmäßig aktualisiert und zur Verfügung gestellt.

- 1998: Urteil - „**Großer Lauschangriff**“

Unter diesem Begriff wurde 1998 die Strafprozessordnung durch das „Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität“ um weitgehende Rechte zur akustischen Wohnraumüberwachung ergänzt. Im Urteil des Bundesverfassungsgerichts vom 3. März 2004 (AZ.: 1 BvR 2378/98)⁵ wird dieses Gesetz für teilweise verfassungswidrig erklärt, unter Bezugnahme auf die Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG. Aus diesem Urteil geht der bekannte **Kernbereich privater Lebensgestaltung** hervor. Das Gesetz wurde daraufhin modifiziert, dass der Lauschangriff eine besondere schwere Straftat betreffen muss.

Zusammenfassend schloss das Bundesverfassungsgericht den Kernbereich privater Lebensgestaltung von einer entsprechenden staatlichen Überwachung aus.

³ Quelle: Bundesdatenschutzgesetz.

⁴ Quelle: Europäische Gemeinschaften, Amtsblatt der Europäischen Gemeinschaften Nr. L 281 vom 23/11/95 S. 31.

⁵ Vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html, abgefragt am 22.03.2008.

- 1999: Urteil - **Fernmeldeüberwachung**

Im Zuge der Verabschiedung des Verbrechensbekämpfungsgesetzes von 1994 erhielt der Bundesnachrichtendienst Befugnisse zur Telekommunikationsüberwachung. Diese Befugnisse wurden vom Bundesverfassungsgericht 1999 aber als verfassungswidrig erklärt. Im sogenannten Fernmeldeüberwachungsurteil vom 14. Juli 1999 (Az.: 1 BvR 2226/94, 2420, 2437/95)⁶ stellte das Bundesverfassungsgericht fest, dass die Eingriffsintensität von der Berücksichtigung von Eintrittsschwellen abhängt, die wiederum abhängig sind von der Schutzbedürftigkeit grundlegender Verfassungsgüter und Zumutbarkeitsgrenzen nicht überschreiten dürfen.

- 2001: Urteil - **Rasterfahndung**

Im Anschluss an die terroristischen Attacken auf das World Trade Center in New York, USA wurde in Deutschland bundesweit nach sog. „Schläfern“ mittels eines maschinellen Datenabgleichs gefahndet. Das Bundesverfassungsgericht hat in seinem Beschluss vom 4. April 2006 (Az.: 1 BvR 518/02)⁷ enge Grenzen für eine Rasterfahndung im Rahmen der Strafprävention gesetzt:

„Das Grundgesetz enthält einen Auftrag zur Abwehr von Beeinträchtigungen der Grundlagen einer freiheitlichen demokratischen Ordnung unter Einhaltung der Regeln des Rechtsstaats [...]. [...] Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen. Das schließt nicht nur die Verfolgung des Zieles absoluter Sicherheit aus, welche ohnehin faktisch kaum, jedenfalls aber nur um den Preis der Aufhebung der Freiheit zu erreichen wäre. [...] Der staatliche Eingriff in den absolut geschützten Achtungsanspruch des Einzelnen auf Wahrung seiner Würde [...] ist ungeachtet des Gewichts der betroffenen Verfassungsgüter stets verboten.“

Zusammenfassend darf nur bei Vorliegen einer konkreten Gefahr in das informationelle Selbstbestimmungsrecht eingegriffen werden.

- 2005 – 2008: Urteil - **Online-Durchsuchung/Bundestrojaner/Computer-Grundrecht**

Laut Peter Altmaier, Parlamentarischen Staatssekretärs im Bundesinnenministerium erlaubte der damalige Bundesinnenminister Otto Schily dem BND per

⁶Vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rs19990714_1bvr222694.html, abgefragt am 22.03.2008.

⁷Vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404_1bvr051802.html, abgefragt am 22.03.2008.

Dienstanweisung, IT-Systeme von Verdächtigen Auszuspionieren. Öffentlich wurde diese Dienstanweisung durch den Nachfolger Schilys, Wolfgang Schäuble, der diese Variante öffentlich bewarb. Das Bundesverfassungsgericht stellte im Urteil BVerfG, 1 BvR 370/07⁸ vom 27.2.2008 fest, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch die Online-Durchsuchung betroffen sei. Dieses durch dieses Urteil neu geschaffene Recht wird auch Computer-Grundrecht genannt und wird als Ausfluss des Persönlichkeitsrechts angesehen. Der Computer zählt somit durch dieses Urteil zum Kernbereich der privaten Lebensgestaltung.

- 2006 – 2008: Urteil - **Massenabgleich von KFZ-Kennzeichen**

Ein massenhafter Abgleich von Kfz-Kennzeichen mit Fahndungslisten, wie es in mehreren Landesgesetzen erlaubt wird, ist nur unter engen Voraussetzungen zulässig. Das Bundesverfassungsgericht gab zwei Autobesitzern recht, die sich in ihren Grundrechten verletzt gesehen hatten. (Az.: 1 BvR 2074/05, 1 BvR 1254/07 vom 11.03.2008)⁹. Stichprobenartig könne die automatisierte Erfassung von Kennzeichen unter bestimmten Voraussetzungen zwar möglich sein. Ein Massenabgleich sei jedoch nur bei einer konkreten Gefahr erlaubt. Dieser Massenabgleich verletze das Recht auf informationelle Selbstbestimmung.

- 2007 bis heute: **Vorratsdatenspeicherung**¹⁰

Gemäß der „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden“¹¹ musste EU-weit bis 15.07.2007 diese Richtlinie in nationales Recht umgesetzt sein. Es war jedoch möglich, auf Erklärung den Termin bis zum 15.03.2009 zu verschieben. Dies wurde unter anderem von Deutschland in Anspruch genommen. Das Umsetzungsgesetz ist zwar nach Ausfertigung durch den Bundespräsidenten zum Jahreswechsel in Kraft

⁸ Vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html, abgefragt am 22.03.2008.

⁹ Vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html, abgefragt am 22.03.2008.

¹⁰ Vgl. Gola (2007).

¹¹ Vgl. Amtsblatt Nr. L 105 vom 13/04/2006 S. 0054 – 0063, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:DE:HTML>, abgefragt am 22.03.2008.

getreten (BGB1. I vom 31.12.2007)¹², Im Rahmen des Gesetzesentwurfs zur Neuordnung der verdeckten Ermittlungsmaßnahmen im Strafverfahren wurden diese Regelungen zur Umsetzung der Vorratsdatenspeicherung-Richtlinie getroffen), jedoch müssen die Dienstleistungsprovider (Internetzugangsanbieter, Anbieter von E-Mail-Diensten und Internettelefonieanbieter (VoIP)) die Daten der Nutzer erst ab dem 1.1.2009 für 6 Monate zwingend speichern. Dies ist in § 113 TKG geregelt. Diese Daten dürfen dann z. B. im Rahmen der Strafverfolgung genutzt werden. Am 19. März 2008 hat das Bundesverfassungsgericht dieses Gesetz zur Massenspeicherung von Telefon- und Internetverbindungsdaten per einstweilige Anordnung beschnitten. Die Unternehmen müssen die Daten zwar weiter auf Vorrat speichern, die Verwendung darf aber nur nach Zustimmung eines Ermittlungsrichters (nicht wie vorher generell Polizei und Staatsanwaltschaft) im Zusammenhang mit Strafverfahren bei schweren Straftaten (z. B. Mord, Geiselnahme oder Kinderpornographie, nicht aber bei weniger schweren Delikten) stattfinden. Zudem soll die Bundesregierung bis zum 1. September 2008 dem BVerfG über die praktischen Auswirkungen der Vorratsdatenspeicherung berichten. Die Hauptverhandlung zur Verfassungsbeschwerde ist somit nicht vor Ende 2008 zu erwarten.

3. Rechtliche Aspekte¹³

3.1. Datenschutzrechtliche Prinzipien

Im Rahmen des informationellen Selbstbestimmungsrechts lassen sich aus den oben genannten höchstrichterlichen Entscheidungen etliche Anforderungen an Datensicherheit und Datenschutzkontrolle ableiten. In Deutschland orientiert sich der Datenschutz somit an grundlegenden Prinzipien, welche bereichsübergreifend gelten.

- Subsidiaritätsprinzip

Aus der Normenklarheit ergibt sich die Anforderung, dass im Datenschutzrecht präzise und bereichsspezifische Regelungen zu treffen sind. Der entsprechende Rechtsgrundsatz „lex specialis derogat lex generalis“ findet sich daher auch in den Datenschutzgesetzen wieder. Als Beispiele dienen z. B. Rechtsvorschriften des Bundes, z. B. zur Telekommunikation oder den Telemedien, aber auch Betriebsvereinbarungen, welche dann allgemeinerrechtliche Bestimmungen verdrängen.

- Verbot mit Erlaubnisvorbehalt

¹² Quelle: Bundesministerium der Justiz, S. 3198 bis S. 3211.

¹³ Vgl. Witt (2008) und Speichert (2007).

Zunächst sind im deutschen Datenschutzrecht das Erheben, Verarbeiten oder Nutzen personenbezogener Daten verboten. Erst durch eine Einwilligung des Betroffenen oder eine gesetzliche Erlaubnis wird diese Regel außer Kraft gesetzt.

- Prinzip der Zweckbindung

Der Zweck der Erhebung ist bereits bei der Erhebung festzulegen und dem Betroffenen mitzuteilen. Dies gilt für alle Verarbeitungsschritte eines Verfahrens (bzw. Geschäftsprozesses).

- Prinzip der Transparenz

Um das informationelle Selbstbestimmungsrecht überhaupt nutzen zu können, muss ein Betroffener ihn betreffende Verfahren kennen. Jede verantwortliche Stelle hat eine Übersicht über die durchgeführten Verfahren mit personenbezogenen Daten zu erstellen (Verfahrensverzeichnis). Jeder, nicht nur die Betroffenen, hat ein Einsichtsrecht in das Verfahrensverzeichnis. Es gehört zu den Aufgaben eines bestellten Datenschutzbeauftragten, hierzu Auskunft zu erteilen. Bei erstmaliger Speicherung von personenbezogenen Daten ergibt sich eine Benachrichtigungspflicht über Art der Daten, Zweckbestimmung und Identität der verantwortlichen Quelle.

- Prinzip des Direkterhebungsvorrangs

Die Erhebung von personenbezogenen Daten soll direkt beim Betroffenen erfolgen. Meist erfolgt die Direkterhebung auf der Grundlage einer Einwilligungserklärung, welche i.d.R. schriftlich zu erfolgen hat.

- Verhältnismäßigkeitsprinzip

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darf nur dann erfolgen, wenn dies zur Aufgabenerledigung erforderlich ist. Entscheidend ist hier der konkrete Einzelfall. Grundsätzlich können alle Betroffenen davon ausgehen, dass die automatisierte Verarbeitung ihrer Daten nach dem Grundsatz von Treu und Glauben erfolgt.

- Prinzip der Datensparsamkeit

Im Vergleich zum Verhältnismäßigkeitsprinzip, in welchem es primär um Verfahren geht, werden in diesem Punkt die IT-Systeme selbst adressiert. Diese sollten die Möglichkeit erhalten, mit möglichst wenig personenbezogenen Daten zu funktionieren, unabhängig davon, ob dies auch tatsächlich erfolgt. Ein Personenbezug sollte nur dann vorgesehen sein, wenn dieses zur Aufgabenbewältigung unbedingt erforderlich ist. Daten dürfen keinesfalls auf Vorrat gespeichert werden.

3.2. Allgemeine Datenschutzregeln

Aus den vom Bundesverfassungsgericht in den oben genannten Urteilen geforderten Schutzvorkehrungen lassen sich gleichfalls allgemein gültige Regelungen ableiten, die sich in den jeweiligen Datenschutzgesetzen bzw. dem anzuwendenden Bereichsrecht zu datenschutzrechtlichen Einzelfragen wiederfinden.

3.2.1. Betroffenenrechte

Basierend auf dem Bundesverfassungsurteil von 1983 ergeben sich zwingend einige Betroffenenrechte. Die verantwortliche Stelle ist angehalten, diese Rechte zu gewähren. Aus dem Rechtsstaatsprinzip folgt, dass sich der Betroffene bei einer Datenschutzkontrollinstanz beschweren kann.

- Auskunftsrecht

Der Betroffene kann jederzeit bedingungslos erfahren, welche personenbezogenen Daten über ihn von der verantwortlichen Stelle erhoben, verarbeitet oder genutzt werden und woher die entsprechenden Daten stammen, an wen die Daten ggf. weitergeleitet werden und zu welchem Zweck die personenbezogenen Daten gespeichert werden. Hierzu muß ein formloser Antrag gestellt werden.

- Benachrichtigungsrecht

Sobald Daten ohne Kenntnis des Betroffenen erhoben bzw. erstmalig gespeichert werden, ist dieser von der Speicherung, der Zweckbestimmung und der Identität der verantwortlichen Stelle zu benachrichtigen, bei nicht-öffentlichen Stellen auch über die Art der gespeicherten Daten. Über eine erstmalige Übermittlung ist der Betroffene ebenfalls zu unterrichten.

- Berichtigungsrecht

Der Betroffene hat das Recht, Daten, die nicht oder nicht mehr den Tatsachen entsprechen, korrigieren lassen zu können.

- Lösungsrecht

Wenn personenbezogene Daten gar nicht oder nicht mehr zu speichern sind, insbesondere weil die damit verbundenen Zwecke bereits erfüllt wurden oder nicht mehr erfüllbar sind.

- Sperrungsrecht

Sofern personenbezogene Daten zwar nicht mehr aktiv benötigt werden oder vom Betroffenen ausdrücklich eine Sperranforderung etwa im Rahmen seines Widerspruchsrechts gegen Werbemaßnahmen verlangt wurde, doch die gespeicherten Daten aufgrund bestehender Aufbewahrungspflichten weiterhin vorzuhalten sind, sind diese zu sperren.

- Anrufungsrecht

Der Betroffene kann die Datenschutzkontrollinstanz auf eventuell vorhandene Mängel bei der datenschutzrechtlichen bzw. sicherheitstechnischen Umsetzung hinweisen und zwar ohne dass auf seine Identität geschlossen werden kann.

- Schadensersatzrecht

Der Betroffene kann Schadensersatz von der verantwortlichen Stelle fordern, wenn diese ihm durch eine fehlerhafte oder unzulässige automatisierte Verarbeitung einen Schaden zugefügt hat und nicht nachweisen kann, dass alle Sorgfaltspflichten eingehalten wurden.

3.2.2. Datenschutzkontrolle

- Selbstkontrolle

Die Betroffenenrechte (siehe oben) stellen die erste Säule im Datenschutzkontroll-Konzept dar.

- Eigenkontrolle

Die Eigenkontrolle obliegt der verantwortlichen Stelle und wird durch den **Datenschutzbeauftragten** durchgeführt. Dessen Bestellung hat schriftlich zu erfolgen und ist seit 2006 eine notwendige Bedingung für Unternehmen, bei welchen mindestens 10 beschäftigte Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst sein. Seine **Aufgaben** umfassen u.a. das Hinwirken auf die Einhaltung datenschutzrechtlicher Vorschriften, Überwachung der Datenverarbeitung auf datenschutzrelevante Konfliktpunkte, datenschutzrechtliche Schulung des Personals, Ansprechpartner für Betroffene, Durchführung der Vorabkontrolle bei besonders riskanten automatisierten Verarbeitungen und der aktiven Pflege des Verfahrensverzeichnis. Zu seinen **Tätigkeiten** zählt die Durchführung und Dokumentation von Vor-Ort-Kontrollen, Erstellung von Stellungnahmen zu aktuellen Datenschutzfragen, Planung und Durchführung von Mitarbeiterschulungen und Sensibilisierung spezifischer Stellen, Verpflichtung von Mitarbeitern auf das Datengeheimnis unter Durchführung entsprechender Belehrungen, Erstellung und Begutachtung von Sicherheits- und Datenschutzkonzepten, Pflege des internen Verfahrensverzeichnis, Recherchen zur aktuellen Rechtslage und Lesen und Auswerten von Fachartikeln. Anforderungen an den Datenschutzbeauftragten sind z. B. Fachkunde, Zuverlässigkeit. Unterstützt wird er im Rahmen der Eigenkontrolle durch die interne Revision, den IT-Sicherheitsbeauftragten und die Mitarbeitervertretung.

- Fremdkontrolle

Die Fremdkontrolle wird durch die **Aufsichtsbehörden** wahrgenommen. Zu ihnen zählen die Landesdatenschutzbeauftragten und der Bundesdatenschutzbeauftragte. Ebenfalls zählt das noch nicht per Gesetz ausdefinierte **Datenschutzaudit**¹⁴ dazu.

3.2.3. Datensicherheit

Die Datensicherheit selbst wird durch die Forderung nach technischen und organisatorischen Maßnahmen mit Leben gefüllt. Diese werden seit 2001 auch die „8 Gebote der Datensicherung“ genannt. Per Definition sind dies „Maßnahmen zur Erhaltung und Sicherung des Datenverarbeitungssystems, der Daten und Datenträger vor höherer Gewalt, Fehler und Missbrauch. Sie sind von der verantwortlichen Stelle auszuwählen, zu planen, umzusetzen und zu kontrollieren. Einzelne Maßnahmen sollten im Rahmen des Risikomanagements bewertet werden.

Die „8 Gebote“ lauten:

- Zutrittskontrolle
(Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren, also z. B. zu Serverräumen und Gebäuden)
- Zugangskontrolle
(Die Nutzung von Datenverarbeitungsanlagen durch Unbefugte ist zu verhindern, dient also dem Schutz des jeweiligen IT-Systems, z. B. vor Angriffen)
- Zugriffskontrolle
(Nur mit Zugriffsberechtigung dürfen Berechtigte auf IT-Systeme zugreifen, dies betrifft z. B. Anwendungen und Applikationen)
- Weitergabekontrolle
(Während des Transports dürfen personenbezogene Daten nicht unbefugt gelesen, verändert, kopiert, gesperrt oder gelöscht werden, dies betrifft in erster Linie den Schutz des Netzwerks)
- Eingabekontrolle
(Nachträglich muss überprüfbar und feststellbar sein, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind. Hier spielt vor allem die Zurechenbarkeit eine Rolle, z. B. durch Protokollierungsvorschriften)
- Auftragskontrolle
(Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden im Rahmen der Rechtsverbindlichkeit)

¹⁴ Vgl. Bitkom (2007) und Roßnagel (1999).

- Verfügbarkeitskontrolle
(Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen im Rahmen der Ausfallsicherheit)
- Datentrennungskontrolle
(Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden)
- Zusätzlich noch sinnvoll: Organisationskontrolle¹⁵
(die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.)

3.2.4. Regeln für Outsourcing und Konzerne

Im Rahmen des Outsourcings (und auch innerhalb von Konzernen, wo eigenständige Teilbereiche kein Konzernprivileg genießen) ist zu unterscheiden, ob eine Auftragsdatenverarbeitung vorliegt oder eine Funktionsübertragung.

Bei der **Auftragsdatenverarbeitung**, welche eine schriftliche Vereinbarung zwingend voraussetzt, aus welcher die Eignung des Auftragnehmers aus Datenschutzsicht ersichtlich ist, ist die Aufgabe so klar beschrieben, dass der Auftragnehmer keine grundlegenden Entscheidungen zum Inhalt der Aufgabenerledigung selbst treffen kann. Der Auftraggeber hat volles Weisungsrecht. Die Tätigkeit des Auftragnehmers fällt unter den Begriff des „Nutzens“ der personenbezogenen Daten. Der Auftraggeber bleibt in diesem Fall die verantwortliche Stelle.

Der Auftraggeber hat sicherzustellen, dass beim Auftragnehmer ein mindestens gleich hohes Datenschutzniveau vorherrscht (z. B. verbindliche Aktionen wie durch Verpflichtung der tätig werdenden Mitarbeiter auf das Datengeheimnis, zur Einhaltung der Weisungen des Auftraggebers und zur Ergreifung ausreichender technischer und organisatorischer Maßnahmen). Ein Untervertragsverhältnis zur Erledigung von Teilaufgaben bedarf notwendigerweise der Zustimmung des Auftraggebers.

Bei der **Funktionsübertragung** (z. B. Bewerbungsmanagement, Personalentwicklungsmanagement, Outplacement, Forderungseinzug, Kundendatenanalyse oder unreglementierte Outbound-Telefonie) liegt eine hinreichend eigenständige Aufgabe vor, welche eine eigenverantwortliche Tätigkeit des Auftragnehmers darstellt. Der Auftragnehmer wird in diesem Fall zur verantwortlichen Stelle, der Auftraggeber hat kein Weisungsrecht. Der Betroffene muß deshalb in diesem Rahmen eine Mitteilung über die Übermittlung seiner Daten erhalten. Der Auftragnehmer hat in diesem Fall eigenständig die nötigen Maßnahmen zur Gewährleistung des Datenschutzes zu ergreifen. Die Einordnung dieser Variante

¹⁵ Vgl. Ulmer (2008), S. 15-20.

erfolgt datenschutzrechtlich als Übermittlung personenbezogener Daten.

3.2.5. Umgang mit besonders riskanten Verfahren

Sobald besonders schützenswerte personenbezogene Daten oder Daten, die der Leistungs- oder Verhaltenskontrolle dienen, automatisiert verarbeitet werden, liegt ein besonders riskantes Verfahren vor. Auch wenn neue, noch nicht hinsichtlich der Technikfolgen abschätzbare IT- oder Kommunikationstechnik eingesetzt wird, trifft dies zu. Dann muss von der verantwortlichen Stelle eine Vorabkontrolle durchgeführt werden. Hier wird in erster Linie die Rechtmäßigkeit der geplanten automatisierten Verarbeitung überprüft. Zielsetzung der Vorabkontrolle ist es, das nach deren Abschluss im Sinne des Datenschutz-Risikomanagements keine besonderen Risiken verbleiben. Die Nichtdurchführung einer Vorabkontrolle ist als Missachtung der „im Verkehr erforderlichen Sorgfalt“ (nach § 276 Abs. 2 BGB) zu beurteilen und berechtigt zur Einforderung eines Schadensersatzes.

3.3. Regelungen zum Mediendatenschutz

Im Rahmen des Mediendatenschutzes spielen vor allem elektronische Kommunikationsmedien (Web, E-Mail, VoIP etc.) eine große Rolle. Im Schichtenmodell existieren drei Ebenen. Die Zugehörigkeit eines Dienstes zu einer der drei Schichten bestimmt, welche Rechtsnorm greift. Der Schichtenaufbau orientiert sich am technischen ISO-/OSI-Schichtenmodell. Jede Kommunikation durchläuft alle drei Schichten.

Schicht 1 ist die Inhalts-Schicht, dort greifen die jeweiligen Bestimmungen der Datenschutzgesetze oder Spezialrecht.

Schicht 2 ist die Dienst-Schicht, hier ist maßgeblich, welche Art von Kommunikation genutzt wird. Es greifen das Telemediengesetz (Web, E-Mail) bzw. das Telekommunikationsgesetz, welches durch Spezialvorschriften des Fernmeldegeheimnis im TKG ergänzt werden (VoIP (schwierige Zuordnung) und klassische Telefonie).

Schicht 3 ist die Transfer-Schicht (auch Netz- oder Netzwerk-Schicht), hier greift das Telekommunikationsgesetz. Hier ist der Transport von Signalen angesiedelt.

Der **Grad der Datenschutzrelevanz** hängt ganz entscheidend davon ab, inwieweit die Privatnutzung solcher Dienste erlaubt ist. Wenn dies nicht der Fall ist, greifen z. B. die Spezialvorschriften des Fernmeldegeheimnisses im TKG.

Terminvereinbarungen bei Ärzten, Kontakt zu öffentlichen Stellen oder Terminverschiebungen aufgrund von Überstunden sind als dienstlich zu betrachten. Wenn bei E-Mail die Privatnutzung verboten ist, kann die verantwortliche Stelle bei

langer Krankheit z. B. die Geschäfts-E-Mails einsehen. Im Intranet greift kein Fernmeldegeheimnis.

4. Auszug aus dem Bundesdatenschutzgesetz (BDSG)¹⁶

- § 1 Abs. 1 BDSG „**Datenschutz**“

„Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten.“

Die reine Existenz eines Datensatzes erzeugt an sich noch keine Datenschutzrelevanz, erst die formale Beschreibung der Daten stellt diese her. Prüfungsmaßstab ist das allgemeine Persönlichkeitsrecht, das sich aus der Verbindung der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) und der Menschenwürde (Art. 1 Abs. 1 GG) zusammensetzt.

- § 3 Abs. 1 BDSG „**Personenbezogene Daten**“

„Daten über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“

„Bestimmt“ meint, dass Daten einer Person direkt zugeordnet werden können, „bestimmbar“, dass Daten durch Ausnutzung von Zusatzinformationen einer Person zugeordnet werden können (z. B. eine IP-Adresse).

„Persönliche Verhältnisse“ sind üblicherweise Identifikationsdaten (wie z. B. Name oder Ausweisnummer), Gesundheitsdaten (wie z. B. Biometrische Daten), Sozialbezugsdaten (wie z. B. Familienstand oder Beruf) und Zeiterfassungsdaten (z. B. Arbeitszeiten). „Sachliche Verhältnisse“ sind z. B. Daten über Einkommens- und Vermögensverhältnisse, Versicherungsdaten oder Daten über Kundenprofile. Im deutschen Recht, anders als in anderen Rechtssystemen, auch innerhalb der EU, kann nur eine natürliche Person betroffen sein. Entscheidend ist also, ob eine zuordenbare Person unmittelbar von der Erhebung, Verarbeitung oder Nutzung seiner Daten betroffen ist.

- § 3 Abs. 7 BDSG „**Verantwortliche Stelle**“

„Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“

Verantwortliche Stelle muss „Herrin über die Daten“ sein.

„Erheben, verarbeiten und nutzen“ werden im Datenschutzrecht unter dem Begriff „**automatisierte Verarbeitung**“ zusammengefasst.

¹⁶ Vgl. Bundesdatenschutzgesetz, <http://www.gesetze-im-internet.de/bdsg1990>, abgefragt am 22.03.2008 und Gola (2007).

- § 3 Abs. 3 BDSG „**Erheben**“

„Beschaffen von Daten über den Betroffenen“

- § 3 Abs. 4 BDSG „**Verarbeiten**“

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

- § 3 Abs. 5 BDSG „**Nutzen**“

„Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt, also z. B. Kenntnisnahme, Auswertung, Auskunftserteilung an Betroffene oder Datentransfer zwischen verantwortlicher Stelle und weisungsgebundenem Auftraggeber.

- § 33 – 35 BDSG „**Rechte des Betroffenen**“

„Der Betroffene hat ein Recht auf Benachrichtigung, Auskunft und die Berechtigung, die Löschung oder Sperrung von seinen personenbezogenen Daten zu verlangen.“

- § 7 BDSG „**Schadensersatz**“

„Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.“

- § 43 Abs. 3 „**Bußgeldvorschriften**“

„Die Ordnungswidrigkeit kann [...] mit einer Geldbuße bis zu zweihundertfünfzigtausend Euro geahndet werden.

Literatur- und Quellenverzeichnis

Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2007): Entwurf eines BundesdatenschutzauditG. Stand 07.09.2007.

Bundesministerium der Justiz (2007): Bundesgesetzblatt, Teil 1 Nr. 70 vom 31.12.2007, Bundesanzeigerverlag.

Bundesministerium der Justiz: Bundesdatenschutzgesetz, http://www.gesetze-im-internet.de/bdsg_1990/, abgefragt am 22.03.2008.

Bundesverfassungsgericht: Entscheidungssammlung des Bundesverfassungsgerichts online, <http://www.bundesverfassungsgericht.de>, abgefragt am 22.03.2008.

Europäische Gemeinschaften (2007): Amtsblatt der Europäischen Gemeinschaften Nr. L 281 vom 23/11/95.

Gola, P. und R. Schomerus und C. Klug (2007): Bundesdatenschutzgesetz (BDSG). Kommentar (Gelbe Kommentare), Beck Juristischer Verlag.

Roßnagel, A. (1999): Datenschutzaudit. Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit. Rechtsgutachten für das Bundesministerium für Wirtschaft und Technologie, <http://www.mydatenschutz-audit.de/datenschutz-audit.htm>, abgefragt am 22.03.2008.

Speichert, H. (2007): Praxis des IT-Rechts. Praktische Rechtsfragen der Internetnutzung und IT-Sicherheit (Zielorientiertes Business Computing), Vieweg.

Ulmer, C.-D. (2008): Das Datenschutz-Management im Unternehmen und der Wertbeitrag der Datenschutzorganisation, Recht der Datenverarbeitung. Zeitschrift für Datenschutz-, Informations- und Kommunikationsheft, Datakontext.

Witt, B. (2008): Datenschutz kompakt und verständlich. Eine praxisorientierte Einführung, Vieweg.