Bundesministerium für
Ernährung, Landwirtschaft
und Verbraucherschutz

# Erhöhung des Datenschutzniveaus zugunsten der Verbraucher


*Studie im Auftrag des BMELV*

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein


Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

# Erhöhung des Datenschutzniveaus zugunsten der Verbraucher

Projektnummer: 04HS052

Studie im Auftrag des
Bundesministeriums für Verbraucherschutz,
Ernährung und Landwirtschaft

Schlussbericht April 2006

Studie

# „Erhöhung des Datenschutzniveaus zugunsten der Verbraucher“

Projektnummer: 04HS052 - Schlussbericht April 2006

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Holstenstr. 98, 24103 Kiel

Tel.: 0431 988 1200

Fax: 0431 988 1223

http://www.datenschutzzentrum.de/

Die Studie wurde verfasst durch:

Dr. Johann Bizer

Meike Kamp

Kirsten Bock

Barbara Körffer

Kai Janneck

Nils Leopold

Jan Möller

Martin Rost

Umschlaggestaltung: Markus Hansen

ISBN 978-3-00-021082-2

# Inhaltsverzeichnis

## Abbildungsverzeichnis:

## Tabellenverzeichnis:

# Abstract – Zusammenfassung

**Verbraucherdatenschutzrecht**

Gegenstand des Verbraucherdatenschutzes ist die Gewährleistung der informationellen Selbstbestimmung von Konsumenten bzw. Privatkunden gegenüber Unternehmen. Gleichzeitig stärkt der Verbraucherdatenschutz die wirtschaftliche und rechtsgeschäftliche Handlungsfreiheit der Verbraucher.

Gemäß dem generellen Verbot mit Erlaubnisvorbehalt des § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten, sofern die Verwendung nicht entweder durch eine Rechtsvorschrift des BDSG bzw. eines anderen Gesetzes oder durch die Einwilligung des Betroffenen erlaubt ist. Fehlt es an Spezialvorschriften für die Verarbeitung von Verbraucherdaten, richtet sich die Verwendung nach den allgemeinen gesetzlichen Verarbeitungsbefugnissen der §§ 28 – 30 BDSG.

Von wesentlicher Bedeutung ist, für welchen Zweck die Verarbeitung vorgenommen wird. Der Zweck ist von der verantwortlichen Stelle bereits bei der Erhebung der Daten festzulegen. Dies ist relativ einfach bei einer Datenverwendung zur Erfüllung eines zwischen Verbraucher und Unternehmer geschlossenen Vertragsverhältnisses. Die Bildung umfassender Kundenprofile ist nur zulässig, wenn der Betroffene in diese Verarbeitung eingewilligt hat. Dasselbe gilt für die Verwendung von über die Daten Name, Anschrift und Geburtsjahr hinausgehenden Informationen im Rahmen von Kundenbindungssystemen.

Die Einwilligung als Legitimationsgrundlage einer Datenverarbeitung entspricht der Ausübung der informationellen Selbstbestimmung des Verbrauchers. In der Praxis gewinnt sie häufig nur dort Bedeutung, wo die beabsichtigen Verarbeitungen nicht mehr von den §§ 28 – 30 BDSG gerechtfertigt werden können. Die Einwilligung entfaltet eine Ausschlusswirkung gegenüber den gesetzlichen Verarbeitungstatbeständen: Wenn die Daten verarbeitende Stelle sich entscheidet, eine bestimmte Datenverarbeitung von der Einwilligung des Verbrauchers abhängig zu machen und der Verbraucher die Einwilligung verweigert, dann kann die Datenverarbeitung nicht mehr auf gesetzlicher Grundlage durchgeführt werden.

Die Einwilligung ist nur wirksam, wenn sie den Anforderungen des § 4a BDSG genügt, d.h. insbesondere freiwillig und schriftlich erfolgt. Wird die Einwilligung in Form einer vorformulierten Klausel eines Formularvertrages eingeholt, unterliegt sie der besonderen Kontrolle der Vorschriften zu den Allgemeinen Geschäftsbedingungen (AGB) nach §§ 305 ff. BGB. Im Rahmen dieser Kontrolle sind auch die wesentlichen Grundgedanken des BDSG zu beachten, so dass die Einbeziehung der schutzwürdigen Interessen des Betroffenen sowie die Erforderlichkeit der Datenverarbeitung als Grundprinzipien des BDSG in der vorformulierten Einwilligungserklärung berücksichtigt werden müssen.

Grundlegendes Prinzip des Verbraucherdatenschutzes ist die Transparenz der Datenverarbeitung. Die Daten verarbeitenden Stellen haben nach dem Datenschutzrecht eine Reihe von Unterrichtungs- bzw. Benachrichtigungspflichten umzusetzen. Zu unterscheiden ist die

Informationspflicht vor Erteilung einer Einwilligung, die Unterrichtung bei einer Datenerhebung mit Kenntnis des Betroffenen und die nachträgliche Benachrichtigung, wenn die Daten ohne Kenntnis des Betroffenen gespeichert wurden. Besondere technikspezifische Informationspflichten sieht das Gesetz vor, wenn aufgrund der Erhebungstechnik, z.B. bei technisch unterstützten heimlichen Erhebungsverfahren wie etwa einer Videobeobachtung, für die Verbraucher spezielle Gefahren für das informationelle Selbstbestimmungsrecht bestehen. Beim Einsatz von RFID ergeben sich zentrale Risiken, wenn in den Hintergrundsystemen der Betreiber Verbraucherprofile gebildet und ausgewertet werden können, ohne dass der Verbraucher das Auslesen des RFID Chips faktisch zu Kenntnis nehmen kann. Wesentlich für den Schutz der Verbraucher ist die Pflicht der Daten verarbeitenden Stelle, den Betroffenen über sein Widerspruchsrecht gegen die Verwendung der Kundendaten zu Werbezwecken zu informieren. Während die Informationspflichten eindeutig formuliert sind, fehlen für ihre konkrete Gestaltung präzise Vorgaben.

Zu den Transparenzregelungen gehören auch die datenschutzspezifischen Auskunfts-, Löschungs-, Berichtigungs-, Sperrungsansprüche und Widerspruchsrechte, mit denen sich der Verbraucher auf eigene Initiative Kenntnis von der Verwendung seiner Daten verschaffen oder dieser widersprechen kann.

**Empirische Untersuchung**

In mehreren empirischen Untersuchungen wurden Kenntnis und Praxis der Datenschutzrechte durch die Verbraucher untersucht. In welchem Umfang die Verbraucher ihre Datenschutzrechte kennen und diese auch wahrnehmen, wurde mit Hilfe einer repräsentativen Telefonbefragung von Verbrauchern sowie schriftlichen Befragungen betrieblicher Datenschutzbeauftragter, von Verbraucherberaterinnen und -beratern sowie von Experten der Aufsichtsbehörden untersucht. Die Verbraucher sind über die Informationspflichten der Unternehmen und über ihre Auskunfts- bzw. Widerspruchsrechte im Kern relativ gut informiert, nehmen aber ihre Rechte nur in geringem Maße wahr. Die Verbraucherberaterinnen und -berater sowie die aufsichtsbehördlichen Experten schätzen die Kenntnisse der Verbraucher im datenschutzrechtlichen Bereich als eher niedrig ein.

Die geringe Wahrnehmung der Datenschutzrechte ist nach Interpretation der Verfasser auf ein gewisses Systemvertrauen der Verbraucher zurückzuführen, das durch die mangelnde Transparenz der tatsächlichen Verwendungsbedingungen aufrechterhalten wird. Die Verbraucher stufen ihr persönliches Risiko aus der Verarbeitung ihrer Daten als eher gering ein. Bedeutung für diese individuelle Risikobewertung hat aber weniger das Wissen über die eigenen Rechte als die Kenntnis der tatsächlichen Verarbeitungsbedingungen. Art und Umfang der Datenflüsse und operativen Verwendungen sind den Verbrauchern eher unbekannt. Sie müssen daher darauf vertrauen, dass die Verarbeitung ihrer Daten in ihrem Interesse erfolgt. Solange dieses Grundvertrauen besteht, fehlt ein hinreichender Grund, eigene Datenschutzrechte wahrzunehmen.

**Defizite des Verbraucherdatenschutzes**

Im dritten Teil der vorgelegten Studie werden die Defizite im Verbraucherdatenschutz analysiert. Nach Ansicht der Verfasser bestehen bei den Rechtsgrundlagen der Datenverarbeitung, beim Gesetzesvollzug und bei den Sanktionsmöglichkeiten von Datenschutzverstößen Mängel. Zwar beruhen die Mängel im Verbraucherdatenschutz nicht so sehr auf Schutzlücken des geltenden Datenschutzrechtes, sondern mehr auf der fehlenden Einhaltung des Rechtes sowie auf Unzulänglichkeiten im internen Datenschutzmanagement. Es werden allerdings Defizite der gesetzlichen Ausgestaltung der Benachrichtigungspflicht sowie beim Auskunftsanspruch des Betroffenen festgestellt. Zudem ist das Vollzugsdefizit auf die Komplexität der an Abwägungsklauseln reichen Datenschutzregelungen zurückzuführen. Ein weiteres Problem stellen die unzureichenden Sanktionsmöglichkeiten von Datenschutzverstößen dar. Insbesondere Bußgeldbewehrungen mit einer präventiven Wirkung sind rar. Das geltende Datenschutzrecht und die Datenschutzpolitik sind nicht auf die Herausforderungen einer allgegenwärtigen vernetzten Totalerfassung eingestellt. Die Verfasser teilen die im Gutachten von Roßnagel/Pfitzmann/Garstka vertretene Auffassung von der mangelnden Technikadäquanz des Datenschutzrechtes.

**Handlungsempfehlungen**

Die Defizite im Verbraucherdatenschutz lassen sich auf drei Ebenen beseitigen: zum einen durch eine Schärfung der materiellen Anforderungen (z.B. präzisere Regelung der Verwendungszwecke, Stärkung der Rechte der Verbraucher und Verschärfung der Transparenzpflichten gewerblich tätiger Übermittlungsdienstleister) an den Datenschutz, zum zweiten durch eine Verbesserung der Maßnahmen der Aufsicht und Kontrolle (z.B. Stärkung des internen Datenschutzmanagements, höhere Bestimmtheit und Erweiterung der Bußgeldtatbestände) und schließlich durch Maßnahmen des proaktiven Datenschutzes (Beratung der Unternehmen, Datenschutz durch Technik, Etablierung des Datenschutzes als Wettbewerbskriterium).

Die Effizienz der staatlichen Datenschutzaufsicht ist zu verbessern. Als geeignete Maßnahmen kommen die Förderung und Schulung der Mitarbeiter im juristischen, technischen, wirtschaftlichen und kommunikativen Bereich, die Verbesserung der Abstimmungsprozesse zwischen den Aufsichtsbehörden z.B. durch ein Mehrheitsprinzip im Düsseldorfer Kreis sowie Maßnahmen zur verbesserten Wahrnehmung der Aufsichtsbehörden durch die Öffentlichkeit in Betracht.

Die als defizitär identifizierte Durchsetzung datenschutzrechtlicher Informationspflichten muss neben datenschutzrechtlichen Sanktionen auch mit zivil- bzw. wettbewerbsrechtlichen Klagemöglichkeiten flankiert werden. Die Verletzung datenschutzrechtlicher Informationspflichten sollte mit Hilfe von Unterlassungsklagen gegen Allgemeine Geschäftsbedingungen sowie im Wege wettbewerbsrechtlicher Klagen geahndet werden können. Maßnahmen der freiwilligen Zertifizierung wie Datenschutzaudit oder Gütesiegel tragen als Wettbewerbsfaktoren zur Einhaltung des Datenschutzes in der Wirtschaft und zu mehr Transparenz für die Verbraucher bei.

# Abstract – Summary

**Consumer Data Protection Law**

Consumer data protection efforts aim at strengthening the consumer's constitutional right to "informational self-determination"/privacy in their (mostly contractual) relationships with the business world. As an effect, the legal and economic status of consumers is being strengthened, too.

The collection, processing and use of personal data shall be lawful only if this Act or another legal provision permits or prescribes them or if the data subject has consented. In cases where sector-specific legislation for consumer data protection has not been adopted the general processing rules of section 28 - 30 BDSG (Federal Data Protection Act - BDSG) apply.

It is of major importance as for what purpose (personalized) consumer data are being processed. The purpose has to be specified clearly before the data are being collected. If the All necessary personal data are solely being used for the purpose of fulfilling a specific contractual relationship between consumer and companies the processing does not pose particular data protection problems. Excessive profiling practices can only be legitimate, if the data subject has given her/his free and unambiguous consent to the processing. The Consent of the consumer is also needed to use personal data in customer relationship management systems, as far as the data being processed do not disclose information beyond the name, address and year of birth of the data subject.

The data subject's consent as the legal basis for processing of personal data serves the interests of the consumers right to self-determination. In practice the data subject's consent will only become relevant where the legal grounds for processing under sections 28 - 30 of the BDSG do not apply. However, once the data processor has chosen to gain the consent of the consumers and this consent is being rejected, it cannot be argued that the missing legal justification should be substituted by the provisions of section 28 - 30 BDSG.

The consent of the consumer will only be valid once the prerequisites of section 4 a of the BDSG are being met. It has to be given free (of external pressure) an be stated unambiguously. Once the consent is part of standardized terms of conditions they have to meet the legal prerequisites of section 305 et.seq. of the German civil code (Bürgerliches Gesetzbuch - BGB). These provisions open up for a broader judicial control as to whether the terms of conditions meet the basic principles of the BDSG. Thus the data subject's legitimate interests and the necessity principle have to be taken into account when obtaining consent via general standardized terms of conditions.

The most fundamental principle of consumer data protection is the transparency principle. Data protection laws provide for a number of duties to inform consumers on their data being processed. Three different types of provisions can be identified: firstly there are duties to inform in advance before consent is being obtained, secondly there are duties to inform on the occasion of the collection of data from the data subject and thirdly there are notification duties where personal data have been processed without the data subject knowing about it. Particular duties to inform have been established for the use of certain information technolo-

gies which bear specific risks like covert/hidden surveillance such as camera surveillance (section 6b BDSG). The use of RFID chips typically bears the risk of hidden profiling by analyzing the content of the chips without the data subject acknowledging. It is of particular importance for the consumers to be informed by the data processor on their right to object to the processing of their data for marketing purposes. While the data processors obligations to inform have received a rather clear legal regulation there is no comparable legal standard for the right to object especially in terms of how these obligations have to be carried out.

The transparency principle encompasses the data subject's rights of access, rectification, erasure, blocking or objection to their data being processed and thus allow for the consumer to gain knowledge on his own initiative.

**Empirical Studies**

The consumers´ knowledge of their privacy rights and the practice of asserting their privacy rights were analyzed in different empirical studies. Consumers were interviewed via telephone in a representative survey as well as data protection officials of companies, consumer advisors and the experts of supervisory authorities were surveyed in a questionnaire to assess to what extent the consumers know about their privacy rights and assert those rights. The consumers have a relatively good knowledge about the obligations of the companies to inform and about their rights of objection; they assert their rights to only a minor degree. The consumer advisors and the experts of the supervisory authorities rank the knowledge of the consumers in the field of privacy as rather low.

In the authors´ interpretation the consumers have a certain trust in the system and therefore assert their rights to a very low degree. The inscrutability of the concrete operations and processing of data perpetuates the consumers´ trust. The consumers estimate their personal risk through the processing of their personal data as low. Relevant for this individual risk evaluation is rather the knowledge of the concrete conditions of the processing than the consumers´ knowledge of their privacy rights. Ways and extent of delivering as well as the functional processing of their personal data are inscrutable to the consumer. They have to have trust, that the processing of their personal data are coherent to their own interests. As long as the consumers trust, there is no reason for them to assert their privacy rights.

**Deficiencies of Consumer Data Protection**

In the third part of the study deficiencies of consumer data protection are analysed. In the authors' opinion deficits exist regarding the legal basis of data processing, the enforcement of laws and the possibility for sanctions of data protection offences. The deficiencies are not mainly accounted for by protection gaps in existing data protection laws but by a missing compliance with the laws and by deficiencies in the internal data protection management. Moreover deficiencies in the legal structure of the data subject's right to information and the right to access were detected. The enforcement deficit owes its existence to the complexity of the applicable data protection regulations which i.e. originates from many balancing of interests clauses. Another problem is the deficient possibilities to sanction breaches of privacy. Especially administrative fines with a preventive effect are scarce.

The existing data protection law and data protection policies are not prepared to the challenges of ubiquitous and comprehensive data collections in a networked world. The authors share the opinion presented in the legal opinion of Roßnagel/Pfitzmann/Garstka of a deficient technical adequacy of data protection laws.

**Recommendations for Action**

The deficiencies in consumer data protection can be eliminated on three levels: On the one hand by sharpening the material requirements of data protection (i.e. more precise definitions of processing purposes in provisions, strengthening of consumer rights and stricter transparency rules for commercial transfer service providers), on the other hand by improving measures of supervision and controls (i.e. strengthening of internal data protection management, better determination and expansion of administrative fines) and finally by measures of pro-active data protection (consulting of companies, data protection by technological means, establishing data protection as a competitive advantage).

The efficiency of supervising authorities should be improved. Adequate measures could be the encouragement and training of employees in the fields of law, technology, economy and communication, improvements of coordination processes between supervising authorities, i.e. by a majority principle in the Duesseldorfer Kreis as well as measures for a better perception of supervising authorities in public.

The enforcement of the data subject's right to information which is considered deficient should be supported by sanctions in the data protection field as well as the facility for civil and competitive law actions in courts. The violation of the right of information in data protection laws should be enforceable with actions for injunction against standard terms and competitive law actions for injunction.

Measures of a voluntary certification like data protection audits or privacy seals as competitive factors can support the compliance of businesses with data protection requirements and can lead to more transparency for the consumer.

# 1 Rechtslage für die Verwendung von Verbraucherdaten

## 1.1 Verfassungsrechtliche Ausgangslage

Mit dem Volkszählungsurteil[1] aus dem Jahre 1983 hat das BVerfG das Grundrecht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) anerkannt. Danach soll der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten entscheiden und vor der unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe geschützt sein.[2]

Als individuelles Abwehrrecht gegen staatliche Eingriffe steht das Grundrecht auf informationelle Selbstbestimmung unter dem Vorbehalt des Gesetzes, d.h. Eingriffe des Staates sind nur durch Gesetz oder auf der Grundlage eines „normenklaren und bestimmten" Gesetzes zulässig, das den Verwendungszweck der erhobenen Daten bereichsspezifisch regelt, den Anforderungen des Verhältnismäßigkeitsgrundsatzes genügt sowie verfahrensrechtliche Vorkehrungen zum Schutz der informationellen Selbstbestimmung enthält.[3]

Daneben entfaltet das Grundrecht aber auch eine objektiv-rechtliche Bedeutung.[4] Eine verfassungsrechtliche Grundlegung findet sich bereits im Volkszählungsurteil, wonach eine „Rechtsordnung" mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar wäre, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".[5] Die objektiv-rechtliche Bedeutung begründet die Verantwortung des Gesetzgebers für ein Schutzkonzept, um eine ausreichende Entfaltung der informationellen Selbstbestimmung zu gewährleisten. In seiner objektiv-rechtlichen Bedeutung wirkt die informationelle Selbstbestimmung auch auf das Rechtsverhältnis zwischen Privaten. Es ist von dem Gesetzgeber bei der Ausgestaltung der Rechtsordnung, bei der Rechtsanwendung sowie von der Rechtsprechung zu beachten.[6]

---

1 BVerfGE 65, 1ff.

2 BVerfGE 65, 1, 45. n

3 BVerfGE 65, 1, 45 ff. st. Rspr.

4 Vgl. Bizer in: Schulte, Handbuch des Technikrechts 2003, S. 569 ff.; Unter Verfassungsrechtlern wird diese objektiv-rechtliche Bedeutungsschicht zunehmend als Ausgangspunkt für die Gestaltung einer umfassenden Informations- und Kommunikationsordnung gewählt. Vgl. bspw. Trute, Der Schutz personenbezogener Daten in der Informationsgesellschaft, JZ 1998, 825. Hoffmann-Riem, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), 513, 524 ff.

5 BVerfGE 65, 1, 43. Die Formulierung geht auf Podlech zurück, siehe in: AK-GG, Art. 2 Abs. 1, Rn. 45, Fn. 66.

6 BVerfGE 84, 192, 194 – Entmündigung. Eine fehlerhafte Würdigung durch ein Gericht verletzt den Betroffenen darüber hinaus als Hoheitsakt in seinem Grundrecht auf informationelle Selbstbestimmung. Siehe auch BVerfG, DuD 2002, 568, 569 – Abtretung.

Eine andere Begründungslinie arbeitet den Zusammenhang des informationellen Selbstbestimmungsrechts mit der ebenfalls durch Art. 2 Abs. 1 GG geschützten Willenserklärungsfreiheit des Einzelnen heraus. Unter der Voraussetzung rechtlicher Gleichordnung der Privaten werden die Verfügungsmöglichkeiten des Anderen über die personenbezogenen Daten des Betroffenen durch die seiner Willenserklärung inhärente Zweckbindung über die Verwendung seiner Daten beschränkt:[7] Eine von dem Betroffenen nicht konsentierte Verwendung personenbezogener Daten erfolgt folglich ohne rechtlichen Grund und ist damit rechtswidrig. Der Gesetzgeber kann für derartige informatorische Eingriffe Privater eine rechtliche Legitimationsgrundlage durch Gesetz schaffen, was er mit den §§ 28 ff. BDSG auch getan hat. Von Bedeutung ist vor allem die Erkenntnis, dass der Betroffene über das Rechtsverhältnis Zwecke für die Verarbeitung seiner Daten festlegt, die den Partner in seinen Verwendungsmöglichkeiten dieser Daten binden und auf den Willen des Betroffenen beschränken.

Der Staat ist darüber hinaus verfassungsrechtlich verpflichtet, im Fall erheblich ungleicher Verhandlungspositionen auch innerhalb eines bestehenden Vertragsverhältnisses zu verhindern, dass sich die Selbstbestimmung des einen Vertragspartners in eine Fremdbestimmung verkehrt.[8] In einer erst kürzlich ergangenen Entscheidung leitet das Bundesverfassungsgericht aus der von Art. 2 Abs. 1 GG geschützten Privatautonomie einen „Maßstab des gebotenen Ausgleichs zwischen strukturell ungleichen Verhandlungssituationen“ ab.[9] Dieser Maßstab ist gleichzeitig auch die „Brücke“ zwischen der informationellen Selbstbestimmung einerseits und der Willenserklärungsfreiheit andererseits. In beiden Fällen hat der Staat von Verfassungswegen, die Entscheidungs- und Handlungsfähigkeit des Einzelnen – hier über seine Daten, dort sich rechtsgeschäftlich zu betätigen – zu gewährleisten. Ein unmittelbarer Zusammenhang besteht, sobald sich die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten auf diese Entscheidungs- und Handlungsfähigkeit auszuwirken und damit Fremdbestimmung droht. Im Begriff des *Verbraucherdatenschutzes* ist der Zusammenhang zwischen rechtsgeschäftlicher Handlungsfähigkeit und informationeller Selbstbestimmung prägnant auf den Punkt gebracht. In beiden Fällen geht es um den Schutz und die Förderung der individuellen Selbstbestimmung.

Die Situation des Verbrauchers ist maßgeblich dadurch bestimmt, dass er als Einzelperson gegenüber einem Unternehmen als Geschäftspartner eine weitaus schwächere Position zur Durchsetzung seiner vertraglichen Interessen hat. Diesem Ungleichgewicht tragen die Regelungen des Verbraucherschutzes in vielen Bereichen Rechnung. Durch spezielle Rechte bspw. der Information soll die Selbstbestimmung des Verbrauches ermöglicht und unterstützt werden, um ein Gleichgewicht der Kräfte zwischen Unternehmen und Verbrauchern zu gewährleisten. Informationell kann dieses Gleichgewicht gestört sein, wenn Unternehmen personenbezogene Daten über Verhalten, Einstellungen, Interessen und Lebensbedingungen

---

7 Bizer, DuD 1998, 558, Ausführlicher Bizer, Forschungsfreiheit und informationelle Selbstbestimmung 1992, S. 300; Roßnagel/Garstka/Pfitzmann, S. 52.

8 BVerfGE 81, 242, 254 – Handelsvertreter; 89, 214, 332 – Bürgschaft; 103, 89, 100 f. – Ehevertrag.

9 BVerfG, Beschluss vom 06.12.2005, Az.: 1 BvR 1905/02. Bislang nur im Internet unter www.bundesverfassungsgericht.de veröffentlicht.

von Verbrauchern sammeln, auswerten und nutzen können, um deren rechtsgeschäftliche Entscheidungen zu beeinflussen. Gestört wäre das informationelle Gleichgewicht zwischen Unternehmen und Verbrauchern ferner, wenn die Tatsache einer Verarbeitung ihrer Daten, die Verantwortlichkeit, die Art der Daten, ihre konkreten Zwecke sowie etwaige Empfänger für den Betroffenen intransparent sind. Es ist Aufgabe des Datenschutzes, für ein informationelles Gleichgewicht zwischen Unternehmen und Verbrauchern Sorge zu tragen.

## 1.2 Generelles Verbot mit Erlaubnisvorbehalt

Dem Schutz der informationellen Selbstbestimmung im Privatrechtsverkehr dient das BDSG. Es legt in § 1 BDSG als Gesetzeszweck fest, der Einzelne solle davor geschützt werden, durch den Umgang (Dritter) mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt zu werden. Unter personenbezogenen Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zu verstehen (§ 3 Abs.1 BDSG). Für das Erheben, Verarbeiten oder Nutzen personenbezogener Daten des einzelnen Verbrauchers (als natürlicher Person) ist der Anwendungsbereich des BDSG folglich immer eröffnet – jedenfalls soweit es sich um eine automatisierte Erhebung, Verarbeitung oder Nutzung seiner Daten handelt oder die Daten aus einer solchen Verarbeitung stammen.

Grundlegendes Konstruktionsprinzip des deutschen Datenschutzrechts ist der datenschutzrechtliche Vorbehalt des Gesetzes in § 4 Abs. 1 BDSG.[10]

Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten, sofern die Verwendung nicht entweder durch eine Rechtsvorschrift des BDSG bzw. eines anderen Gesetzes oder durch die Einwilligung des Betroffenen erlaubt ist. § 4 Abs. 1 BDSG schafft damit ein generelles Verbot der Verwendung personenbezogener Daten mit Erlaubnisvorbehalt. Diese grundsätzliche Wertung des Gesetzgebers beim Umgang mit personenbezogenen Daten muss bei der Anwendung und Auslegung des BDSG Berücksichtigung finden. Insofern sind auch die in §§ 28-30 BDSG normierten gesetzlichen Verwendungsbefugnisse für nichtöffentliche Stellen als Ausnahmen zum grundsätzlichen Verwendungsverbot zu behandeln und entsprechend restriktiv auszulegen.

## 1.3 Erhebung, Verarbeitung und Nutzung nach § 28 BDSG

Soweit andere Rechtsvorschriften des Bundes eine bereichsspezifische Regelung für den Umgang mit personenbezogenen Daten treffen, gehen diese den Vorschriften des BDSG nach § 1 Abs. 3 BDSG vor. Bestehen keine derartigen Spezialvorschriften ist eine Verwendung grundsätzlich unter den Voraussetzungen der §§ 28-30 BDSG möglich. Normadressat ist die verantwortliche Stelle, d.h. nach § 3 Abs. 7 BDSG jede Stelle oder Person, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Nach. § 27 Abs. 1 BDSG gelten die Verwendungsbefugnisse der

[10] Bizer in: Schulte, S. 571.

§ 28 ff. BDSG nur für nichtöffentliche Stellen (§ 2 Abs. 4 BDSG) bzw. gleichgestellte öffentliche Stellen als verantwortliche Stellen.

Die Erlaubnisnormen im nichtöffentlichen Bereich unterscheiden sich danach, ob die Datenverwendung für eigene Geschäftszwecke (§ 28), d.h. zur Erreichung eines internen Geschäftszwecks, oder zum Zweck der Übermittlung an Dritte, d.h. zur Verarbeitung von Daten für Dritte, erfolgt (§§ 29, 30).[11] Die Regelungen weisen in den tatbestandlichen Voraussetzungen große Ähnlichkeiten, in einigen Punkten aber auch bedeutsame Unterschiede auf. Im Vordergrund stehen hier die Anforderungen des § 28 BDSG, weil dieser mit dem Vertragsverhältnis zwischen einer verantwortlichen Stelle und einem Betroffenen strukturell die Datenverarbeitung gegenüber einem Verbraucher abbildet. Die Definition des Verbrauchers in § 13 BGB setzt ein solches Vertragsverhältnis begriffsnotwendig voraus, so dass § 28 BDSG für die Unternehmer-Verbraucher-Beziehung den Ausgangspunkt bildet.

Auch die Datenverarbeitung nach § 29 BDSG ist für den Verbraucher von erheblicher Bedeutung, denn außerhalb von Vertragsbeziehungen[12] ist sie die Rechtsgrundlage für eine geschäftsmäßige Verarbeitung „für Zwecke der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient“. Die Vorschrift regelt mit anderen Worten die geschäftsmäßige Datenverarbeitung „auf Vorrat und zum Zweck der Weitergabe“.[13] Sie ist damit Rechtsgrundlage für eine Verarbeitung von personenbezogenen Daten, die anderen Stellen bspw. zur Vorbereitung von Vertragsabschlüssen dienen können. Unternehmen beziehen bspw. Informationen über Verbraucher aus dem Adresshandel sowie von Auskunfteien, um sie nach Umsatzerwartung und Bonität bewerten zu können.[14] Aus der Sicht informationeller Selbstbestimmung sind diese Verarbeitungen in hohem Maße problematisch, weil sie personenbezogene Datensammlungen über Verbraucher legitimieren, um bspw. für Zwecke der Werbung Einfluss auf ihr Kaufverhalten zu nehmen. Scoringverfahren und Bonitätsdateien sind darüber hinaus in der Lage, die wirtschaftliche Handlungs- und Entscheidungsfreiheit der Betroffenen erheblich einzuschränken, ohne dass dem betroffenen Verbraucher die Daten selbst, ihre Quellen, ihre inhaltliche Korrektheit sowie die Maßstäbe ihrer Bewertung erkennbar sind. Die Anforderungen und Voraussetzungen derartiger Verfahren hat das ULD in seinem Bericht über Scoringverfahren näher erläutert, auf den zur Vermeidung von Wiederholungen insoweit verwiesen wird.[15]

§ 30 BDSG regelt die Datenerhebung und –verarbeitung der Markt- und Meinungsforschungsinstitute, die Daten personenbezogen erheben, sie aber in der Regel nur anonym an Dritte weitergeben bzw. veröffentlichen.

---

[11] Tinnefeld/Ehmann/Gerling, S. 539.

[12] Schaffland/Wiltfang, BDSG § 28, Rn. 11; Mallmann in: Simitis, BDSG, § 29, Rn. 1.

[13] So Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 5.

[14] Vgl. bspw. zusammenfassend Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5; Breinlinger in: ders., Kap. 7.5.

[15] ULD, Scoringsysteme zur Beurteilung der Kreditwürdigkeit 2005.

### 1.3.1 Zum Zwecke der Erfüllung des Verbrauchervertrages

Dreh- und Angelpunkt für die erlaubte Verwendung personenbezogener Daten auf gesetzlicher Grundlage ist der mit der Verwendung verfolgte Zweck (§ 28 Abs. 1 Satz 1 Nr. BDSG). Dieser Verwendungszweck ist bereits bei der Erhebung personenbezogener Daten konkret festzulegen (§ 28 Abs. 1 Satz 2 BDSG).

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die beabsichtigte Verwendung von personenbezogenen Daten nur dann zulässig, wenn sie der Zweckbestimmung des Vertrages oder eines vertragsähnlichen Vertrauensverhältnisses „dient“. Das Erheben, Verarbeiten oder Nutzen von Verbraucherdaten muss also entweder selbst Vertragsinhalt oder für die Vertragserfüllung bzw. -durchführung erforderlich sein. Entscheidend ist nicht, ob die Verwendung den subjektiven Zielen des einen Vertragspartners entgegenkommt, sondern es kommt vielmehr auf den objektiv feststellbaren, von allen Vertragspartnern gebilligten Vertragszweck und die davon abhängige Vertragsabwicklung an.[16] Ausschlaggebend ist mit anderen Worten der konkrete Vertragszweck im Einzelfall, was allerdings gewisse generalisierende Typisierungen nicht ausschließt.

So ist in der Regel die Angabe und Verarbeitung von Namen und Adresse des Verbrauchers erforderlich, um den Verbrauchervertrag überhaupt erfüllen zu können. So z.B. immer dann, wenn der Verbraucher die gekaufte Ware nicht sofort erhält, sondern diese erst bestellt wird, an den Verbraucher versandt werden muss und dann bezahlt werden soll. Name und Anschrift des Verbrauchers können bspw. erforderlich sein, um ihn über den Eingang der bestellten Ware zu informieren oder ihm die bestellte Ware auf seinen Wunsch hin zu übersenden. Auch zur Abwicklung zahlreicher Dauerschuldverhältnisse wie z.B. die Bereitstellung von Telekommunikationsdienstleistungen (Telefon, Internet, Kabel etc.) ist die Adresse des Verbrauchers erforderlich, um ihm die Abrechnung der Leistung zukommen zu lassen.

Hingegen ist die Angabe bspw. des Geburtsdatums des Verbrauchers als Vertragnehmer in einer Vielzahl von Fällen eine für die Vertragsabwicklung überflüssige Information. Dennoch wird sie häufig formularmäßig vom Verbraucher verlangt. Die Angabe des Geburtsdatums in Verbraucherverträgen ist nur in wenigen Fällen eine für die Erfüllung des Vertragszweckes notwendige Information: Eine Fallgruppe ist, wenn die Kenntnis des Alters des Verbrauchers für den Vertragsabschluss rechtlich von Bedeutung und nicht anderweitig feststellbar ist (z.B. bei Internet- oder Telefonbestellungen). So kann es aus Gründen des Jugendschutzes oder zur Feststellung der Geschäftsfähigkeit für den Unternehmer notwendig sein, das Geburtsdatum abzufragen. Eine weitere Fallgruppe bilden die Fälle, in denen der Gesetzgeber die Unternehmer gesetzlich zur Erhebung der persönlichen Identifizierungsdaten ihrer Kunden und Verbraucher verpflichtet hat, um seinerseits das Verhalten des Verbrauchers oder des Unternehmers überwachen zu können. Ein Beispiel ist die Identifizierung des Kunden vor der Eröffnung eines Bankkontos bzw. bei bestimmten Geldverkehren nach Abgabenordnung und Geldwäschegesetz (§ 154 AO, § 1 Abs. 5 GwG). Ein anderes Beispiel ist die gesetzliche

[16] Simitis in: Simitis, BDSG, § 28, Rn. 80.

Verpflichtung der Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit, bei der Vergabe von Rufnummern oder der Bereitstellung von TK-Anschlüssen nicht nur Name und Anschrift des Vertragspartners, sondern auch deren Geburtsdatum zu erheben (§ 111 Abs. 1 TKG). Auch hier ist die Angabe des Geburtsdatums nicht zur Vertragserfüllung erforderlich, sondern ist von den Unternehmen aus Gründen der inneren Sicherheit zu erheben, um den Sicherheitsbehörden auf deren Verlangen Auskunft über die Identität von Anschlussinhabern geben zu können.

Die Datenerhebung, -verarbeitung oder -nutzung kann auch zulässig sein, wenn sie der Zweckbestimmung eines *vertragsähnlichen* Vertrauensverhältnisses dient. Ein solches entsteht in jedem Fall vor Abschluss des Vertrages durch die Aufnahme von Vertragsverhandlungen.[17] In diesem Stadium treffen die Parteien zwar noch keine Verpflichtungen aus dem Vertrag, es bestehen aber bereits beiderseitige Sorgfaltspflichten, die im Interesse des Verhandlungspartners beachtet werden müssen.[18] Es handelt sich um eine Verpflichtung zur Rücksichtnahme auf Rechtsgüter und Interessen des Vertragspartners,[19] wie sie auch in § 241 Abs. 2 BGB statuiert ist. Für die Bestimmung derartiger Sorgfaltspflichten wird § 311 Abs. 2 Nr. 1 – 3 BGB, der die Geltung der Pflichten aus § 241 Abs. 2 BGB auf den vorvertraglichen Bereich erstreckt, als Orientierungsrahmen herangezogen.[20] Danach bestehen Sorgfaltspflichten nicht allein bei der Aufnahme von Vertragsverhandlungen, sondern auch schon bei der Anbahnung eines Vertrages, bei welcher der eine Teil in Hinblick auf eine etwaige rechtsgeschäftliche Beziehung dem anderen Teil die Möglichkeit zur Einwirkung auf seine Rechte, Rechtsgüter und Interessen gewährt oder ihm diese anvertraut.

Für die Zulässigkeit der Datenverwendung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist es nicht erforderlich, dass die Parteien letztendlich den Vertrag auch tatsächlich abschließen. Entscheidend ist, dass sie mit dem Vertragsschluss rechnen und diesen anstreben. Werden lediglich von einer Seite Informationen z.B. in Form einer Akquisition von Interessentendaten zusammengestellt, um Chancen bzw. Zweckmäßigkeit einer vertraglichen Beziehung zu prüfen, so kann die Datenverarbeitung nicht auf den Tatbestand eines vertragsähnlichen Vertrauensverhältnisses als Rechtsgrundlage gestützt werden.[21] Ein derartiges Informationsinteresse ist lediglich einseitig und nicht durch gegenseitige Pflichten zur Rücksichtnahme gedeckt.

Ein vertragsähnliches Vertrauensverhältnis kann auch nach Beendigung eines Vertrages weiter bestehen, wenn Rechte und Pflichten nachwirken, d.h. die Verpflichtung, z.B. in Form einer Akquisition von Interessentendaten, aufeinander Rücksicht zu nehmen.[22]

---

17 Simitis in: Simitis, BDSG, § 28, Rn. 121.

18 Schaffland/Wiltfang, BDSG § 28, Rn. 67.

19 Gola/Schomerus, BDSG § 28, Rn. 26.

20 Bergmann/Möhrle/Herb, BDSG § 28, Rn. 93 unter Hinweis auf zivilrechtliche Institut der culpa in contrahendo.

21 Simitis in: Simitis, BDSG, § 28, Rn. 122.

22 Gola/Schomerus, BDSG § 28, Rn. 26; Simitis in: Simitis, BDSG, § 28, Rn. 123.

### 1.3.2 Außerhalb des Zweckes des Verbrauchervertrages

Sollen personenbezogene Daten außerhalb der Zweckbestimmung eines Vertrages bzw. vertragsähnlichen Vertrauensverhältnisses verwendet werden, so hängt ihre Zulässigkeit von einer Interessenabwägung mit den schutzwürdigen Interessen des Betroffenen ab.

#### 1.3.2.1 Verwendung durch das Unternehmen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Die Verwendung von personenbezogenen Daten außerhalb eines Vertragszweckes, aber zu einem bei der Erhebung festgelegten eigenen Geschäftszweck ist zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle bzw. des Unternehmers erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Das berechtigte Interesse des Unternehmens muss nicht rechtlicher Natur sein, sondern kann auch in einem ideellen oder wirtschaftlichen Interesse liegen, solange es sich um ein von der Rechtsordnung gebilligtes Interesse handelt.[23] Zu beachten gilt allerdings die grundsätzliche Wertung und Zweckrichtung des BDSG. § 28 BDSG ist eng auszulegen und soll nicht zum Auffangtatbestand für beliebige Datenverarbeitung und -nutzung umfunktioniert werden.[24] Insofern bleiben auch bei der Anwendung des Tatbestandes des § 28 Abs. 1 Satz 1 Nr. 2 BDSG die konkreten Vertragsbeziehungen der maßgebliche Anknüpfungspunkt für die Auslegung des „berechtigten Interesses“ einer verantwortlichen Stelle bzw. in Verbraucherbeziehungen des Unternehmers. In jedem Fall müssen die Interessen des Unternehmens mit der konkret geplanten Verwendung zusammenhängen und sich auf Daten beziehen, die zu diesem Zweck verwendet werden.[25] Es muss sich um Belange des konkreten Unternehmens und nicht nur um branchentypische Interessen handeln.[26] Beispiele für die Annahme eines solchen berechtigten Interesses sind Marktanalysen unter der Verwendung eigener Kundendaten zur Vorbereitung konkreter Werbeaktionen.[27] Hierbei ist allerdings zu beachten, dass der Gesetzgeber die Möglichkeiten einer direkten Werbung gegenüber Verbrauchern durch § 7 UWG eingeschränkt hat. Eine Auswertung von Verbraucherdaten zur Vorbereitung einer konkreten Werbemaßnahme ist insbesondere dann nicht „berechtigt“, wenn die beabsichtigte Ansprache auch nach der Wertung des § 7 UWG eine unzumutbare Belästigung darstellt.[28]

---

[23] Gola/Schomerus, BDSG § 28 Rdnr.33; Schaffland/Wiltfang, BDSG § 28, Rn. 85; BGHZ 91, 233, 240.

[24] Simitis in: Simitis, BDSG, § 28, Rn. 133/134; Auernhammer, BDSG 90 § 28, Rn. 17.

[25] Simitis in: Simitis, BDSG, § 28, Rn. 137.

[26] Simitis in: Simitis, BDSG, § 28, Rn. 140, 146.

[27] Vgl. Simitis in: Simitis, BDSG, § 28, Rn. 137.

[28] Breinlinger in: Roßnagel, HdBDatSchR, Kap. 7.6, Rn. 44 f.s.a. Buss, RDV 2005, 260.

Die Anwendung dieser Regelung erfährt eine Restriktion dadurch, dass nach § 28 Abs. 1 Satz 2 BDSG die Zwecke, für die die personenbezogenen Daten verarbeitet oder genutzt werden sollen, bereits bei der Erhebung „konkret" festzulegen sind. Nach § 4 Abs. 1 Satz 1 Nr. 2 BDSG ist der betroffene Verbraucher über diese Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung seiner Daten zu informieren, wenn die Daten bei ihm als dem Betroffenen erhoben werden. Sinn und Zweck dieser Regelungen ist es, dass das Unternehmen seine beabsichtigten Verwendungszwecke gegenüber dem betroffenen Verbraucher bereits bei der Erhebung offen legt. In der Diskussion ist lediglich, ob die bei der Erhebung festgelegte (primäre) Zweckbindung eine spätere (sekundäre) Zweckänderung auf der Grundlage des § 28 Abs. 2 BDSG sperrt.[29] Im Ergebnis wird dies regelmäßig der Fall sein, weil die informationelle Selbstbestimmung die Entscheidung und das Wissen über die Verwendung der eigenen Daten schützen soll. Aus diesem Grund überwiegen schutzwürdige Belange des Betroffenen regelmäßig, wenn er über die Änderung des ihm gegenüber kommunizierten Verwendungszweckes im Unklaren gelassen wird.[30]

Ein weiteres wichtiges Regulativ ist die Anforderung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, dass die Verwendung der personenbezogenen Verbraucherdaten zur Wahrung berechtigter Interessen *erforderlich* sein muss. Nach dem Erforderlichkeitsgrundsatz ist die Erhebung, Verarbeitung oder Nutzung nur gerechtfertigt, wenn keine anderen Mittel zur Verfügung stehen, die ohne oder mit geringerer Verwendung von Kundendaten auskommen und gleichwohl die berechtigten Interessen des Unternehmens wahren würden. Dies wäre bspw. der Fall, wenn das berechtigte Interesse des Unternehmers an einer Verarbeitung der personenbezogenen Daten auch mit anonymisierten Daten erfüllt werden könnte. An der Erforderlichkeit einer Erhebung fehlt es im Übrigen auch, wenn das Unternehmen die Daten der betroffenen Verbraucher auch mit ihrer Mitwirkung und Zustimmung bekommen könnte.[31]

Darüber hinaus darf kein Grund zur Annahme bestehen, dass das *schutzwürdige Interesse* des Verbrauchers an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Wann ein schutzwürdiges Interesse des Betroffenen vorliegt, ist unter Berücksichtigung des Schutzzweckes des BDSG, d.h. des Schutzes vor Beeinträchtigungen des Persönlichkeitsrechtes des betroffenen Verbrauchers, unter Berücksichtigung der verfassungsrechtlichen Wertung des informationellen Selbstbestimmungsrechts zu ermitteln.[32] So liegt es bspw. im schutzwürdigen Interesse des Betroffenen, über die Verwendung seiner Daten grundsätzlich selbst zu entscheiden oder zumindest über die konkrete Verwendung informiert zu werden.

Inwieweit das Persönlichkeitsrecht beeinträchtigt ist und das schutzwürdige Interesse des Betroffenen das berechtigte Interesse der verantwortlichen Stelle überwiegt, hängt vom konkreten Einzelfall ab. Für die *Abwägung* im Einzelfall spielen insbesondere die Verarbeitungs-

---

[29] Für eine Sperrwirkung Simitis in: Simitis, BDSG, § 28, Rn. 61, 205; a.A. Gola/Schomerus, § 28, Rn. 49.

[30] Vgl. auch Brühann in: Grabitz/Hilf, A 30, Art. 10, Rn. 13, der eine Information über die spätere Zweckänderung für erforderlich hält.

[31] Simitis in: Simitis, BDSG, § 28, Rn. 144.

[32] Gola/Schomerus, BDSG § 28, Rn. 35; Bergmann/Möhrle/Herb, BDSG § 28, Rn. 110.

zwecke, die Art der Daten und die Intensität ihrer Verwendung wie bspw. die Speicherdauer sowie die Folgen der Verwendung eine gewichtige Rolle.[33] Die Darlegungslasten hat der Gesetzgeber der Daten verarbeitenden Stelle auferlegt. Dies ergibt sich aus der Formulierung des Gesetzes, wonach eine Verarbeitung nur dann zulässig ist, wenn „kein Grund zu der Annahme besteht", dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Das überwiegende schutzwürdige Interesse des Betroffenen muss also – was häufig übersehen wird – gegenüber dem berechtigten Interesse des Unternehmers positiv ausgeschlossen werden. Bestehen Zweifel, ob die schutzwürdigen Interessen des Betroffenen nicht doch das berechtigte Interesse überwiegen, muss von der geplanten Verarbeitung Abstand genommen werden.[34]

In Umsetzung des Art. 8 der EG-Datenschutzrichtline[35] bestimmt das BDSG in § 3 Abs. 9 BDSG besonders *sensitive Daten* als besondere Arten personenbezogener Daten. Diesen Daten kommt ein erhöhtes Schutzbedürfnis zu, da sie aufgrund ihrer Aussagekraft einen besonders tiefen Einblick in die Intimsphäre des Betroffenen zulassen bzw. die Preisgabe der Daten das Potential hat, den Einzelnen in weitaus schwerwiegenderem Maße zu beeinträchtigen. Solche Angaben sind z.B. Gesundheitsdaten, religiöse Daten, politische Daten, Daten rassischer und ethnischer Herkunft etc. Beabsichtigt ein Unternehmen besondere Arten personenbezogener Daten zu verarbeiten, so hat allein die sensitive Natur dieser Daten zur Folge, dass die schutzwürdigen Interessen des Verbrauchers im Rahmen der Abwägung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG grundsätzlich überwiegen. Der Gesetzgeber hat insofern die klare Entscheidung getroffen, dass sensitive Daten nur unter den besonderen Voraussetzungen des § 28 Abs. 6 bis 9 BDSG verwendet werden dürfen.

#### 1.3.2.2 Sonderfall der Übermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Die Darstellung im vorherigen Abschnitt konzentrierte sich auf die Verwendung von Verbraucherdaten durch den vertragsschließenden Unternehmer selbst. § 28 Abs. 1 Satz 1 Nr. 2 BDSG ermöglicht aber auch die *„Übermittlung" an Dritte* – vorausgesetzt sie sind als Mittel zur Erfüllung eigener Geschäftszwecke erforderlich und es besteht kein Grund zur Annahme, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung das berechtigte Interesse der verantwortlichen Stelle überwiegt.

Eine Übermittlung von Daten des Betroffenen ist grundsätzlich immer Risiko erhöhend für die Ausübung der informationellen Selbstbestimmung, weil mit jeder Weitergabe der Verwendungskontext der Vertragsbeziehung verlassen wird und der Kreis derjenigen wächst, der Informationen über sein Verhalten als Verbraucher erfährt und verwenden kann. Das BDSG versucht diesen Verlust an informationeller Bestimmung über die eigenen Daten

---

[33] Simitis in: Simitis, BDSG, § 28, Rn. 163, 166.

[34] Siehe auch Simitis in: Simitis, BDSG, § 28, Rn. 166.

[35] 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.

durch Unterrichtungs- und Benachrichtigungspflichten der Stellen auszugleichen, die Daten des Verbrauchers übermitteln bzw. erhalten.[36] Diese Regelungen sind jedoch häufig nur eine unzureichende Kompensation, weil der Betroffene zur Wahrung seiner informationellen Selbstbestimmung nun seinen Daten „hinterherlaufen" muss, um die Ketten ihrer Weitgabe und Verwendung konkret aufzuklären. Immerhin unterliegen die personenbezogenen Daten nach § 28 Abs. 5 Satz 1 BDSG bei dem Empfänger einer Zweckbindung. Danach dürfen diese nur zu dem Zweck verarbeitet werden, zu dem sie übermittelt wurden. Satz 2 dieser Vorschrift relativiert diese Zweckbindung aber und eröffnet den Empfängern die Möglichkeit, die empfangenen Daten für andere Zwecke zu verwenden, ohne dass der Betroffene eine Möglichkeit hat, dies vorher zu erfahren oder unterbinden zu können. Der Gesetzgeber hat also gerade keine „Sackgassenregelung" getroffen, sondern den Empfängern die Möglichkeit für weitere Übermittlungsketten eingeräumt.[37]

Eine Übermittlung von Verbraucherdaten an Dritte für deren *Marktforschungs- und Werbezwecke* kann sich nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG stützen, weil in diesem Fall mit den Daten kein eigener Geschäftszweck, sondern der eines Dritten erfüllt werden würde. Unterstellt, ein Unternehmer würde neben dem Abschluss und der Erfüllung von Verbraucherverträgen auch den Geschäftszweck verfolgen, diese für *Werbe- bzw. Marktforschungszwecke* an Dritte zu übermitteln, dann fehlt es regelmäßig an seinem das schutzwürdige Interesse des Betroffenen überwiegenden berechtigten Interesse. Die Grenze verläuft mit den Worten des Nestors des Datenschutzrechtes Spiros Simitis dort, wo sich die Daten des Betroffenen „verselbständigen und in eine eigene, frei verwertbare Ware verwandeln".[38] Ausgeschlossen ist damit auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG bspw. eine Vermietung von Kundenadressen an so genannte „Lettershops", die unter Nutzung eigener und fremder Adressdaten Werbesendungen gezielt an Kunden versenden.[39] Eine Übermittlung von Verbraucherdaten für Zwecke der Werbung und Marktforschung ist damit lediglich nur unter den Voraussetzungen des § 28 Abs. 3 Satz 1 Nr. 3 BDSG zulässig (siehe sogleich S. 28).[40]

Eine andere Fallgruppe der Übermittlung von Verbraucherdaten nach § 28 Abs. 2 Satz 1 Nr. 2 BDSG umfasst Meldungen an die Anbieter von *Warndateien* oder *Kreditauskunfteien*. Solche Systeme werden im Allgemeinen im gegenseitigen Interesse der Wirtschaftsunternehmen betrieben, d.h. die Meldungen des Verbrauchers an den Betreiber einer solchen Warn- oder Auskunftsdatei erfolgt nicht nur zum Schutz des eigenen geschäftlichen Interesses, sondern auch damit andere Unternehmen vor Verbrauchern mit hohem Kreditrisiko ge-

---

[36] Siehe näher unten Kap. 3 (S. 45).

[37] Kritisch bereits Bizer, Informationelle Selbstbestimmung 1992, S. 218 unter Hinweis auf Bull/Dammann, DöV 1981, 221.

[38] Simitis in: Simitis, BDSG, § 28, Rn. 175.

[39] Simitis in: Simitis, § 28, Rn. 175. Soweit es sich nicht im eine Auftragsdatenverarbeitung nach § 11 BDSG handelt, ist § 29 BDSG zu prüfen, vgl. Gola/Schomerus, BDSG, § 29, Rn. 18.

[40] Vgl. Gola/Schomerus, BDSG, § 28, Rn. 50.

warnt werden.[41] Im ersten Fall richtet sich die Rechtsgrundlage nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, weil mit der Meldung ein eigenes Geschäftsinteresse verfolgt wird. Würde die Meldung ausschließlich im Interesse anderer Unternehmen erfolgen, dann wäre § 28 Abs. 3 Nr. 1 BDSG die Rechtsgrundlage der weiteren Verarbeitung. Da jedoch für das Unternehmen im Regelfall das eigene Geschäftsinteresse im Vordergrund steht, weil es sich in erster Linie selbst über den Kunden informieren will, muss die Meldung die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG erfüllen.

Für die datenschutzrechtliche Zulässigkeit solcher Meldungen wird in Anlehnung an die SCHUFA-Rechtsprechung des Bundesgerichtshofes (BGH)[42] nach *„Positiv-„ und „Negativmerkmalen“* unterschieden (s.u. S. 43). Unter Positivmerkmalen werden Informationen über die Aufnahme und die vertragsgemäße Abwicklung einer Geschäftsbeziehung verstanden. Hingegen sind Negativmerkmale die Informationen über ein nicht-vertragsgemäßes Verhalten. Zur Übermittlung von Positivmerkmalen an eine Warndatei oder Kreditauskunft bedarf es immer einer Einwilligung des Betroffenen, denn das schutzwürdige Interesse des Betroffenen überwiegt, wenn er sich vertragsgemäß verhalten hat.

Für *Negativmerkmale* wird zwischen so genannten „harten“ und „weichen“ differenziert. Harte Negativmerkmale sind Informationen, die unter staatlicher Beteiligung und dies meint regelmäßig auch in einem rechtsstaatlichen Verfahren entstanden sind. Hierzu gehören rechtskräftige Urteile, die Abgabe einer eidesstattlichen Versicherung, die Zwangsvollstreckung in das Vermögen sowie die Eröffnung eines Insolvenzverfahrens. Die Übermittlung dieser Daten wird regelmäßig gebilligt, weil die Belange der Wirtschaft in diesen Fällen das schutzwürdige Interesse der Betroffenen überwiegen. Im Regelfall ohne Einwilligung des Betroffenen unzulässig ist die Übermittlung so genannter weicher Negativmerkmale. Sie beruhen auf einseitigen Maßnahmen des Gläubigers wie bspw. Mahnungen, Klageerhebung oder den Antrag auf einen Mahnbescheid, ohne dass die Forderung unstreitig geschweige denn als gerichtlich bewiesen gelten kann. Soweit keine Einwilligung des Betroffenen vorliegt, dürfen sie nur auf der Grundlage einer Abwägung im Einzelfall übermittelt werden.

#### 1.3.2.3 Verwendung von Daten nach § 28 Abs. 2, Abs. 3 BDSG

Die §§ 28 Abs. 2, Abs. 3 stellen Zulässigkeitsanforderungen für die Fälle auf, in denen das Unternehmen Daten zu einem bestimmten Zweck erhoben, gespeichert oder genutzt hat und sie dann zu einem *anderen* Zweck nutzen bzw. *übermitteln* möchte. Die Tatsache, dass die Daten ursprünglich rechtmäßig erhoben, gespeichert bzw. genutzt wurden, legitimiert datenschutzrechtlich noch nicht jede weitere Verwendung durch die verantwortliche Stelle. Jede Zweckänderung erfordert eine erneute Rechtmäßigkeitskontrolle nach den Maßstäben der §§ 28 Abs. 2, Abs. 3 BDSG. In dieser Regelung kommt der Grundsatz der Zweckbindung[43] zum Ausdruck. Personenbezogene Daten müssen grundsätzlich zweckgebunden verwendet

---

41 Näher Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 28 ff.

42 BGH NJW 1984, 436 ff, 1889 ff.; siehe auch Tinnefeld/Ehmann/Gerling, S. 326 f.

43 BVerfGE 65, 1, 45.

werden, d.h. der Verwendungszweck muss im Vorhinein feststehen[44] und die Daten dürfen z.B. nicht auf Vorrat zu unbestimmten, noch nicht feststehenden Zwecken gesammelt werden.[45]

Der § 28 Abs. 2 BDSG verweist auf § 28 Abs. 1 Satz 1 Nr. 2, 3 BDSG, so dass eine Verwendung zu einem geänderten Zweck von einer Interessenabwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und des betroffenen Verbrauchers abhängig ist. Bei der Abwägung ist nunmehr der neue Verwendungszweck zu berücksichtigen. § 28 Abs. 1 Satz 1 Nr. 3 BDSG lässt eine Verwendung zu, wenn die Daten entweder aus allgemein zugänglichen Quellen stammen oder die verantwortliche Stelle sie veröffentlichen durfte. Die Verwendung zu anderen Zwecken ist unzulässig, wenn das schutzwürdige Interesse des Betroffenen das berechtigte Interesse der verantwortlichen Stelle offensichtlich überwiegt. Dies ist regelmäßig der Fall, wenn Kundendaten an Dritte für deren Werbezwecke übermittelt werden sollen.[46]

Nach § 28 Abs. 3 BDSG ist die Übermittlung und Nutzung auch dann zulässig, wenn sie zur Wahrung berechtigter Interessen Dritter oder zur Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist (Nr. 1, 2), sowie nach dem so genannten *Listenprivileg* für Zwecke der Werbung und der Markt- und Meinungsforschung (Nr. 3). Auch in diesen Fällen ist eine Verwendung nur dann gerechtfertigt, wenn kein schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Übermittlung oder Nutzung überwiegt. Unter den spezifischen Anforderungen des § 28 Abs. 3 Satz 1 Nr. 4 BDSG ist die Übermittlung oder Nutzung zur Durchführung wissenschaftlicher Forschung auch ohne Interessenabwägung rechtmäßig.

Für den Bereich der Verarbeitung von Verbraucherdaten ist insbesondere die Verwendungsbefugnis zu Werbe-, Markt- und Meinungsforschungszwecken, d.h. die Tatbestandsalternative des § 28 Abs. 3 Satz 1 Nr. 3 BDSG relevant. Danach ist es dem Unternehmen erlaubt, genau bestimmte und abschließend festgelegte Daten von Verbrauchern, die zu einer bestimmten Personengruppe gehören, *in Listen* oder anders zusammengefasst für Werbezwecke zu übermitteln oder zu nutzen. Die Vorschrift wird daher auch als Listenprivileg bezeichnet. Zu den zulässigen Angaben einer solchen Liste zählen z.B. der Name, die Gruppenzugehörigkeit, die Adresse, sowie das Geburtsjahr. Für die Gruppenzugehörigkeit kommt z.B. die Angabe in Betracht, dass der Verbraucher Kunde eines bestimmten Unternehmens ist oder an einer bestimmten Informationsveranstaltung teilgenommen hat. Unzulässig ist es hingegen, wenn nicht nur eine Eigenschaft die Gruppenzugehörigkeit ausmacht, sondern die verantwortliche Stelle die Verbraucherdaten mehrere Eigenschaften einer Person z.B. als „zahlungsfähige Kunden des Unternehmens X“ zusammenfasst.[47] Die Personengruppe darf nach dem eindeutigen Wortlaut des Gesetzes nur durch ein einziges Merkmal bestimmt sein. Ansonsten wäre der abschließende Katalog des § 28 Abs. 3 Satz 1 Nr. 3 BDSG überflüssig,

---

[44] Vgl. auch § 28 Abs. 1 Satz 2 BDSG.

[45] Simitis in: Simitis, BDSG, § 28, Rn. 36; Tinnefeld/Ehmann/Gerling, Datenschutzrecht, S.150.

[46] Simitis in: Simitis, BDSG, § 28, Rn. 218.

[47] Gola/Schomerus, BDSG § 28, Rn. 56.

denn die Gruppenzugehörigkeit könnte unbegrenzt mit allerlei Informationen aufgestockt werden, die gerade nicht unter das Listenprivileg fallen.[48]

Die Übermittlung oder Nutzung anderer als der in § 28 Abs. 3 Satz 1 Nr. 3 BDSG aufgeführten Daten ist nur zulässig, wenn sie durch einen anderen Erlaubnistatbestand des § 28 BDSG gerechtfertigt ist.[49] Auch ist § 28 Abs. 3 Satz 1 Nr. 3 BDSG dann nicht mehr anwendbar, wenn sich aus der Art der Zusammenstellung der zulässigen Angabe weitere Erkenntnisse über die Personen ergeben (sozusagen mittelbare Informationen), die nach den gesetzlichen Merkmalen der Liste nicht enthalten sein dürften.[50] In diesem Fall besteht ein überwiegendes schutzwürdiges Interesse des Betroffenen, denn der Informationsgehalt geht über das hinaus, was der Gesetzgeber mit dem Listenprivileg offensichtlich zulassen wollte.[51] Dies ist bspw. der Fall, wenn die Adresse der Personen Rückschlüsse auf ein Pflegeheim oder einer Entzugsklinik zulässt. Die Angabe der Adresse ist nach dem Listenprivileg an sich zulässig, in diesen Fällen aber wegen eines überwiegenden schutzwürdigen Interesses der Betroffenen an der Geheimhaltung der mit der Adresse verbundenen Informationen ausgeschlossen.

Ein schutzwürdiges Interesse des Verbrauchers wird per Gesetz nach § 28 Abs. 3 Satz 2 BDSG vermutet, wenn im Rahmen der Zweckbestimmung eines Vertrags- bzw. vertragsähnlichen Vertrauensverhältnisses bestimmte Daten übermittelt werden, die sich auf strafbare Handlungen, Ordnungswidrigkeiten oder arbeitsrechtliche Rechtsverhältnisse beziehen.

Ein schutzwürdiges Interesse des betroffenen Verbrauchers besteht, wenn er nach § 28 Abs. 4 BDSG der Übermittlung oder Nutzung zu Werbung oder Markt- oder Meinungsforschung *widersprochen* hat. Auf dieses Widerspruchsrecht ist der Betroffene von der verantwortlichen Stelle hinzuweisen – nach § 28 Abs. 4 Satz 2 BDSG spätestens „bei der Ansprache“. Im Regelfall muss die Unterrichtung über das Widerspruchsrecht „im direkten Zusammenhang mit der Entscheidung der verantwortlichen Stelle stattfinden“, die Daten des Betroffenen für Zwecke der Werbung oder Markt- oder Meinungsforschung zu verwenden.[52]

Für den Verbraucher besteht die Möglichkeit, sich in der sog. *Robinson-Liste* des privaten Deutschen Direkt-Marketing-Verbandes (DDV) einzutragen und so zum Ausdruck zu bringen, dass Werbezuschriften nicht erwünscht sind. Der DDV stellt diese Liste seinen angeschlossenen Unternehmen zur Verfügung, die sich zur Beachtung der Widersprüche verpflichtet haben. Systematisch handelt es sich bei der Robinson-Liste um eine Form der Selbstregulierung, d.h. um eine freiwillige Verpflichtung.[53] Das Angebot der Robinson-Liste ersetzt jedoch nicht das gesetzlich abgesicherte Widerspruchsrecht des Verbrauchers.[54]

---

[48] Bergmann/Möhrle/Herb, BDSG § 28, Rn. 153; kritisch dazu Weichert, FS Kilian 2004, S. 295 f.

[49] Simitis in: Simitis, BDSG, § 28, Rn. 237.

[50] Simitis in: Simitis, BDSG, § 28, Rn. 245.

[51] Simitis in: Simitis BDSG, § 28, Rn. 245; Schaffland/Wiltfang, BDSG § 28, Rn. 152.

[52] Simitis in: Simitis BDSG, § 28, Rn. 282.

[53] Berghoff, RDV 2002, 78, 79.

[54] Gola/Schomerus, BDSG § 28, Rn. 60.

Zum einen haben sich die angeschlossenen DDV-Unternehmen nur freiwillig verpflichtet, den Wunsch des Verbrauchers zu beachten. Zum anderen besteht keine gesetzliche Verpflichtung der Unternehmen, die Liste auch vor einer Datenverwendung zu konsultieren.[55] Auch kann aus einem fehlenden Eintrag in die Robinson-Liste nicht geschlossen werden, dass der Betroffene einer Verwendung seiner Daten für Werbezwecke nicht widersprochen habe. Schließlich ist zu beachten, dass der Eintrag in die Liste lediglich für fünf Jahre,[56] während der gesetzliche Widerspruch nach § 28 Abs. 4 BDSG unbefristet gilt.

### 1.3.3 Erstellung von Kundenprofilen

Ein Beispiel für die Erhebung, Verarbeitung oder Nutzung von Daten zu weitergehenden, außerhalb des Vertrages liegenden Zwecken ist die Erstellung von Kunden- bzw. Konsumprofilen. Aus Sicht des Verbraucherdatenschutzes geht es um die Verdichtung und Aufbereitung von für sich genommen möglicherweise harmlosen Einzelinformationen zu einem umfassenderen Kundenprofil, wobei über die Summe der Einzelinformationen hinaus neue und weitergehende Meta-Informationen gewonnen werden können.[57] Es stellt sich grundsätzlich die Frage, ob die Verwendung von Kundendaten in dieser Form noch von den gesetzlichen Verwendungsbefugnissen des Datenschutzrechts, insbesondere des § 28 BDSG gedeckt ist.

Für ein Kundenprofil werden Kundenstammdaten, d.h. Namen-, Adress- und Geburtsdaten, mit weiteren Informationen zusammengeführt, die sich aus dem Konsumverhalten der Kunden ergeben. Mit der Zusammenstellung, Verdichtung und Aufbereitung – meistens über Methoden und Verfahren des Data Warehousing und Data Mining – können neue Informationen und Zusammenhänge ermittelt werden, die z.B. Prognosen über das zukünftige Kundenverhalten ermöglichen.[58] Es können Angebote platziert werden, die speziell auf das Kaufverhalten oder den Kunden selbst abgestimmt sind.[59] Neben einer unangemessenen Beeinflussung und gar Manipulation der Kundenwünsche und des Kaufverhaltens[60] können derartige Profile auch zu Persönlichkeitsrechtsverletzungen führen, wenn aus den Informationen über das Verhalten Aussagen über die individuelle Persönlichkeitsstruktur des Kunden gewonnen werden können.

Aus datenschutzrechtlicher Sicht ist Ausgangspunkt für die rechtliche Bewertung eines Kundenprofils § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Die Daten werden im Rahmen des Vertragsverhältnisses erhoben und dienen damit auch nur dazu, die Durchführung des Vertrages zu

---

55 Gola/Schomerus, BDSG § 28, Rn. 60.

56 Simitis in: Simitis, BDSG, § 28, Rn. 272.

57 Scholz, Datenschutz bei Data Warehousing und Data Mining in Roßnagel (Hrsg.), HdBDatSchR, Kap. 9.2, Rn. 35.

58 Scholz, Datenschutz bei Data Warehousing und Data Mining in Roßnagel (Hrsg.), HdBDatSchR, Kap. 9.2, Rn. 35.

59 Baeriswyl, RDV 2000, 6, 7.

60 Scholz, Datenschutz bei Data Warehousing und Data Mining in Roßnagel (Hrsg.), HdBDatSchR, Kap. 9.2, Rn. 36.

sichern. Die Speicherung von Namen und Adresse des Kunden können ebenso wie die Informationen über das konkret gekaufte Produkt bis zur Abwicklung des Zahlungsvorganges erforderlich sein; eine darüber hinausgehende Speicherung dieser Daten für Zwecke der Vertragserfüllung ist im Regelfall jedoch nicht erforderlich. Von der Zweckbestimmung der Vertragsbeziehung nicht mehr erfasst ist die Speicherung von Kundendaten und der Zusammenführung mehrerer Einkäufe derselben Person zu einem Profil, um sie für eine gezielte Werbung oder für individualisierte Angebote gegenüber dem einzelnen Kunden zu nutzen. Eine solche Verarbeitung der Kundendaten stellt vielmehr eine Zweckänderung dar, die allein unter den Voraussetzungen des §§ 28 Abs. 2, Abs. 3 BDSG gerechtfertigt sein kann (s.o. 28 ff.).

Das Unternehmen hat ein wirtschaftliches Interesse, seine Werbung bzw. seine Angebote bei seinen Kunden gezielter zu platzieren. Dieses Interesse wird von der Rechtsordnung grundsätzlich auch als berechtigt anerkannt, vermag jedoch die Bildung von umfassenden Kundenprofilen nicht zu rechtfertigen. Ihm steht das schutzwürdige Interesse des betroffenen Verbrauchers entgegen, sein historisches Bestell- und Kaufverhalten gegenüber Dritten transparent und einer Auswertung nach seinen Interessen zugänglich zu machen. Das überwiegende schutzwürdige Interesse des Betroffenen ergibt sich zum einen, weil er die über ihn gespeicherten Informationen über sein bisheriges Kaufverhalten im Regelfall nicht mehr in dem Umfang wissen wird, wie sie im Warenwirtschaftssystem des Verkäufers zur Verfügung stehen. Vor allem aber kann der betroffene Verbraucher diese Informationen – als Einzelinformationen sowie als Summe – in ihrer Bedeutung als Tatsachenbasis für Schlussfolgerungen und Bewertungen des verbrauchenden Unternehmers zu seiner Person in keiner Weise abschätzen. Während der betroffene Verbraucher aus seiner Sicht in der Vergangenheit lediglich immer mal wieder bei dem Anbieter das eine oder andere Produkt eingekauft hat, akkumuliert der Anbieter diese Informationen zu einem individuellen Verbraucherprofil, aus dem sich bisherige Interessen sowie zukünftige Bedürfnisse ergeben. Es verletzt das Persönlichkeitsrecht des Betroffenen, wenn ein detailliertes Bild seiner Bedürfnisstruktur vorgehalten wird, um es ihm gegenüber für Werbezwecke zu nutzen.

Nach dem Volkszählungsurteil des BVerfG ist sogar auch in der Anonymität der statistischen Erhebung eine umfassende Registrierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen unzulässig.[61] Das informationelle Selbstbestimmungsrecht und die Menschenwürde verbieten die Katalogisierung und Registrierung des Menschen in seiner ganzen Persönlichkeit.[62] Der Einzelne soll also nicht gleichsam als Informationsobjekt behandelt, insbesondere soll seine Persönlichkeit nicht lediglich auf kommerziell Verwertbares reduziert, werden, um den Betroffenen dann zu eigenen Zwecken instrumentalisieren zu können.[63]

Der Erstellung von Kundenprofilen stehen demnach die schutzwürdigen Interessen der Verbraucher gegenüber, da die berechtigten Interessen der Unternehmen an einer solchen

---

[61] BVerfGE 65, 1, 42; siehe auch Wittig, RDV 2000, 59, 61.

[62] BVerfGE 65, 1, 52; siehe auch Wittig, RDV 2000, 59, 61.

[63] Simitis in: Simitis, BDSG, § 28, Rn. 174.

umfassenden Profilbildung nicht überwiegen. Die gesetzliche Ermächtigungsgrundlage des § 28 Abs. 2, Abs. 3 BDSG kann eine solche Datenverwendung nicht rechtfertigen. Sie kann demnach nur auf der Grundlage einer Einwilligung gerechtfertigt sein.

# 2 Einwilligung als Rechtsgrundlage der Verarbeitung

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten erlaubt, wenn der Betroffene wirksam eingewilligt hat. Die datenschutzrechtliche Einwilligung ist mit anderen Worten den gesetzlichen Erlaubnistatbeständen gleichgestellt.

## 2.1 Bedeutung der Einwilligung bei Verbraucherverträgen

Für die Unternehmen gewinnt die Einwilligung als Legitimationsgrundlage an Bedeutung, wenn die geplante Verwendung nicht (mehr) durch die Verwendungsbefugnisse des § 28 BDSG bzw. einer anderen Rechtsvorschrift gedeckt ist. Ausgangspunkt für die Frage, wann eine Einwilligung erforderlich ist und die gesetzlichen Erlaubnistatbestände nicht bzw. nicht (mehr) einschlägig sind, ist der konkrete Zweck des Verbrauchervertrages. Soweit das beabsichtigte Erheben, Speichern, Verändern, Übermitteln oder Nutzen der personenbezogenen Daten dem Vertragszweck dient und für die Durchführung des Vertrages erforderlich ist (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG), braucht das Unternehmen keine Einwilligung des Verbrauchers einzuholen. Der Verwendung von Daten auf der Grundlage von § 28 BDSG sind jedoch enge Grenzen gesteckt, denn die gesetzlichen Verwendungsbefugnisse sind restriktiv auszulegen.[64] Außerhalb ihrer Grenzen kommt eine Verwendung nur mit wirksamer Einwilligung in Betracht.

Liegt die geplante Verwendung der Daten außerhalb des Vertragszweckes bzw. werden die Daten auch noch zu anderen als den ursprünglich vorgesehenen Zwecken verwendet, muss anhand einer Interessenabwägung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) festgestellt werden, ob die Verwendung erforderlich, ein berechtigtes Interesse des Unternehmens zu wahren ist und keine schutzwürdigen Belange des Verbrauchers an einem Ausschluss der Verarbeitung bzw. Nutzung überwiegen (s.o. S. 24).

Im Rahmen von z.B. Bargeschäften des täglichen Lebens ist es nicht notwendig, die Adresse oder den Namen des Vertragspartners zu erheben. Hier wird die Ware sofort bezahlt und mitgenommen. Ein weiterer Kontakt zwischen den Vertragspartnern ist für die Durchführung des Vertrages unerheblich. Auch ein konkretes berechtigtes Interesse zur Ermittlung der Kundendaten ist für diese Art von Geschäften nicht ersichtlich.

Erhebt ein Supermarkt von Kunden, die mit einem 50-Euro-Schein bezahlen wollen, deren Name und Adresse, um im Fall einer Fälschung den Überbringer identifizieren zu können, so ist dieser Vorgang nicht durch die Tatbestände des § 28 BDSG gedeckt. Es fehlt an der Erforderlichkeit. Zur Feststellung der Echtheit eines Geldscheines kommen mildere Mittel wie z.B. die Benutzung eines Fälschungsstiftes[65] oder einer Schwarzlichtlampe in Betracht. Das

---

[64] Breinlinger, RDV 1997, 247, 251; Simitis in: Simitis, BDSG, § 28, Rn. 78.

[65] Mit dem Stift wird ein Strich auf den Schein gemalt; wenn der Strich sich dunkel färbt, handelt es sich um eine Fälschung.

Erheben von Namen und Adressdaten ist also weder zur Durchführung des konkreten Vertrages erforderlich, noch zur Wahrung des berechtigten Interesses, sich vor unechten Scheinen zu schützen. Hier muss eine wirksame Einwilligung des Betroffenen eingeholt werden.

Auch die Übermittlung oder Nutzung von Verbraucherdaten zu anderen als den bei der Erhebung vorgesehenen Zwecken ist nach § 28 Abs. 2, Abs. 3 BDSG von einer Interessenabwägung abhängig (s.o. S. 28 ff.).

Im Rahmen eines Allfinanzkonzeptes werden Kundendaten aus einem Bereich der Finanzdienstleistung an einen anderen Bereich, konzernintern oder zwischen Kooperationspartnern, weitergegeben. Typischerweise wirken bei einem solchen Konzept Banken, Versicherungen und Bausparkassen zusammen, die ihren Kunden z.B. über die mit dem Kunden vereinbarte Bankleistungen hinaus weitere Finanzdienstleistungen „aus einer Hand“ wie Lebensversicherungen oder Bausparverträge anbieten wollen. Um die Verbraucher anzusprechen und ein Angebot zu platzieren, werden Kundendaten aus dem einen Vertragsverhältnis an die kooperierenden bzw. konzernverbundenen Unternehmen durch Weitergabe, Abruf oder Einsichtnahme übermittelt. Eine solche Verarbeitung und Nutzung der Kundendaten ist ohne Einwilligung des Betroffenen unzulässig, denn die in diesem Zusammenhang vorgenommene Verarbeitung und Nutzung der Kundendaten übersteigt den nach § 28 BDSG zulässigen Umfang einer gesetzlich legitimierten Datenverwendung.

Die Übermittlung der Daten an das kooperierende Unternehmen dient nicht mehr dem ursprünglichen Zweck des Vertrages mit dem Vertragspartner, so dass § 28 Abs. 1 Nr. 1 BDSG als Ermächtigungsgrundlage der Übermittlung ausscheidet. Jede weitere Verarbeitung außerhalb des Vertragszwecks ist von einer Interessenabwägung (§ 28 Abs. 1 Nr. 2 oder § 28 Abs. 2, 3 BDSG) abhängig. Für die Teilnehmer am Allfinanzkonzept besteht ein berechtigtes Interesse wirtschaftlicher Natur, die Kundendaten zu bekommen bzw. bei einer Weitergabe zwischen Töchtern eines Konzerns in der Senkung von Transaktionskosten sowie einer Zunahme von Vertragsabschlüssen durch so genannte Synergieeffekte.[66]

Die schutzwürdigen Belange der Kunden überwiegen allerdings gegenüber diesen berechtigten wirtschaftlichen Interessen regelmäßig. Der Verbraucher, der einen Girokontovertrag abschließt, rechnet nicht damit, dass seine Daten auch für eine Bausparkassen- oder Versicherungsvertragsansprache verwertet werden. Nach dem Willen des Gesetzgebers soll es für den Betroffenen überschaubar bzw. transparent sein, wer welche Daten über ihn gespeichert hat bzw. nutzt oder weitergibt. Eine solche Transparenz ist für den Betroffenen bei der unüberschaubaren Übermittlung zwischen den verschiedenen Unternehmen nicht ersichtlich. Insbesondere bei Finanzdaten, die einen besonders tiefen Einblick in die persönlichen und wirtschaftlichen Verhältnisse des Betroffenen zulassen, ist eine Weitergabe im Rahmen von Allfinanzkonzepten für den Betroffenen besonders empfindlich. Diese Daten haben nicht nur Einfluss auf die geschäftliche bzw. wirtschaftliche Betätigung des Betroffenen, sondern ge-

[66] Kilian/Scheja RDV 2002, 177, 184.

ben häufig auch einen besonders tiefen Einblick in das Privat- und Berufsleben.[67] Allein eine wirksame Einwilligung des Betroffenen kann eine derartige Übermittlung rechtfertigen.

Gerade im Zusammenhang mit Kooperationen zwischen Unternehmen oder bei konzerninternen Datenflüssen spielt die Einwilligung des Betroffenen als Legitimationsgrundlage eine große Rolle. Für die Unternehmen ist die Zusammenfassung von Kundendaten oder der Austausch von Adressen insbesondere zur gezielten Werbeansprache eine gewichtige ökonomische Maßnahme, die sich meist nur über die Einwilligung realisieren lässt.

## 2.2 Ausschlusswirkung gegenüber gesetzlichen Tatbeständen

Aus der Sicht der Verbraucher ist die Einwilligung - sofern sie nach den gesetzlichen Anforderungen wirksam ist - diejenige Form, eine Datenverarbeitung zu legitimieren, die dem informationellen Selbstbestimmungsrecht am Besten Rechnung trägt. Die Betroffenen können selbst entscheiden, ob und in welchem Umfang ihre personenbezogenen Daten verwendet werden sollen. Insofern kommt der Einwilligung auch eine gewisse Ausschlusswirkung gegenüber den gesetzlichen Tatbeständen zu.

Entscheidet sich ein Unternehmen, eine Datenverwendung durch eine Einwilligung des Betroffenen zu rechtfertigen, obwohl auch eine gesetzliche Verwendungsbefugnis dazu ermächtigen würde, muss die Verwendung verbindlich von dem Bestehen der Einwilligung abhängig sein. Verweigert der Betroffene die Einwilligung oder widerruft diese, dann ist es dem Unternehmen verwehrt, sich auf die gesetzlichen Erlaubnistatbestände zu stützen, um mit der Verwendung fortzufahren. Ein Rückgriff auf die Rechtsvorschriften ist in diesen Fällen unter dem Gesichtspunkt von Treu und Glauben (§ 242 BGB) problematisch.[68] Dem Verbraucher wird suggeriert, dass die Verwendung der Daten tatsächlich voll und ganz im Rahmen seiner informationellen Selbstbestimmung liege, d.h. von der Erteilung seiner Einwilligung abhängig sei.[69] Er wird getäuscht, wenn die Daten trotz Widerrufs bzw. Verweigerung der Einwilligung (weiter) verwendet werden.[70]

Entscheidet sich ein Unternehmen für den Weg der Einwilligung – sei es zur Sicherheit, weil unklar ist, ob die beabsichtigte Verwendung von einem gesetzlichen Erlaubnistatbestand erfasst wird, sei es, weil die geplante Verwendung gegebenenfalls über das gesetzlich legitimierte hinausgeht – so ist jede Verwendung der Daten an die Erteilung bzw. an das Fortbestehen dieser Einwilligung gebunden.[71]

---

[67] Kilina/Scheja RDV 2002, 177, 184.

[68] Gola RDV 2002, 109, 110.

[69] Gola RDV 2002, 109, 110.

[70] Sokol in: Simitis, BDSG, § 4, Rn. 6.

[71] Sokol in: Simitis, BDSG, § 4, Rn. 6.

## 2.3 Voraussetzungen einer wirksamen Einwilligung

### 2.3.1 Freie Entscheidung des Betroffenen

Die Einwilligung muss nach § 4 a Abs. 1 Satz 1 BDSG auf der freien Entscheidung des Betroffenen beruhen. Die Freiwilligkeit ist nur dann gewahrt, wenn der Betroffene die Einwilligung frei von staatlichen, rechtlichen oder auch faktischen Zwängen abgibt.[72] Für den Verbraucher können sich dann faktische Zwänge ergeben, wenn der Abschluss des Vertrages von der Einwilligung in andere für die Vertragsdurchführung nicht erforderliche Datenverwendungen abhängig gemacht wird.[73] Speziell in den Fällen, in denen die Vertragsbeziehung für den Verbraucher existenziellen Charakter hat, wie z.B. bei bestimmten Versicherungsverträgen, soll durch das Merkmal der Freiwilligkeit eine derartige Erpressungssituation vermieden werden. Für den Bereich des Telekommunikations- und Medienrechts ist ein solches *Koppelungsverbot* ausdrücklich gesetzlich festgeschrieben (§ 3 Abs. 4 TDDSG).[74]

Eine wesentliche Voraussetzung für eine freie Entscheidung des Betroffenen ist die Kenntnis darüber, dass die Erteilung seiner Einwilligung freiwillig ist und welche Folgen sich aus einer Verweigerung ergeben (§ 4 a Abs. 1 Satz 2 BDSG). Mit der Erklärung muss daher ein Hinweis an den Kunden einhergehen, dass die Einwilligung in die Verwendung seiner personenbezogenen Daten zu bestimmten Zwecken freiwillig erteilt wird. Gleichzeitig ist der Verbraucher über die Folgen der Verweigerung der Einwilligung aufzuklären.

### 2.3.2 Zeitpunkt und Form

Die Einwilligung muss vor der Datenverwendung von der für die Verarbeitung verantwortlichen Stelle von dem betroffenen Verbraucher eingeholt werden. Eine nachträgliche Zustimmung genügt dem gesetzlichen Erfordernis der Einwilligung nicht.

Nach § 4 a Abs. 1 Satz 3 BDSG muss die Einwilligung grundsätzlich schriftlich erteilt werden (§ 126 BGB).[75] Der Schriftform wird gegenüber dem Betroffenen eine besondere Warnfunktion beimessen, d.h. sie soll dem Betroffenen bewusst machen, dass seine Einwilligung für ihn von Bedeutung ist.

Eine Ausnahme ist nur dann zulässig, wenn wegen besonderer Umstände eine andere Form angemessen ist. Wenn z.B. bei der Befragung durch ein Marktforschungsinstitut die Daten

---

[72] Sokol in: Simitis, BDSG, § 4 a, Rn. 64.

[73] Simitis in: Simitis, § 4, Rn. 65, 88; Gola/Schomerus, BDSG § 4 a, Rn. 6.

[74] Hierzu LG Potsdam, DuD 2005, 302.

[75] Bergmann/Möhrle/Herb, BDSG § 4 a, Rn. 8.

nach der Speicherung anonymisiert werden oder besondere Eilbedürftigkeit auf Seiten des Betroffenen besteht, ist eine mündliche Einwilligung in der Regel ausreichend.[76]

Nach § 126 Abs. 3 BGB ist die *elektronische Form* nach § 126a BGB der Schriftform gleichgestellt, solange das elektronische Dokument mit dem Namen des Ausstellers und einer qualifizierten elektronischen Signatur verbunden ist. Im Rahmen des Telekommunikations- und Teledienstерechts ist die elektronische Einwilligung auch ohne eine qualifizierte elektronische Signatur wirksam. Im Online-Bereich bestehen also bereichsspezifische Sonderregelungen zu den Formanforderungen der datenschutzrechtlichen Einwilligung.

### 2.3.3 Gestaltungsanforderungen

Insbesondere bei standardisierten Formularverträgen wird die Einwilligungserklärung häufig zusammen mit anderen vertragsrelevanten Erklärungen verbunden. Ein solches Vorgehen ist nach § 4 a Abs. 1 S. 4 BDSG zulässig, wenn die Einwilligungserklärung „besonders hervorgehoben“ wird. In diesem Zusammenhang stellt sich die Frage, ob auch Einwilligungserklärungen in Form von so genannten *Widerspruchs- oder Streichlösungen* (Opt-out) den Anforderungen an eine wirksame Einwilligung i.S.d. § 4 a BDSG genügen.

#### 2.3.3.1 Streichlösung

Bei derartigen Erklärungen ist die Einverständniserklärung zur Einwilligung vorgegeben, so dass der Verbraucher nicht tätig werden muss, um eine Verwendung zu ermöglichen. Er muss im Gegenteil durch Ausstreichen eines bestimmten Passus tätig werden, um eine Verwendung seiner Daten außerhalb des Vertragszweckes zu verhindern. In diesen Fällen findet eine Risikoverlagerung zu Lasten des Verbrauchers statt. Während bei einer Ausgestaltung als aktive Einwilligung das Unternehmen das Risiko trägt, dass der betroffene Verbraucher nicht einwilligt, wird dieses Risiko im Fall der Ausgestaltung als Streichlösung dem Verbraucher auferlegt.

Eine solche sog. Opt-out-Lösung ist im Rahmen der Nutzung von Telediensten nach § 4 Abs. 2 Nr. 1 TDDSG unzulässig, da die Einwilligungserklärung hier allein durch eine „bewusste Handlung“ und nicht durch ein Unterlassen erfolgen darf. Eine technische Ausgestaltung, „die eine bestätigende Wiederholung des Übermittlungsbefehls sicherstellt“, ist in diesen Fällen ausreichend. [77]

Außerhalb von Internetgeschäften wird die Streichlösung im Zusammenhang mit Kundenbindungssystemen zum Teil mit dem Hinweis auf § 4 a Abs. 2 S. 4 BDSG für ausreichend erachtet.[78] Zur Begründung wird angeführt, dass das Gesetz ausdrücklich vorsieht, dass die Einwilligung zusammen mit anderen Erklärungen abgegeben werden kann. Auf welche Art

---

[76] Bergmann/Möhrle/Herb, BDSG§ 4 a, Rn. 86, 87.

[77] LG Paderborn, Urteil vom 10.03.05, Az.: 12 O 287/04, DuD 2005, 308.

[78] So vertreten von einem Teil der Aufsichtsbehörden in Bezug auf Kundenbindungssysteme.

die Einwilligung hervorgehoben werde, bleibe dem Unternehmen überlassen, so dass auch die Streichlösung zulässig sei, solange diese deutlich hervorgehoben und für den Betroffenen erkennbar ist.

Dem ist entgegenzuhalten, dass nach § 4 a BDSG die Einwilligung freiwillig und grundsätzlich schriftlich zu erfolgen hat; d.h. der Betroffene soll davor geschützt werden, sich unter Zwang, übereilt oder vorschnell zu äußern. Um dies sicherzustellen und zweifelsfrei zu dokumentieren, ist ein aktives Handeln des Kunden erforderlich, das entweder durch eine gesonderte Unterschrift oder ein Ankreuzen der gewünschten Erklärung realisiert werden kann. Ein fehlender Handlungsakt des Kunden kann dagegen nicht zweifelsfrei als eine bewusste Erklärung ausgelegt werden.

Zudem handelt es sich bei der Einwilligungserklärung i.S.d. § 4 a BDSG um eine rechtsgeschäftliche Erklärung[79], für die auch die allgemeinen Grundsätze für Willenserklärungen Anwendung finden müssen.[80] Vor diesem Hintergrund ist bereits fraglich, ob bei der Streichlösung die Einwilligung überhaupt konkludent durch schlüssiges Verhalten erteilt wird, indem der Betroffene die Passage nicht ausstreicht. Zwar setzt der Betroffene seine Unterschrift unter den gesamten Text und gibt damit zum Ausdruck, mit dem Inhalt der Erklärung einverstanden zu sein. In Bezug auf das Nichtausstreichen bzw. Nichtankreuzen des Einwilligungskästchens gleicht das Verhalten des Betroffenen jedoch einem Nichthandeln bzw. Nichtstun oder gar einem Schweigen, das als Einverständnis ausgelegt wird. Hierbei handelt es sich jedoch um eine Fiktion. Es kann nicht davon ausgegangen werden, dass der Kunde sämtliche Hinweise über die Möglichkeiten, nicht zutreffende Passagen zu streichen bzw. das Widerspruchskästchen anzukreuzen, zur Kenntnis genommen hat und in dem Unterlassen ein bewusstes Verhalten liegt. Von wenigen Ausnahmen abgesehen (Fiktion einer Willenserklärung durch Gesetz, einer ausdrücklichen Vereinbarung in einem Rahmenvertrag im Vertrag bzw. beim kaufmännischen Bestätigungsschreiben) fehlt dem Schweigen im Rechtsverkehr grundsätzlich ein Erklärungswert und damit die Rechtsverbindlichkeit.

### 2.3.4 Konkludente Einwilligung

Im Übrigen ist selbst bei einer *konkludenten Einwilligungserklärung* zweifelhaft, ob diese den Anforderungen des § 4 a BDSG genügt.[81] § 4 a BDSG ist als Ausnahmevorschrift zum grundsätzlichen Verbot der Verwendung restriktiv auszulegen.[82] Zudem ist es gerade Ausdruck des informationellen Selbstbestimmungsrechts, wenn es außerhalb der gesetzlichen

---

[79] Simitis in: Simitis, BDSG, § 4 a, Rn. 23 m.w.N.; Bergmann/Möhrle/Herb BDSG § 4 a, Rn. 8.

[80] So auch LG Paderborn, Urteil vom 10. März 2005, Az.: 12 O 287/04, DuD 2005, 308, für die elektronische Einwilligungserklärung im Rahmen des § 4 Abs. 2 TDDSG, für die herkömmliche Einwilligungserklärung kann dann nichts anderes gelten.

[81] Simitis in: Simitis, BDSG, § 4 a, Rn. 46 m.w.N.

[82] Simitis in: Simitis, BDSG, § 4 a, Rn. 46.

Verwendungsbefugnisse allein auf die klare, ausdrückliche Entscheidung des Betroffenen ankommt und nicht auf die Interpretation eines nicht immer eindeutigen Unterlassens.[83]

Auch vor dem Hintergrund der Regelungen in der EG-Datenschutzrichtlinie[84] erscheint es eher bedenklich, eine konkludente Einwilligung im Rahmen des § 4 a BDSG ausreichen zu lassen. Nach Art. 7 a der Richtlinie muss die Einwilligung „ohne jeden Zweifel" erteilt sein, um eine wirksame Rechtsgrundlage einer Verarbeitung zu sein. Ohne jeden Zweifel kann ein Verhalten nur sein, wenn es allein eine Art der Deutung zulässt. Bei einem Unterlassen hingegen sind bereits zwei Alternativen gleichermaßen möglich: Der Betroffene kann sich bewusst für eine Einwilligung entschieden und deswegen die Passage nicht gestrichen haben. Es besteht allerdings genauso gut die Möglichkeit, dass dem Betroffenen vollkommen verborgen geblieben ist, dass er soeben seine Einwilligung erteilt hat. Im Lichte des Art. 7 der EG-Datenschutzrichtlinie ausgelegt, ist zumindest in solchen Bereichen, in denen die Verarbeitung personenbezogener Daten deutlich über das gesetzliche Maß hinausgeht, also für den Betroffenen nicht mehr überschaubar ist oder nachteilige Folgen für ihn haben kann, eine bewusste und aktive Erklärungshandlung gefordert.

## 2.4 Hinweispflicht der verantwortlichen Stelle

Gemäß § 4 a Abs. 1 Satz 2 BDSG ist der Betroffene vor Abgabe der Einwilligungserklärung auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen. Der Betroffene muss also noch vor der Einwilligung alle Informationen bekommen, die notwendig sind, um Anlass, Ziel und Folgen der Verarbeitung korrekt abzuschätzen.[85] Den datenschutzrechtlichen Anforderungen genügt die Darstellung in der Einwilligung nur dann, wenn diese hinreichend bestimmt ist, mithin klar zu erkennen gibt, unter welchen Bedingungen sich der Betroffene mit der Verarbeitung welcher Daten einverstanden erklärt.[86]

Nach der Rechtsprechung des BGH[87] muss der Kunde übersehen können, auf welche Daten sich seine Einwilligung erstreckt, welche Daten gespeichert sind und an welche Stellen sie übermittelt werden dürfen. Insbesondere ist dabei auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder sonstigen Nutzung der Daten hinzuweisen.

## 2.5 Einwilligung durch AGB

Wird die Einwilligungserklärung als *vorformulierte Klausel* im Rahmen eines Formularvertrages eingeholt, unterliegt sie der besonderen Kontrolle der Vorschriften zu den Allgemeinen

---

[83] Simitis in: Simitis, BDSG, § 4 a, Rn. 75.

[84] 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.

[85] Simitis in: Simitis, BDSG, § 4 a, Rn. 67.

[86] Simitis in: Simitis, BDSG, § 4 a, Rn. 74.

[87] BGH NJW 2003, 1237, 1241.

Geschäftsbedingungen (AGB) nach § 305 ff. BGB. Schutzzweck der AGB-Vorschriften im BGB ist neben der Verhinderung von wirtschaftlicher Übervorteilung durch alleinige Bestimmung des Vertragsinhaltes auch der Schutz des Verbrauchers (§ 310 Abs. 3 BGB) wegen seiner „rollenspezifischen Unterlegenheit".[88] Für den Verbrauchervertrag gelten die Vorschriften der AGB-Kontrolle nach § 310 Abs. 3 BGB auch dann, wenn die vorformulierten Vertragsbestimmungen nur zur einmaligen Verwendung bestimmt sind.

### 2.5.1 Treu und Glauben

Im Wesentlichen ist für die Überprüfung der Zulässigkeit einer formularmäßigen Einwilligung festzustellen, ob die Klausel ungewöhnlich und damit für den Betroffenen überraschend ist (§ 305 c BGB) oder ob sie ihn entgegen den Geboten von *Treu und Glauben* unangemessen benachteiligt (§ 307 BGB). Eine AGB ist i.S.d. § 305 c BGB überraschend, wenn sie z.B. wegen Unvereinbarkeit mit dem Leitbild des Vertrages, der Höhe des Entgeltes oder einer erheblichen Abweichung vom dispositiven Recht ungewöhnlich ist und der Verbraucher den Umständen nach vernünftigerweise nicht mit dieser zu rechnen braucht.[89] Übertragen auf die Fälle der formularmäßigen Einwilligung bedeutet dies, dass die beabsichtigte Datenverwendung als solche, in ihrer Art – welche Daten werden verwendet – oder ihrem Umfang soweit außerhalb eines Zusammenhanges mit Vertragszweck oder Vertragsdurchführung steht, dass sie vollkommen unüblich ist und für den Betroffenen unerwartet kommt.

Bei einem Preisausschreiben wird durch die Teilnahmebedingungen bestimmt, dass die Gewinner ihre ausdrückliche Zustimmung zur Vermittlung oder gar Veröffentlichung ihres Namens, ihrer Adresse und ihres Lichtbildes für Werbezwecke erteilen. Aus Verbrauchersicht ist die Teilnahme an einem *Gewinnspiel* grundsätzlich ein relativ nebensächlicher Vorgang. Es handelt sich nicht um einen Vertrag, der große Veränderungen oder ein hohes Risiko mit sich bringt. Im Gegenteil geht der Verbraucher insbesondere bei einem unentgeltlichen Vertrag davon aus, „nichts zu verlieren" zu haben. Vor diesem Hintergrund ist für ihn nicht ohne Weiteres erkennbar, dass die Teilnahme entgegen dem üblichen Verfahren einen weitgehenden Eingriff in sein Persönlichkeitsrecht eröffnet, indem er seinen Name, seine Adresse, sein Interesse an einem bestimmten Produkt offenbart. Eine derartige Klausel ist nach § 305 c BGB überraschend und damit unwirksam.[90]

Nach § 307 Abs. 1 BGB sind AGB-Regelungen immer dann unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Diese Generalklausel wird durch § 307 Abs. 2 BGB konkretisiert. Danach wird eine unangemessene Benachteiligung vermutet, wenn nach § 307 Abs. 2 Nr. 1 BGB „die Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinen ist". Der Bewertungsmaßstab für die Zulässigkeit einer

---

[88] Palandt/Heinrichs, BGB Überbl v § 305, Rn. 9; vgl. bspw. BGHZ 95, 362, 368; BGH, DuD 2004, 51 f. AG Elmshorn,MMR 2005, 870 ff.

[89] Palandt/Heinrichs, BGB § 305c, Rn. 3.

[90] OLG Karlsruhe, RDV 1988, 146-148.

AGB-Vertragsbestimmung orientiert sich damit trotz des Grundsatzes der freien Vertragsgestaltung an den gesetzlichen Bestimmungen, denen nach der Rechtsprechung des BGH insoweit eine Ordnungs- und Leitbildfunktion zukommt.[91] Die Rechtsprechung unterscheidet zwischen frei abänderbaren Zweckmäßigkeitsregeln und formularmäßig unabdingbaren Gerechtigkeitsgeboten.[92] Während erstere bei der Überprüfung von AGB-Klauseln keine Bedeutung haben, stellen letztere die wesentlichen Grundgedanken der abbedungenen Norm dar, wenn sie dem Schutze des Vertragspartners zu dienen bestimmt sind.[93]

### 2.5.2 Schutzzweck des BDSG

Die Zulässigkeit einer Einwilligung in die Verwendung von personenbezogenen Daten im Rahmen einer AGB-Bestimmung ist danach am *Schutzzweck des BDSG* und den gesetzlichen Erlaubnistatbeständen zur Verwendung dieser Daten, z.B. in § 28 BDSG, zu messen. Zwar werden die Einwilligung und die Rechtsvorschriften in § 4 Abs. 1 BDSG als gleichrangige Legitimationsgrundlagen für die Verwendung personenbezogener Daten auf eine Stufe gestellt. Durch die vorformulierte Einwilligungserklärung werden die dispositiven Zulässigkeitstatbestände des BDSG allerdings abbedungen. Die wesentlichen Grundgedanken der Regelungen und die darin enthaltenen wesentlichen Schutzvorschriften leben nach der Rechtsprechung als Orientierungsrahmen wieder auf und sind damit Prüfungsmaßstab im Sinne des § 307 Abs. 2 Nr. 1 BDSG. [94]

Die *Schutzrichtung* des BDSG ist in § 1 Abs. 1 BDSG normiert. Danach soll der Einzelne davor geschützt sein, durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt zu werden. Um eine Beeinträchtigung zu vermeiden, ist eine Verwendung grundsätzlich verboten und nur ausnahmsweise mit ausdrücklicher Legitimation durch den Betroffenen selbst oder per Gesetz erlaubt (§ 4 Abs. 1 BDSG). Fehlt es an einer Einwilligung, so ist die Verwendung außerhalb der Zweckbestimmung des Vertrages nach § 28 BDSG nicht nur von der Erforderlichkeitsprüfung, sondern auch von einer Interessenabwägung abhängig. Mit der gesetzlichen Verwendungsbefugnis in § 28 BDSG sollte nicht ein weiterer, die Belange des Betroffenen unberücksichtigt lassender Verwendungsrahmen geschaffen werden. Vielmehr sind die Erlaubnistatbestände des BDSG als Ausnahmetatbestände zum grundsätzlichen Verbot der Verwendung restriktiv auszulegen.[95] Als wesentliche Grundgedanken müssen daher der restriktive Charakter und die Einbeziehung der schutzwürdigen Interessen der Verbraucher durch eine Interessenabwägung sowie die Grenzen der Verwendung durch das Merkmal der Erforderlichkeit in der Einwilligungsklausel abgebildet werden.[96]

---

91 BGHZ 41, 151, 154; 54, 106, 110; 89, 206, 211.

92 BGHZ 115, 38, 42.

93 Palandt/Heinrichs, BGB § 307, Rn. 27.

94 Siehe auch Heidemann-Peuser, DuD 2002, 389 ff.

95 Breinlinger, RDV 1997, 251; Simitis.-Simits, BDSG, § 28, Rn. 78.

96 Heidemann-Peuser, DuD 2002, 389, 392; Schwintowski, VuR 2004, 242, 245.

Bereits in seinem Urteil zur Schufa-Klausel hat der BGH[97] festgestellt, dass eine unangemessene Benachteiligung vorliegt, wenn der Kreditgeber in der Klausel uneingeschränkt ermächtigt wird, auch Negativmerkmale[98] ohne Interessenabwägung im Einzelfall an ein Kreditinformationssystem zu übermitteln. Eine Klausel, die sich in diesem Zusammenhang nicht auf die Übermittlung von Kreditdaten beschränkt, sondern pauschal auf die Übermittlung von Daten des Kreditnehmers hinweist, ist ungenügend und daher unzulässig. [99]

### 2.5.3 Datenweitergabeklauseln

Ähnlich ist die Rechtslage bei den regelmäßig in Versicherungsverträgen anzutreffenden *Datenweitergabeklauseln*.[100] Diese Klauseln dienen für verschiedene Übermittlungen von Versichertendaten u.a. auch als Grundlage für die Übermittlung von Kundendaten an andere Versicherer, indem sie in sog. Warn- und Hinweisdateien der Fachverbände (UNIWAGNIS) eingestellt und von allen angeschlossenen Versicherern abgerufen werden können. Handelt es sich dabei um sog. harte Negativdaten[101], wie z.B. die Verurteilung wegen eines Versicherungsbetruges, so ist eine Einmeldung der Versichertendaten in das System von der gesetzlichen Verwendungsbefugnis nach § 28 Abs. 1 Nr. 2, Abs. 3 Nr. 1 BDSG gedeckt. In diesen Fällen überwiegt das berechtigte Interesse der Versicherer an der Kenntnis solcher Vorfälle gegenüber den schutzwürdigen Belangen des Betroffenen.

Etwas anderes gilt für die Weitergabe sog. „weicher" Negativdaten, die dadurch gekennzeichnet sind, dass sie gerade keine Tatsachen darstellen, sondern, wenn überhaupt, als bloße Indizien für einen negativen Umstand gewertet werden können. Im Bereich des Versicherungswesens sind solche Merkmale z.B. die Kennzeichnung als auffällige Schadensfälle, häufige Kfz-Diebstähle, Verdacht des Versicherungsmissbrauches oder auch die Kündigung der Rechtsschutzversicherung.[102] An letztgenanntem Merkmal wird deutlich, dass die für die Weitergabe solcher Daten formularmäßig erteilte Einwilligungsklausel auch eine Berücksichtigung der schutzwürdigen Belange des Versicherten vorsehen muss.

Dem Versicherungsnehmer einer Rechtsschutzversicherung droht z.B. eine Kündigung, wenn er seine Versicherung innerhalb eines bestimmten Zeitraums mehrmals in Anspruch nimmt. Der Versicherungsnehmer läuft dann Gefahr, dass ein Eintrag in der Gekündigten-

---

97 BGH NJW 1986, 46, 47.

98 Der BGH bezog sich dabei auf „einseitige Maßnahmen des Kreditgebers zur Durchsetzung vermeintlicher Ansprüche gegen den Kreditnehmer, beispielsweise Mahnungen, Kündigungen, Mahnbescheide" NJW 1986, 46, 47.

99 BGH NJW 1986, 46, 47.

100 Siehe eingehend Schwintowski, Rechtsgutachten zur Beurteilung der Datenweitergabeklausel in Antragsformularen der Versicherungswirtschaft im Geschäft mit Verbrauchern in Deutschland, Berlin 2004.

101 BGH NJW, 1986, 46, 47; harte Negativmerkmale besitzen eine gewisse Objektivität durch „im Rechtsverkehr geschaffene Tatsachen" vgl. Schwintowski, Rechtsgutachten zur Beurteilung der Datenweitergabeklausel, S. 23.

102 Vgl. Schwintowski, Rechtsgutachten zur Beurteilung der Datenweitergabeklausel, S. 23.

Datei zu einer pauschalen Ablehnung als Versicherungskandidat bei anderen Rechtsschutzversicherern führt, ohne dass spezielle Umstände des Versicherungsnehmers bei der Einstellung der Kündigung in die Datei Berücksichtigung fänden.

Hat der ehemalige Versicherungsnehmer z.B. einen prozesswütigen Nachbarn, so liegt die häufige Verwicklung in Rechtsstreitigkeiten außerhalb seines Einflussbereiches. Die Einwilligungsklausel ist für die Übermittlung der so genannten „weichen" Negativmerkmale daher so zu gestalten, dass die Interessen des Versicherungsnehmers z.B. durch die Gelegenheit zur Kenntnis- und Stellungnahme vor Einmeldung in das System berücksichtigt werden können, um eine unangemessene Benachteiligung i.S.d. § 307 BGB zu vermeiden.

### 2.5.4 Fehlende Transparenz

Eine unangemessene Benachteiligung kann sich auch aus der fehlenden Transparenz einer Klausel ergeben. Nach § 307 Abs. 1 Satz 2 BGB ist diese „klar und verständlich" auszugestalten und zu formulieren. Die Rechte und Pflichten des Vertragspartners müssen durchschaubar, richtig, bestimmt und möglichst klar dargestellt sein.[103] Für den Betroffenen muss nach der Rechtsprechung des BGH[104] ersichtlich sein, auf welche Daten sich die Einwilligung erstreckt, welche Daten gespeichert und an welche Stellen sie übermittelt werden dürfen. Insbesondere der Zweck der Verwendung muss dem Betroffenen aus der Klausel deutlich sein. Eine pauschal gefasste Erklärung, die weder den Umfang der Verwendung noch den Zweck hinreichend konkret erkennen lässt, ist mit dem Transparenzgebot des § 307 Abs. 1 S. 2 BGB nicht vereinbar.

[103] Palandt/Heinrichs, BGB § 307, Rn. 16.

[104] BGH, Urteil vom 23. Januar 2003, Az.: III ZR 54/02, DuD 2004, 51.

# 3 Informationspflichten der verantwortlichen Stelle

Die Transparenz der Datenverarbeitung gehört zu den grundlegenden Prinzipien des Datenschutzes. Der Betroffene muss wissen können, wer was über ihn weiß. Diesen Grundsatz hat der Gesetzgeber mit Hilfe einer Reihe von datenschutzrechtlichen Informationspflichten umgesetzt, die jedoch mit anderen Informationspflichten nicht abgestimmt sind und keine Hilfestellung für ihre praktische Umsetzung bieten. Defizitär ist insbesondere die rechtliche Durchsetzung der datenschutzrechtlichen Informationspflichten.

## 3.1 Transparenz als Datenschutzprinzip

Die Transparenz der Datenverarbeitung gehört zu den Grundprinzipien des Datenschutzrechts. Ungeachtet der konkreten Rechtsgrundlage der Datenverarbeitung soll der Betroffene – nach einer Formulierung des Bundesverfassungsgerichts – wissen können, wer was über ihn weiß.[105] Dies gilt nicht nur, wenn die Datenverarbeitung durch eine öffentliche Stelle, sondern auch wenn sie im Rahmen einer Privatrechtsbeziehung erfolgt. § 4 Abs. 2 Satz 1 BDSG statuiert daher den Grundsatz der Direkterhebung beim Betroffenen, aus dem sich zwangsläufig die Verpflichtung zur Information des betroffenen Verbrauchers über Art und Verwendungszwecke der beabsichtigten Datenverarbeitung ergibt.

Eine Verarbeitung personenbezogener Daten ohne eine Mitwirkung des Betroffenen wäre ohne Zweifel nicht nur eine Verletzung dieses Grundsatzes[106], sondern auch eine Verletzung vor- bzw. nebenvertraglicher Pflichten. Die EG-Datenschutzrichtlinie 95/46/EG (EG-DatSchRL) nimmt im Zusammenhang mit den Informationspflichten ausdrücklich auf den in Art. 6 Abs. 1 lit. a) genannten Grundsatz einer Datenverarbeitung unter Beachtung von Treu und Glauben Bezug. Sie setzt voraus, dass „die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden“ (Erwägungsgrund 38).

Der Gesetzgeber ist seiner Verpflichtung nachgekommen, durch entsprechende gesetzliche Regelungen für eine ausreichende Transparenz der Datenverarbeitung gegenüber den Betroffenen zu sorgen. Die Erfüllung der im Gesetz geregelten datenschutzrechtlichen Informationspflichten ist Voraussetzung für die Rechtmäßigkeit der Datenverarbeitung. Dies ergibt sich aus dem für die Konstruktion des Datenschutzrechts zentralen „datenschutzrechtlichen Erlaubnisvorbehalt“. Nach § 4 Abs. 1 BDSG ist eine Datenverarbeitung nur unter den gesetzlich näher bestimmten Voraussetzungen oder auf der Grundlage einer so genannten „informierten Einwilligung“ zulässig. Im ersten Fall sind die gesetzlichen Informationspflichten zu

---

[105] BVerfGE 65, 1 44; Bizer, Datenschutzrechtliche Informationspflichten in: Bäumler/v. Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil 2002, S. 125 ff.

[106] Ausnahmen regelt § 4 Abs. 2 BDSG.

erfüllen. Im zweiten Fall ist die Einwilligung unwirksam, wenn der Betroffene nicht ausreichend über die geplante Verarbeitung informiert wurde.

## 3.2 Systematik der Informationspflichten

Das Datenschutzrecht unterscheidet zwischen der Information des Betroffenen vor seiner Einwilligung (§ 4 a BDSG), der *Unterrichtung* bei einer Datenerhebung *mit Kenntnis des Betroffenen* (§ 4 Abs. 3 BDSG) und der nachträglichen *Benachrichtigung*, wenn die Daten *ohne Kenntnis* des Betroffenen gespeichert wurden (§ 33 Abs. 1 BDSG).

### 3.2.1 Einwilligung

Soll sich die Datenverarbeitung auf eine Einwilligung des Betroffenen stützen, dann ist dieser „auf den vor gesehenen Zweck der Erhebung, Verarbeitung oder Nutzung“ hinzuweisen (§ 4 a Abs. 1 Satz 2 BDSG). Ob sich der Betroffene entscheidet, seine Einwilligung zu erteilen, ist nach dem Leitbild des BDSG davon abhängig, dass ihm ausreichende Informationen über den Zweck der Verarbeitung zur Verfügung stehen.

Eine unzureichende Information wirkt sich unmittelbar auf das Erklärungsbewusstsein des Betroffenen mit der Konsequenz aus, dass seine Einwilligung keine ausreichende Rechtsgrundlage für die Datenverarbeitung bietet.[107] Wegen dieser Konsequenz ist der Betroffene auch nicht nur über den vorgesehenen Zweck, sondern über alle entscheidungsrelevanten Umstände zu informieren, die für die Beurteilung der Datenverarbeitung von Bedeutung sind.[108] Hierzu gehören bspw. Name und Anschrift der verantwortlichen Stelle sowie der Umfang der Datenverarbeitung.[109]

Ferner ist der Betroffene über die Folgen seiner Verweigerung zu unterrichten, soweit dies nach den Umständen des Einzelfalles erforderlich ist, oder wenn er dies verlangt.[110]

### 3.2.2 Gesetzliche Direkterhebung

Werden personenbezogene Daten beim Betroffenen erhoben, dann hat ihn die verantwortliche Stelle nach § 4 Abs. 3 Satz 1 BDSG in Übereinstimmung mit Art. 10 EG-DatSchRL über ihre Identität, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern, soweit der Betroffene mit einer Übermittlung an diese nicht rechnen muss, zu unterrichten. Art und Inhalt der gebotenen Informationen liefern dem Betroffenen damit die Möglichkeit einer ersten Einschätzung der von der verantwortlichen Stelle be-

---

[107] Simitis in: Simitis, BDSG, § 4 a, Rn. 67 ff.

[108] Simitis in: Simitis, BDSG, § 4 a, Rn. 72; Holznagel/Sonntag, Einwilligung des Betroffenen, in: Roßnagel (Hrsg.), HdBDatSchR, Kap. 4.8, Rn. 45.

[109] Holznagel/Sonntag, Einwilligung des Betroffenen in: Roßnagel (Hrsg.), HdBDatSchR, Kap. 4.8, Rn. 45.

[110] Simitis in: Simitis, BDSG, § 4 a, Rn. 70.

absichtigten Datenverarbeitung. Gleichzeitig lässt sich aus den gebotenen Informationen schließen, ob und inwieweit sich die verantwortliche Stelle auf die gesetzlichen Tatbestände einer rechtmäßigen Datenverarbeitung stützt oder ob sie für die Verarbeitung die Einwilligung des Betroffenen benötigt.

Vergleichbare Unterrichtungspflichten gelten nach den Regelungen des TK- und Teledienst-Datenschutzrechts. Nach § 93 Satz 1 TKG haben die Dienstanbieter ihre Kunden „bei Vertragsschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten".

§ 4 Abs. 1 TDDSG[111] verpflichtet die Anbieter von Telediensten, ihre Nutzer zu Beginn des Nutzungsvorganges „über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten" zu unterrichten. Nach derselben Regelung ist der Nutzer auch über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereiches der EG-Datenschutzrichtlinie (sog. „Drittstaaten") zu unterrichten. Eine vergleichbare Drittstaatenregelung fehlt im BDSG.

#### 3.2.2.1 Identität

Die Angabe der Identität der verantwortlichen Stelle nach § 4 Abs. 3 Satz 1 Nr. 1 BDSG korrespondiert mit den meldepflichtigen Angaben über „Name oder Firma der verantwortlichen Stelle", deren „Inhaber, Vorstände, Geschäftsführer" sowie der „Anschrift der verantwortlichen Stelle", die nach § 4 e Satz 1 Nr. 1 bis 3 BDSG in das Verfahrensverzeichnis aufzunehmen sind. Die Informationen des Verfahrensverzeichnisses können bei der Aufsichtsbehörde (§ 38 Abs. 2 Satz 2 BDSG) oder – soweit bestellt – bei dem betrieblichen Datenschutzbeauftragten (§ 4 g Abs. 2 Satz 2 BDSG) von jedermann eingesehen werden. Im Rahmen der Informationspflicht sind gegenüber dem Betroffenen also Angaben zu kommunizieren, die bereits auf Grund der allgemeinen Meldepflicht gegenüber jedermann bereit zu halten sind.

Eine weitere Parallele besteht zwischen der Informationspflicht über die Identität der verantwortlichen Stelle und der Verpflichtung des Anbieters eines Teledienstes oder eines Mediendienstes, den Nutzer über seinen Namen und seine Anschrift zu unterrichten (§ 6 Nr. 1 TDG / § 10 Abs. 1 Nr. 1 MD-StV). Eine vergleichbare Informationspflicht über die Identität des Anbieters findet sich auch im Fernabsatzrecht in § 312 c Abs. 1 BGB i.V.m. § 1 Abs. 1 BGB-InfoV.

#### 3.2.2.2 Zweckbestimmung

Die Information über die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung nach § 4 Abs. 3 Satz 1 Nr. 2 BDSG ist ebenfalls eine Information, die nach § 4 e Satz 1 Nr. 4

[111] In der Neufassung des Elektronischen Geschäftsverkehrsgesetzes (EGG) vom 14. Dezember 2001 (BGBl. I. S. 3721).

BDSG in das Verfahrensverzeichnis aufzunehmen ist. Die Information über die Zweckbestimmung korrespondiert im Übrigen mit der Verpflichtung der Daten verarbeitenden Stelle, bereits „bei der Erhebung" personenbezogener Daten, die Zwecke der Verarbeitung und Nutzung „konkret festzulegen" (§ 28 Abs. 1 Satz 2 BDSG).

#### 3.2.2.3 Kategorien von Empfängern

Der Gesetzgeber hat darauf verzichtet, die verantwortliche Stelle zu verpflichten, den Betroffenen über die Empfänger seiner Daten zu unterrichten. Art. 10 c) der EG-DatSchRL nennt diese Alternative als eine Möglichkeit, um den Betroffenen über Dritte zu informieren, die Kenntnis über seine Daten erhalten. Der deutsche Gesetzgeber hat sich für die zweite Alternative entschieden. Danach ist die verantwortliche Stelle lediglich verpflichtet, „die Kategorien von Empfängern" gegenüber dem Betroffenen zu benennen. Und dies auch nur unter dem Vorbehalt, „soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss" (§ 4 Abs. 3 Satz 1 Nr. 3 BDSG). Auf diese Rückausnahme hat der Gesetzgeber bei den meldepflichtigen Angaben zum Verfahrensverzeichnis verzichtet. Danach sind von der verantwortlichen Stelle ausnahmslos Angaben über „Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können", in das Verfahrensverzeichnis zu stellen (§ 4 e Satz 1 Nr. 6 BDSG).

### 3.2.3 Benachrichtigung

Die Verpflichtung zur Benachrichtigung soll sicherstellen, dass der Betroffene von einer Verarbeitung seiner Daten auch dann erfährt, wenn sie nicht direkt bei ihm erhoben worden sind. § 33 Abs. 1 BDSG setzt insoweit Art. 11 Abs. 1 der EG-DatSchRL um. Allerdings droht die Regelung wegen der zahlreichen Ausnahmen in § 33 Abs. 2 BDSG praktisch ins Leere zu laufen.[112] Der Ausnahmekatalog ist restriktiv auszulegen, weil die Benachrichtigung andernfalls ihre kompensatorische Funktion gegenüber dem Betroffenen als „Vorstufe zum Auskunftsanspruch" nicht erfüllen kann.[113] Ohne Benachrichtigung wüsste der Betroffene nicht einmal, gegenüber wem er seinen Auskunftsanspruch realisieren könnte.

Aber auch die Benachrichtigung über die „Art der Daten" ist für die Wahrnehmung des Auskunftsanspruches nach § 34 Abs. 1 BDSG von Bedeutung, denn nach Satz 2 dieser Regelung soll der Betroffene die Art der Daten, über die Auskunft erteilt werden soll, „näher bezeichnen". Dies kann er nur, wenn er im Fall einer Erhebung bei Dritten von der verantwortlichen Stelle über diese Angaben unterrichtet worden ist.

Die Verpflichtung zur *Benachrichtigung* erstreckt sich im Fall der erstmaligen Speicherung *für eigene Zwecke* auf die Tatsache der Speicherung, die Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle (§ 33 Abs. 1 Satz 1 BDSG). Die Angaben entsprechen bis auf die „Art der Daten" den Anga-

---

[112] Kritisch Wedde, Rechte der Betroffenen in: Roßnagel (Hrsg.), HdBDatSchR, Kap. 4.4, Rn. 29.

[113] Mallmann in: Simitis, BDSG, § 33, Rn. 39; Bergmann/Möhrle/Herb, BDSG § 33, Rn. 76.

ben, die die verantwortliche Stelle im Fall einer Erhebung beim Betroffenen nach § 4 Abs. 3 BDSG zu machen hätte. Jedoch sind auch die „Art der Daten“ Informationen, die von der verantwortlichen Stelle bereits im Rahmen ihrer Meldepflicht als Beschreibung der „Daten und Datenkategorien“, die sich auf die von den automatisierten Verfahren betroffenen Personengruppen beziehen, in das Verfahrensverzeichnis einzustellen sind (§ 4 Satz 1 Nr. 5 BDSG).

Werden die Daten zum Zweck der *geschäftsmäßigen Übermittlung* ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene „von der erstmaligen Übermittlung und der Art der übermittelten Daten“ zu benachrichtigen (§ 33 Abs. 1 Satz 2 BDSG). In beiden Fällen des § 33 Abs. 1 BDSG ist der Betroffene auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss (§ 33 Abs. 1 Satz 3 BDSG).

### 3.2.4 Technikspezifische Unterrichtungspflichten

Besondere Informationspflichten hat der Gesetzgeber festgelegt, wenn aufgrund der Erhebungstechnik spezifische Gefährdungen für das informationelle Selbstbestimmungsrecht der Betroffenen zu befürchten sind. Häufig handelt es sich um technisch unterstützte *heimliche Erhebungstechniken*, von denen der Betroffene ohne eine Unterrichtung gar keine Kenntnis hätte. In diesen Fällen gewährleistet die Unterrichtungspflicht gegenüber den Betroffenen ein informationelles Gleichgewicht, indem sie zumindest über die Tatsache einer heimlichen Erhebung informiert werden.

Das prominenteste Beispiel einer technischen Unterrichtungspflicht betrifft das Setzen von *Cookies* in der Online-Kommunikation. Nach § 4 Abs. 1 Satz 2 TDDSG ist der Nutzer zu Beginn automatisierter Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, über diese zu unterrichten.[114]

Ein weiteres wichtiges Beispiel ist die Unterrichtung über den Umstand einer *Videobeobachtung*, die nach § 6 b Abs. 2 BDSG durch „geeignete Maßnahmen erkennbar zu machen ist“.[115]

Ein weiteres Beispiel ist die Unterrichtung des Betroffenen über Art und Umfang der Datenverarbeitung bei der Verwendung „mobiler personenbezogener Speicher- und Verarbeitungsmedien“ (*Chipkarten*) nach § 6 c Abs. 1 BDSG.[116] Diese Regelung gewinnt im Zusammenhang mit der Verbreitung von RFID eine besondere Bedeutung, jedenfalls soweit es sich um aktive Tags handelt, die selbst personenbezogene Daten verarbeiten können (s.u. S. 78).[117] Nach § 6 c Abs. 1 BDSG ist der Betroffene zu unterrichten über die Identität und

---

[114] Näher Bizer in: Roßnagel (Hrsg.), Recht der Multimediadienste, TDDSG, § 4, Rn. 160 ff.

[115] Näher Bizer in: Simitis, BDSG, § 6 b, Rn. 66.

[116] Näher hierzu Bizer in: Simitis, BDSG, § 6 c, Rn. 22 ff.

[117] Vgl. hierzu Hornung, DuD 2004, 15, 16.

Anschrift der verantwortlichen Stelle, die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten, die Ausübung seiner Rechte auf Auskunft, Berichtigung, Löschung und Sperrung und die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen, soweit der Betroffene nicht bereits Kenntnis erlangt hat.[118]

### 3.2.5 Unterrichtung über Widerspruchsrechte

Ein weiterer Ausdruck der Transparenzpflicht ist der Hinweis an den Betroffenen, dass er über ein spezifisches Widerspruchsrecht gegen einen bestimmten Verwendungszweck seiner Daten verfügt. Das wichtigste Beispiel ist der Widerspruch nach § 28 Abs. 4 Satz 1 BDSG gegen eine Nutzung oder Verarbeitung bereits erhobener Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung. Über dieses Widerspruchsrecht ist der Betroffene nach § 28 Abs. 4 Satz 2 BDSG „bei der Ansprache“ von der verantwortlichen Stelle zu unterrichten. Der Betroffene muss ferner Kenntnis über die Herkunft der Daten erhalten, wenn der Ansprechende sie aus anderen Quellen erhalten hat.

Eine vergleichbare Konstruktion der Unterrichtung über ein Widerspruchsrecht kennt auch § 6 Abs. 3 TDDSG. Danach darf der Dienstanbieter eines Teledienstes Nutzungsprofile unter Verwendung von Pseudonymen für Zwecke der Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste verwenden, sofern der Nutzer nicht widersprochen hat.

Ein weiteres Widerspruchsrecht enthält § 95 Abs. 2 Satz 2 TKG, wonach der Teilnehmer einer Verwendung seiner Bestandsdaten für Zwecke der Werbung und Marktforschung durch seinen Dienstanbieter widersprechen kann, wenn dieser Rufnummer oder (elektronische) Postadresse für die Versendung von Text- oder Bildmitteilungen zu den genannten Zwecken verwenden will. Auf dieses Widerspruchsrecht ist der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung seiner Rufnummer oder Adresse sowie bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse „deutlich sichtbar und gut lesbar“ hinzuweisen (§ 95 Abs. 2 Satz 3 TKG).

Nicht zu verwechseln sind diese Widerspruchsrechte mit dem Recht des Betroffenen, die Rechtmäßigkeit der Verarbeitung seiner Daten überprüfen zu lassen. Art. 14 EG-DatSchRL bezeichnet dieses Recht nach französischem Vorbild ebenfalls als ein Widerspruchsrecht.[119] Etwas versteckt ist es als Prüfungspflicht in § 35 Abs. 5 bzw. § 20 Abs. 5 BDSG aufgenommen worden.[120]

---

[118] Näher in Bizer in: Simitis, BDSG, § 6 c, Rn. 55 f.

[119] Simitis/Dammann, EG-Datenschutzrichtlinie, Art. 14, Erl. 2.

[120] Mallmann in: Simitis, BDSG, § 20, Rn. 80 ff.

## 3.3 Gestaltung

Während das Datenschutzrecht trotz heterogener Begrifflichkeiten über Art und Umfang der Informationen relativ klare Vorstellungen vermittelt, enthält es über die Art und Weise der Gestaltung der Informationen entweder keine oder nur unpräzise Vorgaben.

### 3.3.1 Einwilligung

Während bspw. § 4 a Abs. 1 Satz 3 BDSG für die Einwilligung regelmäßig die Schriftform vorschreibt, fehlt eine entsprechende ausdrückliche Bestimmung für die Gestaltung des Hinweises nach Satz 1 über den „vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung“ derselben Regelung.

Deutlicher ist das Recht der Allgemeinen Geschäftsbedingungen, das in Konstellationen vorformulierter Datenschutzklauseln regelmäßig zu beachten ist.[121] Danach setzt die Geltung Allgemeiner Geschäftsbedingungen das Einverständnis der „anderen Vertragspartei“ voraus (§ 305 Abs. 2 BGB), welches – nicht anders als im Datenschutzrecht – Kenntnis ihres Inhaltes voraussetzt, weil es anders an dem für das Einverständnis konstitutiven Erklärungswillen fehlen würde. Das AGB-Recht verlangt folglich „einen ausdrücklichen Hinweis“ auf die AGB, zumindest aber einen „deutlich sichtbaren Aushang am Ort des Vertragsschlusses“ sowie die Möglichkeit „in zumutbarer Weise (...) von ihrem Inhalt Kenntnis zu nehmen“.

Die Anforderungen an eine „zumutbare Weise“ der Kenntnisnahme muss nunmehr auch eine *körperliche Behinderung* der anderen Vertragspartei berücksichtigen (§ 305 Abs. 2 Nr. 2 BGB), d.h. die Anforderungen richten sich prinzipiell nach dem Empfängerhorizont einer in ihrer Wahrnehmung eingeschränkten Personengruppe. Die Orientierung an einem – wenngleich typisierenden – subjektiven Wahrnehmungshorizont des Empfängers hat seinen tieferen Grund in dem Umstand, dass ohne eine ausreichende Unterrichtung die datenschutzrechtliche Einwilligung keine Rechtsgrundlage für die Datenverarbeitung sein kann.

### 3.3.2 Datenschutzgesetze

Während in den allgemeinen Regelungen über Informationspflichten Hinweise auf ihre Gestaltung fehlen, finden sich zumindest in den neueren Regelungen Zielvorgaben an die Qualität der Unterrichtung. So sind die Betroffenen nach § 6 b Abs. 2 BDSG über eine Videoüberwachung „*in geeigneter Weise*“ zu unterrichten. Über eine Datenverarbeitung mit Hilfe von Chipkarten sind die Betroffenen nach § 6 c Abs. 1 Nr. 2 BDSG, „*in allgemein verständlicher Form“* über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten zu unterrichten.

---

[121] Vgl. bspw. zuletzt LG München vom 01.02.2001, DuD 2001, 292, 294 – Payback; Holznagel/Sonntag, Einwilligung des Betroffenen in: Roßnagel (Hrsg.), HdBDatSchR, Kap. 4.8., Rn. 58 ff.

Nach § 93 Satz 1 TKG sollen die Teilnehmer „in allgemein verständlicher Form“ Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Zudem sind die Nutzer nach derselben Regelung (§ 93 Satz 2 TKG), „durch *allgemein zugängliche* Informationen“ über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten.

### 3.3.3 E-Commerce und Fernabsatz

Aussagekräftiger sind die Gestaltungsanforderungen an die Verbraucherinformationen nach dem Recht des Fernabsatzes und des E-Commerce.[122] Nach § 312 c Abs. 1 BGB in der Fassung des Gesetzes zur Modernisierung des Schuldrechts hat der Unternehmer den Verbraucher „*klar und verständlich*“ rechtzeitig vor Abschluss eines Fernabsatzvertrages, in einer dem eingesetzten Fernkommunikationsmittel entsprechenden Weise, über Einzelheiten des Vertrages zu informieren.

Eine vergleichbare Regelung enthält § 312 e Abs. 1 Nr. 2 BGB für Verträge im elektronischen Geschäftsverkehr. In einer Rechtsverordnung sind näher bestimmte Informationen dem Verbraucher spätestens bei Lieferung der Ware in Textform mitzuteilen (§ 312 c Abs. 2 BGB). Die auf der Rechtsgrundlage des Art. 240 f. des EG BGB erlassene BGB-Informationspflichten-Verordnung vom 2. Januar 2002[123] präzisiert diese Anforderungen allerdings nicht weiter und verweist in § 1 Abs. 2 auf die Textform nach § 126 b BGB. Eine Harmonisierung der Informationspflichten nach dem Recht des Fernabsatzes und des E-Commerce mit denen des Datenschutzrechtes hat der Gesetzgeber bislang leider nicht als Aufgabe begriffen.[124]

[122] Mit dem Gesetz zur Modernisierung des Schuldrechts vom 26. November 2001 (BGBl. I S. 3138) sind diese Regelungen in das BGB integriert worden.

[123] BGBl. I S. 342.

[124] Vgl. Bizer, DuD 2001, 274, 275.

# 4 Rechte des Betroffenen

Zu den datenschutzrechtlichen Transparenzregelungen gehören die Rechte der Betroffenen. Während bei den Informationspflichten die verantwortliche Stelle von sich aus die Betroffenen unterrichten muss, gewährt das Datenschutzrecht den Betroffenen auch eigene Initiativrechte, mit denen sie sich Kenntnis von einer Verwendung ihrer Daten verschaffen oder dieser widersprechen kann. Die Transparenzregeln haben ihren Rechtsgrund im Ausgleich, der Verfügungsmöglichkeiten und Informationen über eine heimliche Verarbeitung personenbezogener Daten. Die Transparenzregeln sollen es den Betroffenen ermöglichen, zu wissen, wer was über sie weiß. Darüber hinaus versetzen sie in die Lage, die rechtliche Legitimation ihrer Datenverarbeitung zu hinterfragen.

## 4.1 Auskunftsrecht

Das Auskunftsrecht ist ein zentraler Bestandteil des Rechts auf informationelle Selbstbestimmung. Das Bundesverfassungsgericht hat im Volkszählungsurteil dem Einzelnen das Recht zugesprochen zu wissen, „wer was wann und bei welcher Gelegenheit über (ihn) weiß“[125].[126] Es hat darüber hinaus die Aufgabe, dem Betroffenen „handlungsvorbereitendes Wissen“ für sein weiteres Handeln gegenüber der verantwortlichen Stelle zu vermitteln.[127] Darüber hinaus ist das Wissen um die Verwendung seiner Daten für den Betroffenen auch von Bedeutung, um die Art und den Umfang, seine Daten gegenüber Dritten zu offenbaren, zu gestalten bzw. zu verändern.

*Anspruchsgegner* ist die verantwortliche[128] nicht-öffentliche Stelle, die im Sinne von § 3 Abs. 7 BDSG personenbezogene Daten für sich erhebt, verarbeitet oder nutzt oder im Auftrag durch andere verarbeiten lässt.

Das Recht auf Auskunft ist unabdingbar, d.h. es kann nicht zu Lasten des betroffenen Verbrauchers durch ein Rechtsgeschäft ausgeschlossen werden.[129] Voraussetzung für die Auskunftserteilung ist allein das Auskunftsverlangen des Betroffenen.[130] Darüber hinaus muss der Betroffene kein besonderes oder rechtliches Interesse nachweisen, um seinen Auskunftsanspruch geltend zu machen.[131]

---

[125] BVerfGE 65, 1, 43.

[126] Das Recht auf informationelle Selbstbestimmung hat nach BVerfGE 84, 192, 194 f. auch Ausstrahlungswirkung im privatrechtlichen Bereich.

[127] Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5; Rn. 82; AG Altona, DuD 2005, 171; LG Ulm, DuD 2005, 102.

[128] i.S.d. § 3 Abs. 7 BDSG.

[129] § 6 Abs. 1 BDSG.

[130] Das Auskunftsrecht steht nur dem Betroffenen und nicht anderen Personen zu Mallmann in: Simitis, BDSG, § 34, Rn. 11.

[131] Mallmann in: Simitis, BDSG, § 34, Rn. 9; LG Ulm, DuD 2005, 100, 101.

### 4.1.1 Inhalt des Auskunftsanspruches

Werden personenbezogene Daten von einer nicht-öffentlichen Stelle verarbeitet und gespeichert, kann der Betroffene nach § 34 BDSG *Auskunft* über die zu seiner Person gespeicherten Daten, deren Herkunft (§ 34 Abs. 1 Satz Nr. 1 BDSG), die Empfänger, an die die Daten weitergegeben wurden (Nr. 2) ,und den Zweck der Speicherung (Nr. 3) verlangen.[132] Werden die Daten zu verschiedenen Zwecken gespeichert, sind alle Zwecke anzugeben.[133]

Der Auskunftsanspruch des Betroffenen über Empfänger und Verwendungszweck der Daten entspricht seinem Umfang nach der Verpflichtung der verantwortlichen Stelle, nach § 4 Abs. 3 BDSG den Betroffenen bei der Erhebung (s.o. S. 46) bzw. nach § 33 Abs. 1 BDSG nachträglich zu benachrichtigen (s.o. S. 48).

#### 4.1.1.1 Umfang

Der Anspruch umfasst alle[134] zur Person des Betroffenen gespeicherten personenbezogenen[135] Daten. Dazu gehören auch die Dateibezeichnungen und u.U. auch physisch nicht gespeicherte Angaben wie bspw. Verfahrensüberschriften.[136] Auch die Tatsache, dass keine personenbezogenen Daten gespeichert sind, unterliegt dem Auskunftsanspruch.[137]

Der datenschutzrechtliche Auskunftsanspruch bezieht sich grundsätzlich nur auf Daten in automatisierten Dateien bzw. auf solche, die aus solchen Dateien stammen (§ 3 Abs. 2 Satz 2 BDSG).[138] Angesichts der Bedeutung der automatisierten Datenverarbeitung durch Textverarbeitungsprogramme oder elektronische Adressbücher, werden auch in Akten oder Handkarteien befindliche personenbezogene Daten regelmäßig aus einer automatisierten Datei stammen. Darüber hinaus gilt jedoch, dass Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Auskunftsteilung speichern, immer Auskunft über die Daten des Betroffenen zu erteilen haben, auch wenn sie ausschließlich in einer Schriftakte oder

---

[132] Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten anzuwenden sind, gehen sie nach § 1 Abs. 3 BDSG den Vorschriften des BDSG vor.

[133] Bergmann/Möhrle/Herb, BDSG § 34, Rn. 44; Mallmann in: Simitis, BDSG, § 34, Rn. 27.

[134] Auch bei einer wiederholten Anfrage erstreckt sich das Auskunftsrecht auf alle gespeicherten Daten. Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 17.

[135] Vgl. BGH, NJW 1981, 1738.

[136] Siehe dazu Dammann in: Simitis, BDSG, § 3, Rn. 125, der eine physische Speicherung nicht für begriffsnotwendig hält. So genüge bereits die „Wiedergewinnbarkeit der Information unter Anwendung der im vorhandenen Kontext bestehenden Regeln“ wie dies bspw. bei Datei- und Verfahrensüberschriften der Fall sei, da sie in der Regel ein Selektionskriterium (z.B. „Schlechte Zahler“) bilden.

[137] Mallmann in: Simitis, BDSG, § 34, Rn. 14.

[138] LG Ulm, DuD 2005, 100, 101.

Kartei abgelegt sind.[139] Grund für diese Erweiterung ist das bei diesem Verwendungszweck erhöhte Risiko einer rechtswidrigen Verarbeitung personenbezogener Daten.[140] Im Übrigen ist zu beachten, dass der Betroffene einen Auskunftsanspruch auch außerhalb des Anwendungsbereiches des BDSG aus § 1004 BGB geltend machen kann.[141]

#### 4.1.1.2 Herkunft und Empfänger

Nach § 34 Abs. 1 Satz 1 Nr. 1 BDSG ist die *Herkunft* der zur Person des Betroffenen gespeicherten Daten mitzuteilen. Auf diese Weise kann der Betroffene auch die Rechtmäßigkeit einer Übermittlung seiner Daten überprüfen.

Darüber hinaus kann der Betroffene Auskunft über die Empfänger oder Kategorien von *Empfängern* verlangen, an die Daten weitergegeben werden (§ 34 Abs. 1 Nr. 2 BDSG). Es ist also nicht nur Auskunft zu erteilen, an wen bislang personenbezogene Daten des Betroffenen übermittelt worden sind, sondern auch an wen zukünftig seine Daten weitergegeben „werden". Lassen sich die zukünftigen Empfänger nicht konkret benennen, so sind nach dem Wortlaut des Gesetzes zumindest die „Kategorien von Empfängern, an die Daten weitergegeben werden", zu benennen. Mit dieser Verpflichtung korrespondiert die Verpflichtung der verantwortlichen Stelle aus § 28 Abs. 1 Satz 2 BDSG, bereits bei der Erhebung personenbezogener Daten festzulegen, zu welchen konkreten Zwecken sie die Daten verwenden wird. Diese Regelung unterbindet die Ausrede, über eine zukünftige Verwendung keine Aussage treffen zu können.

Die verantwortliche Stelle ist verpflichtet, die Informationen über die Empfänger vorzuhalten, um Betroffenen Auskunft erteilen zu können.[142]

#### 4.1.1.3 Einschränkung bei überwiegenden Geschäftsgeheimnissen

Inhaltlich eingeschränkt wird der Auskunftsanspruch auf Herkunft und Empfänger gegenüber Stellen, die personenbezogene Daten geschäftsmäßig *zum Zwecke der Übermittlung* verarbeiten. Diese Einschränkungen sind nicht unproblematisch, weil die Betroffenen gerade bei einer Verbreitung ihrer Daten an Dritte ein besonderes Interesse daran haben, Herkunft und Empfänger dieser Daten in Erfahrung zu bringen. Neben dem schlichten Wissen um diese Informationen können die Daten auch unvollständig oder falsch sein, so dass der Betroffene aus diesem Grund ein besonderes schutzwürdiges Interesse hat, Herkunft und Empfänger seiner Daten in Erfahrung zu bringen.[143]

---

[139] Auernhammer, BDSG 90, § 34, Rn. 8; Mallmann in: Simitis, BDSG, § 34, Rn. 28; LG Ulm, DuD 2005, 100, 102.

[140] Mallmann in: Simitis, BDSG, § 34, Rn. 28.

[141] Mallmann in: Simitis, BDSG. § 34, Rn. 26.

[142] Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 19.

[143] Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5; Rn. 82; AG Altona, DuD 2005, 171.

Nach § 34 Abs. 1 Satz 3 BDSG kann der Betroffene von solchen Stellen Auskunft über *Herkunft und Empfänger* seiner Daten nur verlangen, „sofern nicht das Interesse der an der Wahrung des Geschäftsgeheimnisses überwiegt". Diese Einschränkung des Auskunftsanspruches kann allerdings von der verantwortlichen Stelle nicht für die Auskunft über Kategorien der Empfänger im Sinne von § 34 Abs. 1 Nr. 2 BDSG in Anspruch genommen werden.[144] Über diese ist in jedem Fall Auskunft zu erteilen. Eine gleich lautende Ausnahmeregelung gilt nach § 34 Abs. 2 Satz 2 BDSG. Auf diese Ausnahmen können sich bspw. Auskunfteien beziehen, aber auch Unternehmen, die die Überprüfung personenbezogener Daten gegenüber Dritten für Zwecke der Bonität oder zur Erstellung eines Kreditscoring anbieten und hierzu personenbezogene Daten als Geschäftszweck übermitteln.

Die Formulierung des Gesetzes macht allerdings deutlich, dass die Auskunftsverweigerung unter Berufung auf das *Geschäftsgeheimnis* von dem Gesetzgeber als Ausnahme gedacht ist. Sie ist aus diesem Grund auch eng auszulegen.[145] Im Übrigen ist ein allgemeines Geschäftsinteresse an der Geheimhaltung der Datenquellen nicht ausreichend, sondern es bedarf eines darüber hinausgehenden Geheimhaltungsinteresses.[146] So genügt eine gegenüber der Datenquelle bestehende vertragliche Geheimhaltungsverpflichtung nicht, um ein überwiegendes Interesse an der Geheimhaltung zu begründen.[147] Das Geheimhaltungsinteresse kann auch nicht überwiegen, wenn begründete Zweifel an der Richtigkeit der Daten des Betroffenen bestehen.[148]

### 4.1.2 Konkretisierung des Auskunftsbegehrens

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen (§ 34 Abs. 1 Satz 2 BDSG).

Die vom Gesetzgeber als *Sollvorschrift* ausgestaltete Regelung soll verhindern, dass bei einem zu allgemein formulierten Auskunftsverlangen die Auskunft von der verarbeitenden Stelle verweigert wird. Sie gibt ihr jedoch das Recht, von dem Betroffenen eine Konkretisierung seines Auskunftsbegehrens zu verlangen.[149] Ausreichend für diese Konkretisierung ist, wenn der Betroffene angibt, in welchem sachlichen oder zeitlichen Zusammenhang er mit der verarbeitenden Stelle in Kontakt getreten ist und daher mit einer Speicherung seiner Daten rechnet. Der Auskunftsanspruch wird jedoch nicht ausgeschlossen, wenn der Betroffene sein Auskunftsbegehren nicht konkretisieren kann. Kann oder will der Betroffene sein Auskunftsbegehren nicht konkretisieren, so hat die verantwortliche Stelle gleichwohl eine umfas-

---

[144] Mallmann in: Simitis, BDSG, § 34, Rn. 21.

[145] AG Altona, DuD 2005, S. 170.

[146] AG Altona, DuD 2005, 170.

[147] Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5; Rn. 82; AG Altona, DuD 2005, 171; LG Ulm, DuD 2005, 100, 102.

[148] Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5; Rn. 82.

[149] Gola/Schomerus, BDSG § 34, Rn. 5.

sende Auskunft zu erteilen.[150] Unter den Bedingungen der automatisierten Datenverarbeitung mit leistungsfähigen Suchprogrammen wird sich der Aufwand jedoch in Grenzen halten.

### 4.1.3 Form- und Fristfragen

Da das Gesetz keine besondere Form für das *Auskunftsverlangen* vorsieht, kann die Anfrage schriftlich, mündlich bzw. telefonisch oder elektronisch gestellt werden.[151]

Die *Auskunft* ist grundsätzlich schriftlich[152] zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist (§ 34 Abs. 3 BDSG). Sie ist so abzufassen, dass der Inhalt vom Betroffenen ohne besondere Vorkenntnisse verstanden werden kann.[153] Besondere Umstände liegen bspw. vor, wenn der Betroffene sich aus Zeitgründen mit einer mündlichen Auskunft oder der Einsichtnahme begnügt.[154] Sie liegen nicht schon dann vor, wenn sie bei der verarbeitenden Stelle Schwierigkeiten oder Kosten verursachen, da diese nach § 9 BDSG verpflichtet ist, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine schriftliche Auskunftserteilung sicherzustellen.[155]

Das Gesetz sieht keine Frist vor, innerhalb derer die Auskunft zu erteilen ist. Allerdings ergibt sich aus dem Schutzzweck der Norm, das nur eine schnelle Auskunftserteilung das Risiko einer unrichtigen Datenübermittlung reduzieren kann. Als angemessen wird eine Frist von ein bis drei Wochen erachtet.[156]

Der Betroffene ist von der verantwortlichen Stelle zu identifizieren, bevor ihm die Auskunft erteilt wird. Diese Anforderung ergibt sich aus dem Verbot, Daten unbefugt zu übermitteln.[157] Es sind stets Vorkehrungen zu treffen, die eine Kenntnisnahme des Auskunftsinhaltes von Dritten verhindern.[158] Hierzu ist es ausreichend, wenn die Auskunft an die Anschrift erteilt wird, die die verantwortliche Stelle zu dem Datensatz gespeichert hat.

---

[150] Mallmann in: Simitis, BDSG, § 34, Rn. 31; Gola/Schomerus, § 34, Rn. 6.

[151] Mallmann in: Simitis, BDSG, § 34, Rn. 10.

[152] Es sind für die Schriftform die gesetzlichen Anforderungen nach § 126 BGB zu beachten. Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 39.

[153] S. Art. 12 Buchst. a) zweiter Spiegelstrich EG-Datenschutzrichtlinie 95/46/EG, wonach die Mitteilung „in verständlicher Form“ erfolgen muss.

[154] Auch für die mündliche Auskunft gelten die übrigen gesetzlichen Anforderungen. Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 44.

[155] Mallmann in: Simitis, BDSG, § 34, Rn. 41 m.w.N.

[156] Vgl. Gola/Schomerus, BDSG § 34, Rn. 26 und Mallmann in: Simitis, BDSG, § 34, Rn. 32: bis zwei Wochen; Dörr/Schmidt, Neues BDSG, 2. Aufl. 1992, § 34, Rn. 16: bis drei Wochen.

[157] So ist bei einer schriftlichen Anfrage die Absenderangabe mit der gespeicherten Adresse abzuklären und gegebenenfalls Nachweis der Identität des Betroffenen zu verlangen. Bei einem telefonischen Auskunftsersuchen ist ein Rückruf nach erfolgter Überprüfung der Telefonnummer erforderlich. Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 34.

[158] So sind schriftliche Auskünfte im verschlossenen Briefumschlag zu versenden. Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 34.

Der Betroffene ist von einer Ablehnung seines Auskunftsersuchens zu informieren.[159]

### 4.1.4 Ausnahmen

Eine Auskunftspflicht besteht nicht, wenn der Betroffene über die Verarbeitung seiner Daten auch nicht nachträglich von der verantwortlichen Stelle zu benachrichtigen ist (§ 34 Abs. 4 BDSG). Dies ist nach der Bezugsnorm der Fall, wenn

- die Daten nur deshalb gespeichert sind, weil sie aufgrund einer gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsvorschrift nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde (§ 33 Abs. 2 Nr. 2 BDSG)
  (Aus dieser Ausnahme folgt jedoch nicht, dass gesperrte Daten grundsätzlich dem Auskunftsanspruch entzogen sind.[160] Das Gegenteil ist der Fall. Um diese Ausnahme gegenüber dem Auskunftsanspruch geltend machen zu können, muss die Auskunft zusätzlich einen unverhältnismäßigen Aufwand erfordern.),
- die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen (§ 33 Abs. 2 Nr. 3 BDSG)
  (Nach der Rechtsprechung ist allein die Zusicherung der Vertraulichkeit gegenüber der Informationsquelle kein ausreichender Grund, den Auskunftsanspruch zu verweigern.[161]),
- die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist (…) (§ 33 Abs. 2 Nr. 5 BDSG),
- die zuständige Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde (§ 33 Abs. 2 Nr. 6 BDSG) oder
- die Daten für eigene Zwecke gespeichert sind und

  a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder

  b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt (§ 33 Abs. 2 Nr. 7 BDSG).
  Ein Beispiel für die erste Alternative sind Informationen, die aus dem Gewerbezentralre-

[159] Mallmann in: Simitis, BDSG, § 34, Rn. 3.

[160] AG Altona, DuD 2005, 170, 171.

[161] Siehe oben Fn. 147 f.

gister entnommen worden sind.[162] Für die zweite Alternative kann auf die Rechtsprechung zur Auskunftsverweigerung unter Berufung auf die Vertraulichkeit des Informanten bzw. der Datenquelle Bezug genommen werden.[163]

Die Ablehnung ist von der verarbeitenden Stelle schriftlich unter Nennung der zugrunde liegenden Rechtsvorschrift zu begründen, um sich ggf. an die Aufsichtsbehörde wenden oder um gerichtlichen Rechtsschutz nachsuchen zu können.[164] Der Betroffene muss daraus erkennen können, dass Daten über ihn gespeichert sind und dass nach Auffassung der verarbeitenden Stelle ein Ausnahmetatbestand vorliegt.

### 4.1.5 Kosten

Die Auskunftserteilung[165] ist nach § 34 Abs. 5 Satz 1 BDSG grundsätzlich unentgeltlich.

Werden die personenbezogenen Daten jedoch geschäftsmäßig zum Zwecke der Übermittlung gespeichert und kann der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen, so kann nach § 34 Abs. 5 Satz 2 BDSG ein Entgelt erhoben werden.[166] Dies wird bspw. angenommen, wenn die Auskunft über die Bonität gegenüber einem Kreditgeber Voraussetzung seiner Kreditprüfung ist.[167] Die Entgeltlichkeit wird damit begründet, dass im Fall der Kostenlosigkeit die Kreditgeber sich die Auskünfte kostenlos ausschließlich über ihre potenziellen Kreditnehmer besorgen würden. Die Entgeltlichkeit derartiger Auskünfte soll mit anderen Worten wirtschaftliche Nachteile von den Auskunfteien abwenden.[168]

Das Entgelt darf nach § 34 Abs. 5 Satz 3 BDSG über die durch die Auskunftserteilung entstandenen Kosten nicht hinausgehen.[169] Ein Entgelt darf nicht erhoben werden, wenn besondere Umstände[170] die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden oder die Auskunft ergibt, dass die Daten zu berichtigen oder zu löschen sind, § 34 Abs. 5 Satz 4 BDSG.

---

[162] AG Bad Schwartau, DuD 2005, 372 f. Die Information aus dem Gewerbezentralregister setzt zwar nach § 14 Abs. 8 GewO ein berechtigtes Interesse an der Auskunft voraus, die Allgemeinzugänglichkeit der Daten hat das Gericht in dem Streitfall aber auch aus der Verpflichtung zur Angabe entsprechender Informationen auf den Geschäftsbriefen nach § 35 a Abs. 1 GmbHG abgeleitet.

[163] Siehe oben Fn. 147 f.

[164] Mallmann in: Simitis, BDSG, § 34, Rn. 47.

[165] Zur Auskunft gehört auch die Negativauskunft. Vgl. Mallmann in: Simitis, § 34, Rn. 57.

[166] Wird die Auskunftserteilung verweigert kann ein Entgelt nicht erhoben werden, auch wenn die Bearbeitung Kosten verursacht hat. Vgl. dazu Mallmann in: Simitis, BDSG, § 34, Rn. 57.

[167] Mallmann in: Simitis, BDSG, § 34, Rn. 51; Gola/Schomerus, BDSG, § 34, Rn. 21.

[168] Mallmann in: Simitis, BDSG, § 34, Rn. 51.

[169] Eine SCHUFA-Auskunft kostet derzeit 7,60 €.

[170] Besondere Umstände liegen vor, „wenn konkrete, auf Tatsachen beruhende Anhaltspunkte für die Unrichtigkeit oder die Unzulässigkeit der Speicherung bestehen“. Mallmann in: Simitis, BDSG, § 34, Rn. 62.

Will der Betroffene die Auskunft nicht wirtschaftlich nutzen, so kann er von der verarbeitenden Stelle eine unentgeltliche Auskunft in einer wirtschaftlich nicht verwertbaren Form[171] verlangen.[172]

Ist die Auskunftserteilung nicht unentgeltlich (§ 34 Abs. 5 Satz 2 BDSG), so hat der Betroffene nach § 34 Abs. 6 BDSG das Recht auf persönliche Kenntnisverschaffung (z.B. Bildschirmanzeige und Akteneinsicht). Die Kenntnisnahme ist dem Betroffenen möglichst ortsnah anzubieten.[173] Der Betroffene ist auf dieses Recht vor entgeltlicher Auskunftserteilung hinzuweisen. Eine solche Einsicht ist jedoch angesichts des zeitlichen und kostenmäßigen Zeitaufwandes wenig praktikabel.

### 4.1.6 Auskunftsrechte nach BGB und HGB

Auskunftsrechte des Betroffenen entstehen nach Treu und Glauben, wenn in einem bestehenden Rechtsverhältnis der Berechtigte unverschuldet über Bestehen und Umfang eines Rechts im Ungewissen und der Verpflichtete in der Lage ist, die zur Beseitigung der Ungewissheit erforderliche Auskunft zu geben.[174] Treu- und Glaubenreglungen finden sich sowohl im Bürgerlichen Gesetzbuch (BGB) als auch in handels- und gesellschaftlichen Regelungen.[175]

Eine unzulässige Übermittlung personenbezogener Daten stellt nach Rechtsprechung des BGH einen Eingriff in das allgemeine Persönlichkeitsrecht des Betroffenen dar, der in entsprechender Anwendung des § 1004 BGB einen Anspruch auf Benennung des Datenempfängers gegen die verarbeitende Stelle hat.[176]

### 4.1.7 Auskunftsrecht nach § 7 TDDSG

Einen speziellen Auskunftstatbestand enthält das Datenschutzrecht für Online-Dienste. Als Nutzer eines Teledienstes ist der Betroffene nach § 7 TDDSG berechtigt, jederzeit die zu seiner Person oder seinem Pseudonym gespeicherten Daten unentgeltlich beim Dienstanbieter einzusehen oder sich die Auskunft elektronisch erteilen zu lassen. Entsprechendes ergibt sich allerdings auch aus dem Auskunftsanspruch nach § 34 Abs. 1 BDSG. Denn

---

[171] Die wirtschaftliche Verwertbarkeit kann durch einen entsprechenden Zusatz, der die Vorlage Dritten gegenüber untersagt, oder durch fehlende Urkundsqualität erreicht werden. Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 52.

[172] Mallmann in: Simitis, BDSG, § 34, Rn. 52.

[173] Mallmann in: Simitis, BDSG, § 34, Rn. 68.

[174] Palandt/Heinrichs, BGB § 261, Rn. 8.

[175] Bspw. § 259 f., 666, 810, 1379 BGB; 118, 166 HGB; im Einzelnen s. dazu Palandt/Heinrichs, BGB § 261, Rn. 3 ff.

[176] BGH, NJW 1984, 1886, 1887.

pseudonymisierte Daten gelten als personenbeziehbare Daten, weil sich über die Zuordnungsliste die Pseudonyme auf die Klarnamen zurückführen lassen.[177]

## 4.2 Einsicht in das Verfahrensverzeichnis

In der Praxis von geringer Bedeutung, weil kaum einem Verbraucher bekannt ist, dass er über dieses Recht verfügt, ist die Möglichkeit, Einsicht in das von der verantwortlichen Stelle zu führende Verfahrensverzeichnis (§ 4 e Satz 1 BDSG) zu nehmen. Nach § 4 g Abs. 2 Satz 1 BDSG hat der betriebliche Datenschutzbeauftragte „auf Antrag jedermann" die Angaben aus dem Verfahrensverzeichnis „in geeigneter Weise" zugänglich zu machen.[178]

Hat die verantwortliche Stelle keinen betrieblichen Datenschutzbeauftragten, dann sind die Angaben des Verfahrensverzeichnisses an die zuständige Aufsichtsbehörde zu melden (§ 4 d Abs. 1 BDSG), die diese Informationen mit Ausnahme von sicherheitsrelevanten Details in einem Register führt, das „von jedem eingesehen werden kann" (§ 38 Abs. 2 BDSG).

Sinn und Zweck des Verfahrensverzeichnisses ist die Übersicht über die wesentlichen Merkmale der personenbezogenen Datenverarbeitung in der verantwortlichen Stelle selbst, aber auch gegenüber der Aufsichtsbehörde (s.u. S. 156).

## 4.3 Berichtigung, Löschung und Sperrung von Daten

Die Rechte auf Berichtigung, Löschung und Sperrung von Daten gehören zum Recht auf informationelle Selbstbestimmung. Löschung und Sperrung dienen zur Umsetzung des Grundsatzes der Erforderlichkeit der Datenverarbeitung: Werden die personenbezogenen Daten nicht mehr benötigt, so sind sie zu löschen oder zu sperren. Der Berichtigungsanspruch stellt die „Qualität" der Daten sicher und schützt den Betroffenen vor der Verarbeitung unrichtiger Daten. Die Rechte auf Berichtigung, Löschung oder Sperrung sind wie das Auskunftsrecht unabdingbare Rechte im Sinne von § 6 Abs. 1 BDSG, die durch ein Rechtsgeschäft nicht ausgeschlossen oder beschränkt werden können.

Den Rechten des Betroffenen korrespondieren die entsprechenden Pflichten der verantwortlichen Stelle, personenbezogene Daten unter den Voraussetzungen des Gesetzes zu berichtigen, zu löschen bzw. zu sperren. Diese Verpflichtung besteht unabhängig davon, ob der Betroffene seinen Anspruch gegenüber der verantwortlichen Stelle geltend macht. So hat die verantwortliche Stelle nach § 35 Abs. 1 BDSG von sich aus falsche Daten zu berichtigen.[179] Ebenso ist sie nach § 35 Abs. 2 BDSG verpflichtet, die personenbezogenen Daten zu löschen bzw. zu sperren, wenn sie nicht mehr erforderlich sind.[180]

---

[177] Bizer in: Simitis, BDSG, § 3, Rn. 223.

[178] Zu den einschränkenden Voraussetzungen siehe Simitis in: Simitis, BDSG, § 4 g, Rn. 73 ff.

[179] Mallmann in: Simitis, BDSG, § 35, Rn. 7.

[180] Mallmann in: Simitis, BDSG, § 35, Rn. 20.

Darüber hinaus hat die verantwortliche Stelle eine so genannte Nachberichtspflicht nach § 35 Abs. 7 BDSG. Danach hat die verantwortliche Stelle die Stellen von der Berichtigung, Sperrung oder Löschung personenbezogener Daten zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden. Diese Nachberichtspflicht besteht nicht, wenn sie einen unverhältnismäßigen Aufwand bedeutet[181] und schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Bei der verantwortlichen Stelle entstehende Kosten muss diese selbst tragen; sie sind nicht vom Betroffenen zu erstatten.

### 4.3.1 Berichtigung von Daten

Unrichtige Daten sind nach § 35 Abs. 1 BDSG unabhängig von einem Ersuchen des Betroffenen zu berichtigen.[182] Daten sind unrichtig, wenn „die Information, welche die einzelnen Angaben über die persönlichen oder sachlichen Verhältnisse des Betroffenen vermitteln, mit der Realität nicht übereinstimmt“ oder „die durch sie vermittelte Information unvollständig ist oder wenn durch Verwendung – für sich genommen richtiger – Daten durch Verwendung in einem anderen Zusammenhang ein falsches Gesamtbild entsteht (Kontextverlust)“.[183] Eine Berichtigung liegt vor, wenn die Daten wieder im Einklang mit den tatsächlichen Verhältnissen stehen.

Wird die Richtigkeit von personenbezogenen Daten bestritten, ohne dass sich feststellen lässt, ob die Daten richtig oder falsch sind, dann sind die Daten nach § 35 Abs. 4 BDSG zu sperren. Eine Sonderregelung besteht nach § 35 Abs. 6 BDSG für die Stellen, die personenbezogene Daten zum Zweck der Übermittlung verarbeiten. Diese müssen die personenbezogenen Daten, die aus allgemein zugänglichen Quellen stammen und zu Dokumentationszwecken gespeichert sind, nicht sperren, wenn sie unrichtig sind oder ihre Richtigkeit bestritten worden ist. In diesen Fällen ist jedoch den Daten auf Verlangen des Betroffenen für die Dauer ihrer Speicherung eine Gegendarstellung beizufügen, ohne die sie nicht übermittelt werden dürfen.

### 4.3.2 Löschung von Daten

Löschen ist nach der Legaldefinition des § 3 Abs. 4 Nr. 5 BDSG das Unkenntlichmachen gespeicherter personenbezogener Daten. Die verantwortlichen Stellen dürfen personenbezogene Daten nach § 35 Abs. 2 Satz 1 BDSG jederzeit löschen, es sei denn, es stehen gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegen, oder es besteht Grund zu der Annahme, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden (§ 35 Abs. 3 Nr. 1 und 2 BDSG). Letzteres ist insbesondere

---

[181] Unverhältnismäßig ist der Aufwand bei gänzlich belanglosen Korrekturen. Mallmann in: Simitis, BDSG, § 20, Rn. 96.

[182] Mallmann in: Simitis, BDSG, § 35, Rn. 7.

[183] Mallmann in: Simitis, BDSG, § 35, Rn. 7.

dann der Fall, wenn eine Löschung dazu führen würde, dass die ansonsten zulässigerweise gespeicherten personenbezogenen Daten unrichtig bzw. unvollständig werden.[184] In diesen Fällen ist eine Löschung nur zulässig, soweit der Betroffene in sie eingewilligt hat oder eine andere Rechtsvorschrift die Löschung vorschreibt oder erlaubt.[185]

Eine Löschungspflicht besteht unabhängig von einem Löschungsbegehren des Betroffenen und ist unverzüglich vorzunehmen.[186] Der Betroffene kann nach § 34 BDSG Auskunft verlangen, ob die Löschung durchgeführt worden ist.

Die verarbeitende Stelle hat die personenbezogenen Daten nach § 35 Abs. 2 Satz 2 BDSG zu löschen, wenn

1. ihre Speicherung unzulässig[187] ist,
2. es sich um Daten über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerfristige Speicherung nicht erforderlich ist.

Im Verfahrensverzeichnis hat die verantwortliche Stelle Angaben über die „Regelfristen für die Löschung“ zu machen (§ 4 e Satz 1 Nr. 7 BDSG).

### 4.3.3 Sperrung von Daten

An die Stelle einer Löschung tritt nach § 35 Abs. 3 BDSG eine Sperrung der personenbezogenen Daten. Die Sperrung bewirkt ein „relatives Nutzungsverbot“ der Daten.[188] Sie sind noch vorhanden, dürfen aber nicht verwendet werden. Die Sperrung erfolgt soweit

1. gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen[189] des Betroffenen beeinträchtigt würden, oder

---

[184] Vgl. Mallmann in: Simitis, BDSG, § 35, Rn. 17.

[185] Mallmann in: Simitis, BDSG, § 35, Rn. 18.

[186] Mallmann in: Simitis, BDSG, § 35, Rn. 20.

[187] Unzulässig ist die Speicherung, wenn weder der Betroffene in die Speicherung eingewilligt hat noch diese nach § 28 oder § 29 BDSG oder einer anderen Rechtsvorschrift zulässig ist. Maßgeblich ist die gegenwärtige Sach- und Rechtslage. Mallmann in: Simitis, BDSG, § 35, Rn. 21.

[188] Mallmann in: Simitis, BDSG, § 35, Rn. 39.

[189] Der Begriff ist weit auszulegen. Es ist in jedem Einzelfall zu prüfen, ob dem Betroffenen durch die Löschung Nachteile entstehen. S. Mallmann in: Simitis, BDSG, § 35, Rn. 41.

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Gesetzliche Aufbewahrungspflichten ergeben sich aus dem Handelsrecht nach § 257 HGB für Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Lageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, die empfangenen und Wiedergaben der abgesandten Handelsbriefe sowie die Buchungsbelege. Die Aufbewahrungspflicht beträgt 10 Jahre. Eine entsprechende Regelung gilt für die steuerlichen Unterlagen nach § 147 AO.

Weiterhin sind personenbezogene Daten nach § 35 Abs. 4 BDSG zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Dies trifft insbesondere dann zu, wenn die Identität des Betroffenen nicht eindeutig feststellbar ist.[190]

Wie bei der Löschung ist die Sperrung ausnahmsweise dann nicht vorzunehmen, wenn personenbezogene Daten bei der geschäftsmäßigen Speicherung zum Zweck der Übermittlung aus allgemein zugänglichen Quellen stammen und es sich nicht um sensitive Daten nach § 35 Abs. 2 Nr. 2 BDSG handelt.

Gesperrte Daten dürfen nach § 35 Abs. 8 BDSG nur mit Einwilligung des Betroffenen[191] oder ohne dessen Einwilligung nur zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten übermittelt oder genutzt werden (§ 35 Abs. 8 Nr. 1 BDSG), wenn sie auch ohne die Sperrung übermittelt oder genutzt werden dürften (§ 35 Abs. 8 Nr. 2 BDSG).

Die Sperrung schränkt die Rechte der Betroffenen nicht ein, eine Auskunft, eine Löschung oder Berichtigung zu verlangen.[192]

## 4.4 Rechtmäßigkeit der Datenverarbeitung

Der Betroffene kann die Rechtmäßigkeit einer Datenverarbeitung durch einen Widerspruch oder Einwand, durch eine Eingabe an eine Aufsichtsbehörde oder im Wege einer gerichtlichen Klage überprüfen lassen.

### 4.4.1 Widerspruch oder Einwand

§ 35 Abs. 5 BDSG gibt dem Betroffenen das Recht, einem Erheben, Verarbeiten oder Nutzen seiner personenbezogenen Daten in einer automatischen Verarbeitung oder in einer Verarbeitung in nicht automatisierten Dateien zu widersprechen. Adressat des Widerspruchs ist die verantwortliche Stelle (§ 3 Abs. 7 BDSG).

---

[190] Mallmann in: Simitis, BDSG, § 35, Rn. 44.

[191] § 4, 4 a BDSG findet Anwendung.

[192] Vgl. Mallmann in: Simitis, BDSG, § 20, Rn. 66.

Die personenbezogenen Daten dürfen nicht erhoben, verarbeitet oder genutzt werden, wenn der Widerspruch begründet ist. Er ist begründet, wenn eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung und Nutzung überwiegt.

Der Betroffene kann bestimmen, inwieweit er der Erhebung, Verarbeitung oder Nutzung widersprechen will. Er kann sein Widerspruchsrecht auch auf bestimmte Daten oder Datenarten beschränken oder zum Teil beschränken.[193] Nach einer Auffassung soll der Betroffene einer Löschung oder Sperrung seiner Daten[194] nicht widersprechen können, weil es sich um alternative und grundsätzlich abschließend geregelte Schutzinstrumente handele.[195] Dem steht entgegen, dass der Betroffene mit seinem Widerspruch sein schutzwürdiges Interesse artikuliert. Es besteht also auf Grund des Widerspruches Grund zu der Annahme, dass durch eine Löschung seiner Daten seine schutzwürdigen Interessen beeinträchtigt sein könnten und insoweit ein Fall des § 35 Abs. 3 Nr. 2 BDSG besteht. Der Anspruch auf Sperrung hat zwar Vorrang vor dem Widerspruchsrecht, weil er eine unmittelbare Verpflichtung der verantwortlichen Stelle gegenüber dem Betroffenen begründet. Diese Verpflichtung schließt jedoch den Widerspruch gegen eine Löschung nicht von vornherein aus.

Der Widerspruch kann formlos erhoben werden. Der Petent muss ihn nicht als einen solchen bezeichnen, um Beachtung zu finden. Es muss sich lediglich aus dem Inhalt ergeben, dass der Erhebung, Verarbeitung oder Nutzung bestimmter personenbezogener Daten widersprochen wird. Ob das schutzwürdige Interesse des Betroffenen überwiegt, muss anhand des konkreten Einzelfalles im Rahmen einer Interessenabwägung geprüft werden. Insoweit ist es zweckmäßig, wenn der Betroffene seinen Widerspruch begründet.

Ein Widerspruch scheidet aus, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung der Daten verpflichtet.[196]

### 4.4.2 Anrufung der Aufsichtsbehörde

Jedermann hat nach § 38 Abs. 1 Satz 7 i.V.m. § 21 Satz 1 BDSG das Recht, sich an die Aufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung durch nicht-öffentliche Stellen in seinen Rechten verletzt worden zu sein.[197] Eine Betroffenheit in eigenen Rechten ist nicht erforderlich.[198] Die Aufsichtbehörde hat die Eingabe zu bescheiden und den Eingebenden über das weitere Verfahren und das inhaltliche Er-

---

[193] Mallmann in: Simitis, BDSG, § 20, Rn. 84.

[194] Löschung und Sperrung gehören nach § 3 Abs. 4 BDSG zur Verarbeitung.

[195] Mallmann in: Simitis, BDSG, § 20, Rn. 84.

[196] Rechtsnormen, die die verantwortliche Stelle dazu ermächtigen, verpflichten diese nicht und komen insoweit nicht in Betracht. Mallmann in: Simitis, BDSG, § 20, Rn. 90.

[197] Vgl. Art. 28 Abs. 4 Satz 1 der Europäischen Datenschutzrichtlinie, 95/46/EG.

[198] Walz in: Simitis, § 38, Rn. 19; Ehmann/Helfrich, EG-Datenschutzrichtlinie, Art. 28, Rn. 11.

gebnis zu unterrichten.[199] Der Betroffene hat jedoch keinen Anspruch auf ein bestimmtes Vorgehen oder Prüfungsverhalten der Behörde.[200]

### 4.4.3 Klage

Die Zivilgerichte sind zuständig, wenn Betroffene ihre Datenschutzrechte wie bspw. ihren Auskunftsanspruch nach § 34 BDSG durchsetzen wollen.[201] Soll die Tätigkeit der Aufsichtsbehörde gerichtlich überprüft werden, so ist der Verwaltungsrechtsweg einzuschlagen. Allerdings sind keine Fälle bekannt, in denen ein Betroffener ein Einschreiten der Aufsichtsbehörde gerichtlich erzwungen hätte. Lässt sich die Richtigkeit bzw. Unrichtigkeit der personenbezogenen Daten nicht feststellen, so sind die Daten nach § 35 Abs. 4 BDSG zu sperren.[202]

## 4.5 Kompensation von Schäden

### 4.5.1 Schadensersatz nach BDSG

Wer durch eine unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden erlitten hat, ist nach § 7 BDSG berechtigt, von der verantwortlichen Stelle Schadensersatz zu verlangen. Der Anspruch steht nur dem Betroffenen i.S.d. § 3 Abs. 1 BDSG und nicht Dritten oder juristischen Personen zu. Ersatzpflichtig ist die verantwortliche Stelle, die durch eine rechtswidrige Verwendung der Daten dem Betroffenen einen Schaden zugefügt hat. Dies gilt auch dann, wenn ein Auftragnehmer der verantwortlichen Stelle den Schaden verursacht hat, denn das Handeln des Auftragnehmers muss sich der Auftrageber zurechnen lassen.[203] Der Anspruch kann nicht gegen den Beauftragten für den Datenschutz der verantwortlichen Stelle, gegen den ein separater Anspruch bestehen kann, geltend gemacht werden, denn dieser ist nur ein unselbständiger Teil der nicht-öffentlichen Stelle.

Der Schadensersatzanspruch unterliegt keiner Beschränkung auf einzelne Phasen der Datenverarbeitung oder bestimmte Verwendungsarten.[204] Er ist auch anwendbar bei Verletzungen von datenschutzrechtlichen Vorschriften außerhalb des BDSG.[205]

---

[199] Art. 28 Abs. 4 Satz 2 der Europäischen Datenschutzrichtlinie, 95/46/EG sieht dies ausdrücklich vor. § 38 BDSG ist insoweit Richtlinienkonform auszulegen.

[200] Siehe Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 28, Rn. 15.

[201] Hiervon sind Streitigkeiten im Rahmen von Arbeitsverhältnissen ausgenommen. Zuständig sind die Arbeitsgerichte. Vgl. Mallmann in: Simitis, BDSG, § 34, Rn. 82.

[202] Mallmann in: Simitis, BDSG, § 35, Rn. 43 m.w.Nachw.

[203] Simitis in: Simitis, BDSG, § 7, Rn. 11.

[204] Vgl. Art. 23 Abs. 1 Europäische Datenschutzrichtlinie, 95/46/EG.

[205] Simitis in: Simitis, BDSG, § 7, Rn. 9, 16; in Betracht kommen bspw. § 8 ff TKG, § 3 ff. TDDSG.

Die verantwortliche Stelle haftet für Schäden, die durch eine unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung der Daten entstehen (§ 7 Satz 1 BDSG). Unzulässig sind alle rechtswidrigen Verwendungen personenbezogener Daten. Dazu zählt auch die Verarbeitung personenbezogener Daten ohne Einwilligung des Betroffenen, soweit nicht eine Rechtsvorschrift die Verarbeitung legitimiert (§ 4 Abs. 1 BDSG). Unrichtig ist „jede Verarbeitung falscher, unvollständiger oder durch den Verarbeitungsprozess verfälschter Daten".[206] Dem Betroffenen obliegt es nachzuweisen, dass die verantwortliche Stelle ihm durch eine unrichtige oder unzulässige Erhebung, Verarbeitung oder Nutzung seiner Daten einen Schaden zugefügt hat.[207]

Die Ersatzpflicht der verantwortlichen Stelle kann jedoch nach § 7 Satz 2 BDSG entfallen, wenn sie die nach den Umständen des Falles gebotene Sorgfalt beachtet hat. Ihr Verhalten muss den gesetzlichen Anforderungen im konkreten Fall entsprochen haben. Dies ist dann nicht der Fall, wenn die unzulässige oder unrichtige Verarbeitung auf Fehlern oder Nachlässigkeit der Beschäftigten der verantwortlichen Stelle beruht, für die sie haftet. Sie haftet ebenfalls für die internen und externen Beauftragten für den Datenschutz.[208] Die verantwortliche Stelle trägt die Beweislast für ihr gesetzeskonformes Verhalten. Sie kann sich aber durch den Nachweis eines Mitverschuldens des Betroffenen nach § 254 BGB entlasten.

Der Schadensersatz erstreckt sich auf alle erlittenen materiellen Schäden, die durch die unzulässige oder unrichtige Verarbeitung tatsächlich entstanden sind. Immaterielle Schäden sind von der Ersatzpflicht ausgeschlossen.[209]

Soweit mehrere verantwortliche Stellen den Schaden verursacht haben, haften sie als Gesamtschuldner.[210]

### 4.5.2 Schadensersatzansprüche nach BDSG gegen den Beauftragten für den Datenschutz

Bei Verschulden eines Beauftragten für den Datenschutz kommt ein vertraglicher Anspruch des Betroffenen gegen den Beauftragten nicht in Betracht. Jedoch kann eine deliktische Haftung nach § 823 Abs. 1 BGB vorliegen, wenn der Beauftragte durch einen Pflichtverstoß in die informationelle Selbstbestimmung des Betroffenen eingegriffen und dadurch das in § 823 Abs. 1 BGB geschützte Persönlichkeitsrecht verletzt hat.[211] Da aber in erster Linie die verantwortliche Stelle die erforderlichen Maßnahmen zu treffen hat und damit auch die Verant-

---

[206] Simitis in: Simitis, BDSG, § 7, Rn. 20.

[207] Simitis in: Simitis, BDSG, § 7, Rn. 23.

[208] Simitis in: Simitis, BDSG, § 7, Rn. 26 f.

[209] Einen solchen Anspruch sieht das Gesetz nur bei automatisierter Verarbeitung personenbezogener Daten durch öffentliche Stellen vor (§ 8 Abs. 2 BDSG). Vgl. Simitis in: Simitis, BDSG, § 7, Rn. 32.

[210] Es ist insoweit § 840 Abs. 1 BGB anwendbar. Der Betroffene kann entweder eine der Stellen für den gesamten Schaden in Anspruch nehmen oder von jeder Stelle einen Teilbetrag fordern (§ 421 Satz 1 BGB). Vgl. Simitis in: Simitis, BDSG, § 7, Rn. 36.

[211] Simitis in: Simitis, BDSG, § 4 g, Rn. 103.

wortung für entstandene Schäden trägt, kommt eine Haftung des Beauftragten nur ausnahmsweise in Betracht. Dies ist bspw. dann der Fall, wenn die Verletzung unmittelbar durch die Person des Beauftragten verursacht wurde.[212] Dies wäre der Fall, wenn die Rechtsverletzung auf einer Verletzung seiner Verpflichtung zur Verschwiegenheit beruhen würde.

Darüber hinaus kommt bei Verschulden des Beauftragten eine Haftung nach § 823 Abs. 2 BGB i.V.m den Vorschriften über seine Aufgaben nach § 4 f und 4 g BDSG sowie aus § 824 und 826 BGB in Betracht.[213]

Die Beweislast bei der Durchsetzung von Schadensersatzansprüchen gegen den Beauftragten[214] liegt bei dem Betroffenen.

### 4.5.3 Schadensersatzanspruch nach § 824 BGB wegen Kreditgefährdung

Bezieht sich die unzulässige oder unrichtige Verwendung personenbezogener Daten auf die Behauptung oder Verbreitung einer Tatsache, die geeignet ist, den Kredit eines anderen zu gefährden oder sonstige Nachteile für dessen Erwerb oder Fortkommen herbeizuführen, so hat der Betroffene einen Anspruch auf Schadensersatz auch dann, wenn der andere die Unwahrheit zwar nicht kannte aber hätte kennen müssen (§ 824 Abs. 1 BGB). Eine Ausnahme gilt, wenn es sich um eine Mitteilung handelt, deren Unwahrheit dem Mitteilenden unbekannt war und er oder der Empfänger der Mitteilung an ihr ein berechtigtes Interesse hatten (§ 824 Abs. 2 BGB). Jedoch wird dieser Anspruch durch den spezielleren Schadensersatzanspruch aus § 7 BDSG verdrängt, über den ein Schaden im selben Umfang liquidiert werden kann.[215]

## 4.6 Anspruch auf Unterlassung

Ein Anspruch auf Unterlassung der unzulässigen oder unrichtigen Verwendung von personenbezogenen Daten ergibt sich nicht unmittelbar aus dem Gesetz. In Rechtsprechung und Literatur wird jedoch über den Schadensersatzanspruch hinaus ein Unterlassungsanspruch abgeleitet.[216] Dieser wird zum Teil auf § 7 BDSG[217] und zum Teil auch auf eine analoge Anwendung des allgemeinen Störerabwehranspruches aus § 1004, 12 BGB gestützt[218].

---

[212] Simitis in: Simitis, BDSG, § 4 g, Rn. 105.

[213] Simitis in: Simitis, BDSG, § 4 g, Rn. 106.

[214] Bei externen Beauftragten kommt es bisweilen zu einer Umkehr der Beweislast nach den von der Rechtsprechung zur Produzentenhaftung entwickelten Grundsätzen, vgl. dazu Simitis in: Simitis, BDSG, § 4g, Rn. 110 m.w.Nachw.

[215] Simitis in: Simitis, BDSG, § 7, Rn. 65.

[216] Vgl. OLG Hamm, NJW 1996, 131; BAGE 50, 202, 208 f.

[217] Simitis in: Simitis, BDSG, § 7, Rn. 34 f.

[218] Schaffland/Wiltfang, BDSG, § 6, Rn. 22; Gola/Schomerus, BDSG, § 6, Rn. 2.

## 4.7 Anspruch auf Widerruf

Die Beseitigung der durch den Schadensersatz nicht abgedeckten Folgen[219] unrichtiger oder unzulässiger Verwendungen von personenbezogenen Daten kann der Betroffene in Form des Widerrufs von der verantwortlichen Stelle verlangen.[220]

[219] Dies sind in erster Linie, die von § 35 Abs. 7 nicht erfassten Fällen, in denen die Pflicht der verantwortlichen Stelle zur Benachrichtigung der Stellen an die fehlerhaft übermittelt wurde, unverhältnismäßig ist.

[220] Vgl. BGH NJW 1984, 436 f., OLG Hamm, RDV 1990, 36.

# 5 Datenschutz bei der Verwendung von Kundenkarten

Kundenbindungssysteme sind Programme, mit denen Unternehmen treuen Kunden Rabatte auf die von ihnen angebotenen Waren oder Dienstleistungen anbieten. Solche Bonusprogramme werden sowohl in personalisierter als auch in anonymer Form angeboten.[221] Klassisches Beispiel für ein Bonusprogramm ohne Personenbezug ist die Sammelkarte, auf der Leistungen vermerkt und bei Erwerb einer bestimmten Anzahl von Waren oder Leistungen ein Bonus in Form eines Preisnachlasses gewährt wird. Die Auszahlung des Rabatts erfolgt nach Vorlage der Rabattsammelkarte, die als Nachweis des Rabattanspruchs dient. Teilnehmer an personalisierten Kundenbindungssystemen sind dagegen dem Betreiber des Bonusprogramms bekannt. Dieser führt für jeden Teilnehmer ein Bonuskonto, in dem die erworbenen Rabattansprüche verwaltet werden. Zur Erfassung der Rabattansprüche dient in der Regel eine Karte, die mit einem Magnetstreifen oder Chip versehen ist, der die identifizierenden Daten über den Teilnehmer enthält.

Solche personalisierten Bonusprogramme werden in zwei unterschiedlichen Konstellationen angeboten. Bonusprogramme im Zwei-Parteien-Verhältnis werden vom einem Unternehmen für die eigenen Kunden angeboten und betrieben. In solchen Fällen besteht bereits eine Kundenbeziehung zwischen beiden Parteien, die durch das Bonusprogramm personalisiert wird. Daneben gibt es unternehmensübergreifende Bonusprogramme im Drei- oder Mehr-Parteien-Verhältnis. Diese Programme werden üblicherweise zentral durch einen Systembetreiber betrieben. Der Systembetreiber ist in der Regel Vertragspartner des Kunden im Hinblick auf dessen Teilnahme am Programm und die Verwaltung und Gutschrift seiner Rabattansprüche. Die Rabattansprüche werden in dieser Konstellation durch den Kunden bei teilnehmenden Partnerunternehmen erworben. Dies sind Händler oder Dienstleister, die sich zur Gewährung von Rabatten dem Systembetreiber angeschlossen haben. Üblicherweise sind an einem solchen Bonusprogramm mehrere Partnerunternehmen beteiligt; die Bonuskarte des Teilnehmers ist in allen Partnerunternehmen einsetzbar.[222]

Im Folgenden werden die datenschutzrechtlichen Anforderungen an die Gestaltung von Kundenbindungssystemen beschrieben[223]. Die Darstellung orientiert sich an der Konstellation des unternehmensübergreifenden Kundenbindungssystems, bei dem die Kundendaten zentral beim Systembetreiber verarbeitet werden. Im Grundsatz sind die nachfolgenden Ausführungen auf Kundenbindungssysteme im Zwei-Parteien-Verhältnis übertragbar.

---

[221] Übersicht über das Angebot auf dem deutschen Markt bei van Boxlaer, Card-Forum 04/2003, 24 ff.

[222] Zur genauen Funktionsweise dieser Systeme siehe Weichert, DuD 2003, 161 ff.; Weber/Jacob/Rieß/Ullmann, DuD 2003, 614, 615 f.

[223] Eine umfassende Darstellung der datenschutzrechtlichen Anforderungen und deren Umsetzung in der Praxis enthält das Gutachten des Unabhängigen Landeszentrums für Datenschutz für den Verbraucherzentrale Bundesverband e.V. aus dem Jahr 2003, veröffentlicht unter www.datenschutzzentrum.de/wirtschaft/kundbisy.htm und www.vzbv.de/mediapics/gutachten_kundenbindungssysteme_2003.pdf. Eine Kurzfassung der Studie bei Körffer, DuD 2004, 267 ff.

## 5.1 Zulässigkeit der Datenverarbeitung

Im Rahmen des Kundenbindungssystems werden unterschiedliche Daten des Kunden von unterschiedlichen Beteiligten zu unterschiedlichen Zwecken verarbeitet. Bei einer rechtlichen Beurteilung dieser Vorgänge ist demgemäß zu differenzieren. In datenschutzrechtlicher Hinsicht ist der jeweilige Zweck der Datenverarbeitung für die rechtliche Bewertung relevant. Aus diesem Grund erfolgt die Beurteilung getrennt nach den unterschiedlichen Verarbeitungszwecken „Rabattabwicklung“ und „Werbung und Marktforschung“. Innerhalb dieser Zwecke ist weiterhin danach zu differenzieren, welche Daten verarbeitet werden. Es ist zu unterscheiden nach den Stammdaten des Kunden wie Name, Anschrift oder Geburtsdatum und den Programmdaten, die bei der Teilnahme am Bonusprogramm anfallen. Schließlich kann es für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung auch auf die Person des Verarbeitenden ankommen, d.h. darauf, ob Daten durch eines der Partnerunternehmen oder durch den Systembetreiber verarbeitet werden.

### 5.1.1 Datenverarbeitung zum Zweck der Programmabwicklung

#### 5.1.1.1 Verarbeitung der Stammdaten

Mit dem Anmeldeformular werden regelmäßig Pflichtangaben des Kunden erfragt, die der Systembetreiber für die Durchführung des Rabattprogramms als erforderlich ansieht. Hierbei handelt es sich in der Regel um den vollständigen Namen, die Anschrift sowie in einigen Fällen auch um weitere Daten wie das vollständige Geburtsdatum oder die Telefonnummer (so genannte Stammdaten).

Als Rechtsgrundlage für die Verarbeitung der Daten kommt § 28 Abs. 1 Nr. 1 BDSG in Betracht. Danach ist die Verarbeitung der Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Diese Voraussetzung ist erfüllt, wenn die Kenntnis der zu erhebenden Daten für die Erfüllung des Vertragszwecks erforderlich ist.[224] Dies gilt etwa für den Namen und die Anschrift des Kunden, die zur eindeutigen Identifizierung und zu dessen Ansprache erforderlich sind. Darüber hinaus ist die Kenntnis einer weiteren Kontaktmöglichkeit, wie etwa der Telefonnummer oder der E-Mail-Adresse, für die Vereinfachung der Vertragsabwicklung etwa durch telefonische Rückfragen zumindest sinnvoll, so dass gegen die Erhebung einer weiteren Kontaktmöglichkeit keine Bedenken bestehen.

Die Kenntnis des vollständigen Geburtsdatums des Teilnehmers ist für ein Bonusprogramm nicht erforderlich, ausreichend ist die Kenntnis des Geburtsjahrs.[225] Dem wird von Bonus-

[224] Bergmann/Möhrle/Herb, BDSG, § 28, Rn. 26; ähnlich Simitis in: Simitis, BDSG, § 28, Rn. 79, der voraussetzt, dass die Daten für die Erfüllung des Vertragszwecks benötigt werden.

[225] Weichert, DuD 2003, 161, 164.

programmbetreibern oft entgegengehalten, die Kenntnis des Geburtsdatums sei erforderlich, um das genaue Alter der Antragsteller und somit ihre Berechtigung zur Teilnahme, die häufig Volljährigkeit oder ein bestimmtes Alter voraussetze, zu prüfen. Um die Erreichung der Altersgrenze festzustellen, sind jedoch datensparsamere Lösungen möglich. Hierzu gehört die Angabe des Antragstellers, ob er eine bestimmte Altersgrenze erreicht hat. Da die Notwendigkeit der Kenntnis des genauen Alters nur eine kleine Gruppe der Antragsteller betrifft, ist nach den Grundsätzen der Datenvermeidung und Datensparsamkeit nach § 3 a BDSG auf die routinemäßige Abfrage des Geburtsdatums zu verzichten. Auch zur eindeutigen Identifizierung eines Teilnehmers in dem (seltenen) Fall, dass sowohl Namen als auch Adresse identisch sind, genügt das Geburtsjahr.

#### 5.1.1.2 Verarbeitung der Programmdaten

Setzt der Kunde seine Karte bei einem Einkauf oder bei der Inanspruchnahme einer Dienstleistung bei einem der Partnerunternehmen ein, wird dort eine Reihe von Daten über diesen Vorgang festgehalten. Bei diesen Daten handelt es sich gewöhnlich um eine Kennung des Kunden, etwa durch eine Kunden- oder Kartennummer, die Kennung des beteiligten Partnerunternehmens, Ort, Datum und Uhrzeit des Karteneinsatzes, den Umsatz sowie u.U. auch Angaben über die erworbene Ware oder die in Anspruch genommene Dienstleistung nach Waren- oder Dienstleistungsgruppen (Programmdaten).[226] Diese Daten werden durch das jeweils beteiligte Partnerunternehmen erhoben und anschließend an den Systembetreiber übermittelt.

Die Zulässigkeit der Verarbeitung dieser Daten beurteilt sich wiederum am Maßstab des § 28 Abs. 1 BDSG. Um die für den Karteneinsatz gewährten Punkte auf dem vom Systembetreiber geführten Bonuskonto des Kunden gutzuschreiben, ist in der Regel lediglich die Kenntnis der Höhe des Rabattbetrages sowie zusätzlich Ort und Zeitpunkt des Vorgangs, des Partnerunternehmens und ggf. des Preises der Ware oder Dienstleistung erforderlich. Wird das Grundgeschäft bei gleichzeitiger Stornierung der Punktegutschrift rückgängig gemacht oder hat sich ein Kunde beschwert, dann muss sichergestellt sein, dass auch nachträglich die Bonusgutschrift eindeutig dem jeweils zu Grunde liegenden Geschäft zugeordnet werden kann. Auch die ordnungsgemäße Berechnung der Bonuspunkte muss jederzeit nachvollziehbar sein. Für diese Zwecke sind die oben aufgezählten Daten in aller Regel auch ausreichend. Die Kenntnis der Warengruppe oder der Gruppe der in Anspruch genommenen Dienstleistungen ist dagegen in der Regel nicht unbedingt notwendig, es sei denn, diese sind für die Berechnung der Bonuspunkte erforderlich. Dies ist nur dann der Fall, wenn unterschiedliche Warengruppen oder Dienstleistungen in unterschiedlicher Höhe rabattiert werden.

[226] Weber/Jacob/Rieß/Ullmann, DuD 2003, 614, 616.

### 5.1.2 Datenverarbeitung zum Zweck der Werbung und Marktforschung

Die im Rahmen des Kundenbindungssystems erhobenen Kundendaten werden in der Regel durch die Partnerunternehmen und/oder durch den Systembetreiber für Zwecke der Werbung oder Marktforschung der Partnerunternehmen genutzt. Oft beschränkt sich der Umfang der Daten nicht auf die bereits genannten Stamm- und Programmdaten, sondern es werden auch Angaben der Kunden einbezogen, die diese mittels des Anmeldeformulars freiwillig erklären. Hierzu gehören etwa Angaben zu Familienstand, Haushaltseinkommen, Hobbies oder Konsumvorlieben. Als Rechtsgrundlage für eine solche Nutzung der Kundendaten kommt neben einer Einwilligung des Verbrauchers der gesetzliche Erlaubnistatbestand § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht.[227]

Gemäß § 28 Abs. 1 Nr. 2 BDSG ist die Verwendung von Daten für eigene Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Zu den berechtigten Interessen eines Unternehmens gehört grundsätzlich auch die Durchführung von Werbeaktionen und Marktanalysen.[228] Das am Bonusprogramm beteiligte Partnerunternehmen hat somit ein berechtigtes Interesse, seine eigenen Kunden kennen zu lernen und dadurch die Möglichkeit der Werbeansprache oder auch einer optimierten Gestaltung seines Angebots zu erhalten. Auch dem zentralen Systembetreiber dürfte in der Regel ein berechtigtes Interesse an der Durchführung von Werbemaßnahmen oder Marktanalysen zustehen.

Diesem Interesse der Betreiberunternehmen ist nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG das schutzwürdige Interesse des Betroffenen gegenüberzustellen. Für die Verwendung der zulässigerweise erhobenen Stammdaten des Kunden (Name, Anschrift, Geburtsjahr) kann regelmäßig davon ausgegangen werden, dass schutzwürdige Interessen des Betroffenen nicht überwiegen, diese somit nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig ist.

Für die Verwendung von weiteren Kundendaten kann § 28 Abs. 1 Satz 1 Nr. 2 BDSG dagegen nicht als Rechtsgrundlage herangezogen werden. Dem stehen regelmäßig schutzwürdige Interessen der Betroffenen entgegen. Dies gilt bspw., wenn bei der Programmabwicklung zusätzliche Kontaktmöglichkeiten für den Zweck der Werbung und Marktforschung erhoben und verwendet werden sollen. Die Verwendung der Telefonnummer zum Zweck der Telefonwerbung wird in der Rechtsprechung als besonders schwerer Eingriff in die Privatsphäre des Kunden angesehen[229], so dass ihr überwiegende schutzwürdige Belange des Kunden entgegenstehen. Gleiches gilt für die Nutzung der Fax-Nummer[230] oder der E-Mail-

---

[227] § 28 Abs. 1 Nr. 1 BDSG scheidet als Rechtsgrundlage regelmäßig aus, da die Durchführung von Maßnahmen der Werbung oder Marktforschung anhand der Kundendaten üblicherweise nicht Gegenstand des Rabattvertrags ist.

[228] Simitis in: Simitis, BDSG, § 28, Rn. 137; Schaffland/Wiltfang, BDSG, § 28, Rn. 92.

[229] Vgl. dazu etwa BGH NJW 2000, 2677.

[230] Vgl. dazu BGH NJW 1996, 660.

Adresse.[231] Auch der Nutzung des vollständigen Geburtsdatums zu Werbe- oder Marktforschungszwecken, um dem Betroffenen bspw. zum Geburtstag zu gratulieren, können schutzwürdige Interessen der Betroffenen entgegenstehen. Verbraucherfreundlich ist hier eine Lösung, die dem Kunden die Angabe seines vollständigen Geburtsdatums unter Beschreibung des vorgesehenen Verwendungszwecks freistellt.

Der Nutzung der mit dem Antragsformular häufig erhobenen Angaben, etwa über Konsumvorlieben, Familienstand, Haushaltsgröße und -einkommen sowie Beruf und Hobbies stehen ebenfalls schutzwürdige Interessen der Betroffenen entgegen. Für eine zielgruppengerechte Werbung und insbesondere auch für die Marktforschung sind solche Informationen von Interesse. Je breiter die Informationsgrundlage über den Kunden ist, desto gezielter kann dieser beworben werden und desto genauere Analysen lassen sich über dessen Kaufverhalten treffen. Im Hinblick auf die Werbung kann dies sogar für den Kunden von Vorteil sein, da ihm durch eine gezielte Ansprache unliebsame Werbung erspart werden kann. Bei der Abwägung der Interessen ist aber zu berücksichtigen, dass es sich bei diesen Daten regelmäßig um Informationen handelt, die eine Aussagekraft über die Persönlichkeit des Kunden, dessen Lebenssituation oder wirtschaftliche Verhältnisse haben. Aus diesem Grund muss das Interesse der Betroffenen am Ausschluss der Verwendung dieser Daten zu Werbe- und Marktforschungszwecken das Interesse des Partnerunternehmens ohne ihre Kenntnis und Zustimmung überwiegen.

Gleiches gilt auch für die bei der Teilnahme am Programm anfallenden Programmdaten.[232] Wegen ihres Aussagegehalts über das Kaufverhalten bzw. ggf. auch über andere Verhaltensweisen, etwa über die Nutzung von Telefonverbindungen, ist auch hinsichtlich dieser Daten ein überwiegendes Interesse der Betroffenen am Ausschluss der Verwendung für Werbe- und Marktforschungszwecke anzunehmen. Dies gilt insbesondere, wenn nicht nur Programmdaten verwendet werden, die für die Abwicklung des Programms erforderlich sind, sondern darüber hinaus auch Daten über die Art des zu Grunde liegenden Geschäfts, also die erworbene Ware oder die in Anspruch genommene Dienstleistung.

Diese Grundsätze, die bereits für die Verwendung der Daten im Zwei-Parteien-Verhältnis gelten, gelten erst recht für die Verwendung von Kundendaten durch einen zentralen Systembetreiber.

Die schutzwürdigen Interessen der Kunden sind bei einer Datenverarbeitung durch den Systembetreiber weitaus stärker betroffen als bei einer Verarbeitung durch das Partnerunternehmen. Die Identität des Systembetreibers ist dem Kunden i.d.R. nicht in gleicher Weise bekannt wie die des Partnerunternehmens. Aufgrund der zentralen Rolle des Systembetreibers innerhalb des Bonusprogramms kann der Kunde häufig nicht einschätzen und überblicken, welche Daten der Systembetreiber über ihn gespeichert hat und welche davon für welche Art von Werbung bzw. zur Marktforschung herangezogen werden. Der Systembetreiber

---

[231] Ayad, CR 2001, 533 ff.

[232] So auch Weber/Jacob/Rieß/Ullmann, DuD 2003, 614, 618.

verfügt regelmäßig über weitaus umfangreichere Informationen über das Kaufverhalten der Teilnehmer als es im Zwei-Parteien-Verhältnis der Fall ist.

Der vorhandene Datenbestand kann häufig geeignet sein, Kundenprofile zu erstellen, die je nach Datenmenge und -qualität detaillierten Aufschluss über das Konsumverhalten und auch weitere Faktoren, wie etwa die Bonität des Kunden, geben können.[233] Auf welche Weise solche Profile gebildet und anschließend verwendet werden, entzieht sich im Normalfall der Kenntnis des Kunden.[234] Durch die Bildung von solchen aussagekräftigen Kundenprofilen ist regelmäßig ein schutzwürdiges Interesse des Kunden berührt.[235] Hierbei ist auch zu berücksichtigen, dass der Systembetreiber vertragliche Beziehungen zu sämtlichen an das Bonusprogramm angeschlossenen Partnerunternehmen hat. Es ist für den Kunden nicht auszuschließen, dass über den Systembetreiber auch Unternehmen Kenntnis von Daten über Personen erhalten, die nicht zu ihrem Kundenstamm gehören. Eine solche weitreichende Datenverarbeitung berührt ebenfalls das schutzwürdige Interesse der Kunden in erheblichem Maße.

Im Ergebnis ist für die Verwendung von weiteren Daten als Name, Anschrift und Geburtsjahr eine Einwilligung des Kunden erforderlich.

## 5.2 Anforderungen an die Einwilligungserklärung

Die Einwilligungserklärung ist bei Kundenbindungssystemen regelmäßig von zentraler Bedeutung. Hier gilt es, der Komplexität dieser Systeme durch eine überschaubar und kundenfreundlich gestaltete Einwilligungserklärung gerecht zu werden und für den Betroffenen Transparenz und Wahlfreiheit zu schaffen. Die datenschutzrechtlichen Anforderungen an die Wirksamkeit der Einwilligung ergeben sich aus § 4 a BDSG (s.o. S. 37 ff.)

Die Einwilligung muss nach § 4 a Abs. 1 Satz 1 BDSG auf der freien Entscheidung des Betroffenen beruhen. Durch dieses Erfordernis soll sicher gestellt werden, dass eine Daten verarbeitende Stelle ihre Leistung gegenüber dem Betroffenen nicht davon abhängig machen kann, dass dieser Daten preisgibt und einer Verarbeitung zustimmt, die für die Erbringung der Leistung nicht erforderlich ist.[236] Dieses für den Bereich der Telekommunikation gesetzlich ausdrücklich geregelte Kopplungsverbot (s.o. S. 37) gilt auch für den Bereich der Werbung und Markt- oder Meinungsforschung. Durch § 28 Abs. 4, § 29 Abs. 4 BDSG hat der Gesetzgeber zum Ausdruck gebracht, dass die Nutzung für Zwecke der Werbung und Marktforschung der freien Disposition des Verbrauchers unterworfen sein soll und dass der Widerspruch gegen eine solche Nutzung keine Auswirkungen auf das Grundverhältnis haben darf.

---

[233] Vgl. dazu auch Weber/Jacob/Rieß/Ullmann, DuD 2003, 614, 618.

[234] Dazu Jacob/Jost, DuD 2003, 621; Weichert, DuD 2003, 161, 165.

[235] So auch Weber/Jacob/Rieß/Ullmann, DuD 2003, 614, 618, die hierdurch den Kern des Rechts auf informationelle Selbstbestimmung berührt sehen.

[236] Simitis in: Simitis, BDSG, § 4 a, Rn. 65; ders. DuD 2000, 721 f.; Bergmann/Möhrle/Herb, BDSG, § 4 a, Rn. 6.

Im Hinblick auf die Informationspflichten stellt sich bei Kundenbindungssystemen die Frage, welche Informationen im Einwilligungstext selbst enthalten sein müssen bzw. ob und in welchen Fällen es ausreicht, wenn sich Angaben aus dem gesamten Formular, z.B. aus den Teilnahmebedingungen oder aus gesonderten Hinweisen zum Datenschutz, ergeben. Unternehmensübergreifende Kundenbindungssysteme lassen sich im Regelfall nicht kurz und präzise in einer Einwilligungserklärung darstellen. Die Einwilligungserklärung soll den Kunden möglichst schnell und überschaubar informieren und nicht derart mit Informationen überfrachtet werden, dass die Verständlichkeit darunter leidet. Der Text der Einwilligungserklärung sollte sich daher auf die wesentlichen Punkte beschränken, aber auch über die wichtigsten Fakten informieren. Dies sind

- Benennung der für die Datenverarbeitung verantwortlichen Stelle(n)
- Aufzählung der verarbeiteten Datenkategorien
- Darstellung der einzelnen Phasen der Datenverarbeitung und Datenflüsse
- Adressaten einer Datenübermittlung
- Benennung der Zwecke der Datenverarbeitung
- Hinweis auf die Folgen der Verweigerung
- Hinweis auf Widerrufbarkeit mit Kontaktmöglichkeit, evtl. Folgen des Widerrufs

Erhalten neben dem Systembetreiber auch angeschlossene Partnerunternehmen Kundendaten, so ist der Kunde auch über sämtliche Partnerunternehmen zu informieren. In der Praxis geschieht dies meist durch einen Verweis auf Broschüren oder Internetauftritte, denen die aktuell teilnehmenden Partnerunternehmen entnommen werden können. Treten später neue Partnerunternehmen dem Bonussystem bei, ist der anfängliche Hinweis auf Möglichkeiten, den jeweils aktuellen Bestand einzusehen, nur dann ausreichend, wenn nur die vom Kunden selbst kontaktierten Unternehmen Kundendaten erhalten. In diesem Fall entscheidet der Kunde durch die Verwendung seiner Kundenkarte bei dem neu hinzugekommenen Partnerunternehmen selbst über die Verarbeitung seiner Kundendaten durch dieses Unternehmen. Erhalten automatisch auch weitere Partnerunternehmen Kundendaten, so sind neu hinzutretende Partnerunternehmen nicht von der ursprünglichen Einwilligungserklärung erfasst.

Die notwendige Information über die verarbeiteten Kundendaten umfasst sämtliche im Rahmen des Programms zu verarbeitende Datenkategorien, insbesondere ist hier eine präzise Benennung der anfallenden Programmdaten erforderlich.

Hinsichtlich der Zweckbeschreibung ist darauf zu achten, dass die Zwecke der Werbung und Marktforschung deutlich als solche benannt nicht durch beschönigende Formulierungen verschleiert werden. Sollen zum Zweck der Werbung und Marktforschung Kundenprofile gebildet werden, dann genügt nicht nur ein allgemeiner Hinweis auf die Zwecke der Werbung und Marktforschung, vielmehr ist hier der Zweck der Profilbildung deutlich herauszustellen. Ist eine Auswertung der im Kundenprofil zusammengetragenen Kundendaten beabsichtigt, so muss, wenn dies durch eine wirksame Einwilligung legitimiert sein soll, der Kunde auf die geplante Auswertung einschließlich des Zwecks der Auswertung hingewiesen werden. Ist die Zielrichtung einer Auswertung vor deren Abschluss nicht bekannt, weil etwa mittels Data-

Mining gerade bislang unbekannte Zusammenhänge und deren Ergebnisse aufgedeckt werden sollen, kann mangels einer präzisen Zweckangabe eine Einwilligung des Kunden nicht wirksam herbeigeführt werden.

## 5.3 Weitere Anforderungen

Neben den dargestellten Anforderungen sind im Rahmen von Kundenbindungssystemen die allgemeinen Anforderungen des Bundesdatenschutzgesetzes zu beachten, wie etwa die Informationspflicht gemäß § 4 Abs. 3 BDSG (s.o. S. 46) oder die Pflicht zur Löschung der Daten, wenn ihre Kenntnis zur Erfüllung des Vertragszwecks nicht mehr erforderlich ist, § 35 Abs. 2 Nr. 3 BDSG. Unterliegen die Daten einer gesetzlichen Aufbewahrungsfrist, was im Bereich der Kundenbindungssysteme regelmäßig aufgrund der handels- und steuerrechtlichen Aufbewahrungsfristen der Fall ist, so sind die Daten nach Wegfall der Erforderlichkeit gemäß § 35 Abs. 3 Nr. 1 BDSG zu sperren.

Besondere Bedeutung für die Teilnehmer erlangt im Rahmen von Kundenbindungssystemen das Auskunftsrecht der Betroffenen gemäß § 34 BDSG (S. 53 ff.). Der Auskunftspflicht der verantwortlichen Stelle unterliegen nicht nur die gespeicherten Stammdaten des Kunden, sondern sämtliche zu seiner Person gespeicherten Angaben, inklusive der daraus abgeleiteten Kundenprofile sowie die Empfänger von Datenübermittlungen einschließlich Auftragsdatenverarbeiter. Der Auskunftsanspruch hilft dem Teilnehmer an dem Kundenbindungsprogramm, Erkenntnisse über den Umfang, die Art und Weise und die Folgen der Datenverarbeitung zu gewinnen, die ihm bei Erklärung seiner Einwilligung bereits abstrakt erläutert werden sollte. Anhand der Auskunft der Daten verarbeitenden Stelle kann die abstrakte Vorstellung konkretisiert werden.

# 6 Datenschutz beim Einsatz von RFID

## 6.1 Einsatz von RFID

### 6.1.1 Handel

„Die Zukunft im Handel hat schon begonnen!“ titelte eine Veranstaltung[237], die sich mit dem Einsatz von sog. Radio Frequency Identification Tags (RFID) im Einzelhandel befasste. Mit diesem Fortschrittsverweis wird auf den möglicherweise revolutionierenden Charakter einer Technik hingewiesen, die das Einkaufserlebnis des Verbrauchers wie auch den Arbeitsplatz des Mitarbeiters im Einzelhandel und der vorgeschalteten Logistikkette nachhaltig verändern könnte.

RFID sind kleine, kostengünstig zu produzierende Transponder (Computer-Chips)[238], die in Produkte oder Verpackungen dauerhaft eingebracht werden sollen. Sie enthalten in der Regel einen Erkennungscode, der das Produkt eindeutig identifiziert und der kontaktlos und ohne Sichtverbindung über Funk ausgelesen werden kann. Dieser Erkennungscode kann in Datenbanken hinterlegt und mit Zusatzinformationen zur Produktgattung, aber auch zum Produkt selber ergänzt werden.[239] Eine Produktdatenbank soll z.B. mit EPC Global[240] auf weltweiter Basis standardisiert und allgemein zugänglich gemacht werden.

Der Einsatz der RFID-Technik im Handel verspricht eine Reihe von Rationalisierungseffekten. So könnte die Eingangs- und Ausgangsverwaltung von Ware stückzahlgenau ohne aufwändige Zählungen automatisiert erfolgen, indem die RFID-Tags am Lagereingang und -ausgang kontaktlos ausgelesen werden. Eine Einzelbepreisung könnte entfallen, wenn Preisdisplays an den Regalen die RFID der dort ausliegenden Produkte auslesen und den aktuellen Preis der Produkte aus einer Datenbank erhalten und anzeigen. Legt der Verbraucher ein Produkt in seinen Warenkorb, so könnte ein dort angebrachtes RFID-Lesegerät den Gesamtpreis der Produkte im Warenkorb anzeigen, so dass das Kassenband (und die zugehörige Schlange) künftig entfallen würden.[241]

---

[237] Gemeinsamer Workshop der IQPT und ver.di Einzelhandel, http://www.bwbtq.de/btq/list_asp/..\medien\Die_Zukunft_im_Handel_hat_schon_begonnen.pdf.

[238] Siehe hierzu die (noch unveröffentlichte) Studie von ULD und Humboldt-Universität, TAUCIS – Technikfolgenabschätzung und Ubiquitäres Computing vom 31.03.2006.

[239] Ausführlich zu den technischen Grundlagen von RFID siehe http://de.wikipedia.org/wiki/Rfid und Meyer, Computerwoche, 25/2005, S. 22 f.

[240] Siehe http://www.epcglobalinc.org.

[241] Näheres zur Vision und seiner testweisen Realisierung siehe die Berichterstattung bei Heise über den Metro Future Store in Nordrhein-Westfalen, http://www.heise.de/newsticker/meldung/40963 und http://www.heise.de/newsticker/meldung/36487.

Diese beispielhaft aufgezählten Einsatzmöglichkeiten zeigen auf, dass die Vorteile sich vor allem aus einer omnipräsenten kontaktlosen Produktkontrolle ergeben, die die Logistik z.B. durch automatisierte Überprüfung von Produktmengen vereinfachen. Darüber hinaus helfen RFID-Tags bei der Lokalisierung der Produktstandorte, indem bspw. Lesegeräte an den Ein- und Ausgängen verschiedener Räume den Fluss von Ware registrieren und in einer Datenbank speichern. Auch können über RFID-Tags Informationen über das Auswahl- und Kaufverhalten von Verbrauchern erhoben und gespeichert werden, indem die Zusammenstellung der Produkte ausgewertet wird, in welcher Reihenfolge sie aus dem Regal entnommen worden sind und wie lange die Auswahl gedauert hat.

Solche zunächst pseudonymen Verbraucherprofile können einen Namen und ein Gesicht erhalten, wenn auch Kundenkarten RFID-Tags enthalten und diese ausgelesen werden können und so auf die hinterlegten Stammdaten des Kunden zugegriffen werden kann. Eine andere Zuordnung der Objektinformationen zu einem Verbraucher erfolgt, wenn die Informationen aus einem elektronischen Zahlungsmittel (EC-Karten-Beleg) mit den Verbraucherprofilen der Verkaufsvorgänge verknüpft werden. Die Erhebungsvorgänge werden beschleunigt, wenn RFID-Tags in den Karten der Zahlungsmittel implementiert sind und ein kontaktloses Auslesen ermöglichen. Auch die Zuordnung von Personenbildern aus einer Videoüberwachung zu bestimmten Verkaufsvorgängen oder die automatisierte Nachverfolgung bestimmter Produkte im Verkaufsraum mit Unterstützung einer Videoüberwachung ist prinzipiell denkbar.

### 6.1.2 Stadien

Ein weiteres, unmittelbar bevorstehendes Einsatzfeld der RFID-Technik soll die Verwendung in Eintrittskarten der Fußballweltmeisterschaft 2006 werden.[242] Von einem solchen Einsatz verspricht man sich ebenfalls mehr Kontrolle, in diesem Fall über den Verbleib der Karten (Bekämpfung des Schwarzmarkts) und die Identität und den Aufenthaltsort ihrer Besitzer während eines Spiels. Gleichzeitig sollen durch die kontaktlose Auslesung der Zugangsberechtigung Wartezeiten am Einlass verkürzt werden. Eine Deaktivierung oder Unbrauchbarmachung des RFID-Tags hat demnach zur Folge, dass die Funktion des Tickets, die Zutrittserlaubnis, verloren geht.

Für den Erwerb der Karten sind umfangreiche Personenprofile zu hinterlegen, denen eine bestimmte Kennnummer des Tickets zugeordnet wird. Wird eine solche Kennnummer in RFID-Tags der Eintrittskarte hinterlegt, kann über im Stadion aufgestellte Lesegeräte die Anwesenheit einer solchen Karte und damit im Regelfall ihres Besitzers in bestimmten Teilbereichen des Stadions festgestellt werden. Damit wird der Aufenthaltsort einer bestimmten Person näher eingegrenzt. Auch hier kann eine Verknüpfung mit der Videoüberwachung ein besonderes Kontrollpotential eröffnen.[243]

---

[242] Siehe Berichterstattung bei Heise, http://www.heise.de/newsticker/meldung/61251 m.w.N.

[243] Siehe Berichterstattung bei Heise vom 15.01.2004, www.heise.de/newsticker/meldung/43645.

## 6.2 Rechtmäßigkeit der Datenverarbeitung

Der Einsatz der RFID-Technik in den geschilderten Anwendungsumfeldern ist unter dem Gesichtspunkt des Verbraucherdatenschutzrechts zu betrachten, soweit personenbezogene Daten der Kunden mit den RFID-Systemen verarbeitet werden. Personenbezogene Daten[244] sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

### 6.2.1 Funktionsweise von RFID

RFID in Produkten kennzeichnen einen Gegenstand in der Regel eindeutig,[245] da über Hintergrunddatenbanken des einsetzenden Unternehmens oder über allgemein zugängliche Datenquellen wie z.B. EPC Global[246] die im RFID abgespeicherte Kennnummer einem konkreten Produkt zugeordnet werden kann (stückweise Identifizierbarkeit des Produkts). Wenn ein derart identifizierbares Produkt einer Person zugeordnet wird, entstehen Informationen über die persönlichen oder sachlichen Verhältnisse des Besitzers des RFID (z.B. die Eigenschaft als Käufer oder Eigentümer des Produkts). Eine solche Zuordnung kann sowohl kontextbasiert und zunächst pseudonym als auch durch direkte Identifizierung z.B. durch ein RFID-Tag in der Kundenkarte, dem Zahlungsmittel oder einem Ausweispapier des Kunden erfolgen. Eine Zuordnung von Produkten in einer bestimmten zeitlichen und räumlichen Reihenfolge im Geschäft ermöglicht eine differenzierte Profilbildung der Konsumgewohnheiten. Insofern liegen in der Verarbeitung von RFID-Daten personenbezogene Daten vor, so dass datenschutzrechtliche Regelungen[247] eingreifen.

RFID in Eintrittskarten für Veranstaltungen enthalten eine Kennnummer, der es dem Veranstalter oder Sicherheitsorganen ermöglicht, bestimmte Eintrittskarten ihrem Erwerber zuzuordnen, der im Rahmen des Erwerbs personenbezogene Daten hinterlegen musste. Wird eine bestimmte Karte an einem Lesegerät erkannt, ist bekannt, an welchem Ort sich der Besitzer der Karte zu einer bestimmten Zeit befunden hat und welche Personen sich in räumlicher Nähe aufhielten.

Damit liegen in beiden Anwendungsbeispielen personenbezogene Daten von Konsumenten (Kunden, Veranstaltungsbesuchern) vor, so dass der Anwendungsbereich des BDSG nach § 1 Abs. 1 eröffnet ist. Die Datenverarbeitung erfolgt durch die verantwortlichen Stellen im Rahmen der Leistungserbringung im Vorfeld oder bei der Durchführung eines Vertrages. Ein ausschließlich familiärer oder persönlicher Zweck der Verarbeitung, der eine Anwendbarkeit

---

[244] § 3 Abs. 1 BDSG.

[245] Siehe zu den technischen Grundlagen von RFID siehe http://de.wikipedia.org/wiki/Rfid und Meyer, Computerwoche, 25/2005, S. 22 f.

[246] Zum Umfang von EPCGlobal siehe http://www.epcglobalinc.org.

[247] § 1 Abs. 1 und 2 BDSG.

des Bundesdatenschutzgesetzes ausschließen würde, liegt damit beim Verantwortlichen der Verarbeitung nicht vor.

### 6.2.2 Allgemeine datenschutzrechtliche Zulässigkeit

Nach § 4 Abs. 1 BDSG sind personenbezogene Datenverarbeitungen nur dann zulässig, wenn eine Rechtsvorschrift diese explizit erlaubt oder vorschreibt oder eine wirksame Einwilligung des Betroffenen vorliegt. Als Erlaubnisnormen kommt in den geschilderten Anwendungsbeispielen grundsätzlich § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG in Betracht, da die Verarbeitung personenbezogener Daten mittels RFID während der Vertragsanbahnung oder zur Vertragsdurchführung oder aber im Interesse der verantwortlichen Stelle stattfindet. Darüber hinaus könnte die Verarbeitung durch eine wirksame Einwilligung gedeckt sein.

### 6.2.3 Verantwortliche Stelle

Ausgangspunkt ist die Frage nach der datenschutzrechtlichen Verantwortlichkeit. Verantwortlich ist, wer personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. (§ 3 Abs. 7 BDSG). Personenbezogene Verarbeitungsprozesse erfolgen zunächst in den technischen Hintergrundsystemen, in denen die personenbezogenen Kundendaten bspw. aus dem Zahlungsvorgang wie Name, Anschrift, Konto und gekaufte Waren verarbeitet und mit den Identifikatoren der Objekte korreliert werden. Verantwortlich für diese Datenverarbeitung ist der Betreiber des Hintergrundsystems – in den beiden Anwendungsbeispielen der Betreiber des Kaufhauses bzw. des Stadions.

Automatisierte Verarbeitungsvorgänge können technisch auch auf den RFID-Tags ablaufen. Allerdings ist Voraussetzung, dass diese technisch mit Prozessoren ausgestattet sind, die eine automatisierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ermöglichen. Wegen der hohen Kosten derartiger Tags ist diese derartige technische Ausstattung nur von geringer praktischer Bedeutung. Unterstellt, die Voraussetzung wäre jedoch erfüllt und auf dem Prozessor-Tag würden auch personenbezogene Daten verarbeitet, dann wäre verantwortliche Stelle derjenige, der Daten auf diesen RFID-Tags für sich verarbeitet. Datenschutzrechtlich verantwortlich ist also die Stelle, die über die Steuerung des auf dem Prozessor installierten Programms, für eigene Zwecke personenbezogene Daten bspw. ihres Kunden oder Mitarbeiters erhebt, verarbeitet oder nutzt.

### 6.2.4 Zur Erfüllung eines Vertragsverhältnisses

Nach § 28 Abs. 1 S. 1 Nr.1 BDSG sind das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Im Handel werden über RFID personenbezogene Daten in einem Hintergrundsystem insoweit erhoben, als die Zuordnung von Produkten zu einzelnen Kunden erfolgt. Dies geschieht beispielsweise dadurch, dass der Kunde Produkte in seinen Warenkorb legt und diese in einem Hintergrundsystem erfasst werden. Die Zuordnung erfolgt zunächst nicht unmittelbar personenbezogen bis der Kunde sich beim Zahlungsvorgang über seine Kundenkarte oder seine Zahlungskarte authentifiziert. Es besteht jedoch ein Personenbezug, weil der Verbraucher jederzeit identifiziert werden kann, solange er das Geschäft noch nicht verlassen hat. Sofern sich der Kunde bereits beim Betreten des Ladens bspw. an dem Einkaufswagen über seine Kundenkarte authentifiziert, erfolgt die Zuordnung seiner Einkaufshandlungen unmittelbar zu seiner Person von Beginn an.

Die Verwendung der über den Einkaufsvorgang erhobenen Daten ist zu unterschiedlichen Zwecken denkbar.[248] Eine Rechtfertigung der Erhebung, Verarbeitung oder Nutzung über § 28 Abs. 1 Satz 1 Nr. 1 BDSG kommt nur insoweit in Betracht, als die Verarbeitung oder Nutzung unmittelbar dem Zweck der Vertragsanbahnung und Vertragsdurchführung dient und dafür auch erforderlich ist. Der Einkaufsvorgang als solcher ist dem Vertragsschluss unmittelbar vorgelagert und ist auch im Hinblick auf die Verkehrssicherungspflichten des Geschäftseigentümers als vertragsähnliches Vertrauensverhältnis einzuordnen. Soweit die Verarbeitung der über RFID ausgelesenen Informationen im Warenkorb des Kunden beispielsweise zum Zweck der Gesamtkaufpreisberechnung und –anzeige für den konkreten Kunden erforderlich ist, ist dies nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig. Eine Zusammenführung der Einkaufsdaten mit den Bestandsdaten der Zahlungskarte würde zwar auch der Vertragsabwicklung dienen, sie ist aber über die Gesamtsumme des Einkaufes hinaus nicht erforderlich und bedarf deshalb einer gesonderten Rechtsgrundlage außerhalb eines Vertragsverhältnisses.[249]

Im Fall der mit einem RFID-Chip versehenen Eintrittskarte ergibt sich der Personenbezug der auf dem Ticket gespeicherten Kennnummer zu ihrem Inhaber zunächst über den Zahlungsvorgang. Soweit dies nicht der Fall ist, weil das Ticket bar bezahlt worden ist, kann sich der Personenbezug aus dem Besitz des Tickets ergeben, wenn der Inhaber sein Ticket innerhalb des Veranstaltungsraums immer bei sich führen muss. Allerdings bedeutet das Auslesen der Kennnummer des Tickets noch nicht, dass der Inhaber auch automatisch als Person identifiziert wird. So kann die Kontrolle, dass nur berechtigte Personen mit einem Ticket den Veranstaltungsraum betreten, allein über den Besitz eines Tickets erfolgen, ohne dass es auf die Person des Ticketinhabers ankommt. Der Sachverhalt stellt sich jedoch anders dar, wenn über das Auslesen des Tickets auch die konkrete Person gezielt erfasst wird. Dies wäre bspw. der Fall, wenn im Rahmen einer Zugangskontrolle die Ticketinhaber photographiert würden. Vorstellbar wäre es auch, dass eine Identifikation des Ticketinhabers über das kontaktlose Auslesen einer anderen ID-Karte erfolgt.

Ein Personenbezug ist aus Gründen der Missbrauchsbekämpfung (Schwarzmarkt) und der Stadionsicherheit bspw. bei den WM-Tickets ausdrücklich beabsichtigt. Die Erfassung dient

---

[248] Zur Zweckbindung und Zweckänderung siehe auch Müller/Handy, DuD 2004, 655.

[249] So auch Holznagel/Bonnekoh, MMR 2006, 20.

in diesem Fall vorrangig nicht der Erfüllung des Vertragsverhältnisses mit dem Betroffenen, sondern den Geschäftszwecken des Veranstalters. Dies könnte anders zu bewerten sein, wenn die personenbezogene Erfassung der Ticketinhaber aus Gründen der Stadionsicherheit erfolgt. Die vertragliche Leistung wird sich regelmäßig nicht nur auf den Stadionzugang, sondern auch auf Nebenpflichten erstrecken, die einen sicheren Besuch des Stadions ermöglichen. Allerdings stößt eine solche Vertragsauslegung in Anbetracht der in der AGB-Praxis üblichen Haftungsausschlüsse des Stadionbetreibers an Grenzen, mit denen er eine Haftung für durch Dritte verursachte Schäden oder für Akte höherer Gewalt gerade ausschließen will.

### 6.2.5 Andere Zwecke: Wahrnehmung berechtigter Interessen

Personenbezogene Datenverarbeitungen, die nicht der unmittelbaren Vertragsanbahnung oder Vertragsdurchführung dienen, sind nicht durch die Rechtsgrundlage des § 28 Abs. 1 Satz 1 Nr. 1 BDSG abgedeckt, sie können jedoch zur Wahrung berechtigter Interessen der verantwortlichen Stelle nach Nr. 2 dieser Vorschrift erforderlich sein. Weitere Voraussetzung ist allerdings, dass kein Grund zu der Annahme bestehen darf, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt. Im Anwendungsbeispiel des Ticketfalls bestünde ein derartiges berechtigtes Interesse des Veranstalters darin, mit der personenbezogenen Zuordnung von Ticket und Inhaber die Fälschung von Tickets oder einen Schwarzmarkt zu unterbinden.

Dem stehen allerdings datenschutzrechtlich schutzwürdige Interessen der betroffenen Inhaber gegenüber, deren konkretes Interesse an einer bestimmten Veranstaltung, Ort und Zeit ihres konkreten Aufenthaltes einschließlich ihrer Begleitung nun für den Veranstalter transparent und verfügbar werden. Allein zur Abwehr von Fälschungen kann die Fälschungssicherheit des Tickets selbst erhöht werden, so dass eine personenbezogene Erfassung der Inhaber nicht erforderlich ist. Das wirtschaftliche Interesse, den Weiterverkauf erworbener Tickets zu unterbinden, rechtfertigt für sich genommen nicht, den Erwerb von Eintrittskarten zu Museen, Kinos, Theatern und Sportveranstaltungen jeder Art nur noch personenbezogen zu ermöglichen. Zum einen steht einer solchen Praxis das grundsätzliche Recht eines jeden Käufers entgegen, ein von ihm erworbenes Recht zum Besuch einer Veranstaltung, auch an Dritte zu veräußern. Dass knappe Güter auf dem Markt eine Preissteigerung erfahren, gehört zu den Regeln von Angebot und Nachfrage der durch Art. 2 Abs. 1 GG geschützten Abschlussfreiheit im Privatrechtsverkehr. Im Übrigen wäre eine solche Restriktion auch nicht erforderlich, weil sich ein etwaiger Schwarzmarkt zumindest dadurch beschränken lässt, dass nur eine begrenzte Anzahl von Tickets je Käufer abgegeben werden.

### 6.2.6 Andere Zwecke: Werbung, Markt- und Meinungsforschung

Soweit die verantwortliche Stelle die von ihr im Rahmen eines Erwerbs von Gütern oder Rechten erhobenen personenbezogene Daten für Zwecke der Werbung oder Markt- oder Meinungsforschung verwenden will, kann eine Verarbeitung oder Nutzung für diesen Verwendungszweck nach den einschlägigen Regelungen des Listenprivilegs nach § 28 Abs. 3

Satz 1 Nr. 3 BDSG erfolgen. Danach dürfen personenbezogene Daten der in dieser Regelung aufgeführten Merkmale wie z.B. Name, Anschrift und Geburtsjahr mit *einer* weiteren Angabe zur Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe für Zwecke der Werbung oder Markt- oder Meinungsforschung verarbeitet werden, soweit kein überwiegendes schutzwürdiges Interesse des Betroffenen anzunehmen ist und er einer Verwendung für Zwecke der Werbung, Markt- oder Meinungsforschung auch nicht widersprochen hat.

Ein Beispiel ist die Zusammenstellung der Eigenschaft „Käufer von Produkt A“ mit den weiteren Informationen der Liste wie Name, Anschrift und Geburtsjahr. Von diesem Listenprivileg nicht abgedeckt werden komplexere Zuordnungen von mehreren Produkten oder Merkmalen zu der Person des Verbrauchers. So ist insbesondere über das Listenprivileg die Erfassung von Standortdaten sowie der Einkaufswege des Verbrauchers im Geschäft nicht erfasst.

Für eine derart umfassende Auswertung des Kaufverhaltens kommt nur die bereits erwähnte Regelung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Unterstellt, der Geschäftsbetreiber habe an einer solchen Auswertung ein berechtigtes Interesse, so steht einer Anwendung entgegen, dass das schutzwürdige Interesse des Verbrauchers überwiegt, sein Kaufverhalten „bis zur Ladenkasse“ nicht von dem Betreiber des Geschäftes ohne seine Kenntnis und Zustimmung erfassen zu lassen. Damit ist eine Verwendung der vor der Einkaufskasse erfassten Verhaltensdaten des Verbrauchers in den Geschäftsräumen für Zwecke der Werbung oder Markt- oder Meinungsforschung nur auf der Grundlage einer Einwilligung des Betroffenen zulässig.[250] Entsprechendes gilt für das Anwendungsbeispiel des Ticketing. Auch hier gilt, dass bspw. einer vollständigen Erfassung der Bewegungen des Verbrauchers innerhalb der Veranstaltungsräume überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

### 6.2.7 Einwilligung

Soweit die Voraussetzungen einer gesetzlichen Erlaubnisnorm für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nicht vorliegen, bedarf es einer wirksamen Einwilligung des Betroffenen nach § 4 a BDSG. Diese setzt eine freiwillige und informierte Entscheidung des Betroffenen voraus, die schriftlich oder – als Ausnahme - in anderer angemessener Form zu erteilen ist.

Da die Erhebung personenbezogener Daten bei RFID-Anwendungen berührungslos und für den Betroffenen unsichtbar erfolgt, kann er auch den Zeitpunkt der ersten Erhebung nicht wahrnehmen. Die Einwilligung ist demnach so zu gestalten, dass sie vor der ersten Erhebung, Verarbeitung oder Nutzung erteilt wird.[251] Dies setzt aber voraus, dass die Betroffenen über die Datenerhebung ausreichend informiert werden. Bei einem RFID-Einsatz im Geschäftsumfeld könnte diese Information z.B. durch ein hinreichend großes Schild im Eingangsbereich erfolgen. Sinnvoll kann auch ein einheitliches Piktogramm sein, das in Anlehnung an das Zeichen für Videoüberwachung die Verbraucher auf eine RFID-Anwendung

[250] Vgl. auch Holznagel/Bonnoh, CR 2004, 20 f.

[251] Zum Zeitpunkt der Einwilligung siehe Simitis in: Simitis, BDSG, § 4 a, Rn. 29 ff.

aufmerksam macht. Jedoch setzt eine derartige Information voraus, dass den Verbrauchern die grundsätzliche Funktionsweise von RFID-gestützten Einkaufssystemen vertraut ist. Gleichwohl würde eine solche verkürzte Information den inhaltlichen Anforderungen an eine informierte Einwilligung nicht genügen, sondern nur generalisierend über die allgemeine Verarbeitungsart informieren. Darüber hinaus bedarf es auf den Einzelfall angepasster Informationen, aus denen der Betroffene entnehmen kann, wer zu welchem Zweck und zu welcher Zeit welche seiner Daten erhebt, verarbeitet oder nutzt.

Die bloße Information erfüllt allerdings noch nicht die Anforderungen an einen ausdrücklichen Erklärungsakt. Im Fall des RFID-Ticketing kann bspw. eine Einwilligung beim Buchungsprozess in schriftlicher Form oder auf elektronischem Wege (bei der Onlinebuchung) eingeholt werden. Bei einem Ticketerwerb für Dritte - z.B. als Geschenk – muss eine das informationelle Selbstbestimmungsrecht des Dritten angemessene Lösung gefunden werden. In Verkaufsräumen könnte die datenschutzrechtliche Einwilligung im Zusammenhang mit dem Erwerb einer Kundenkarte erfolgen, wenn diese vor einer ersten Identifizierungsmöglichkeit durch die verantwortliche Stelle abgegeben wird. In anderen Fällen muss sie bereits beim Betreten der Geschäftsräume vor einer ersten elektronischen Erfassung erfolgen.

### 6.2.8 Auslesen von Objektnummern durch Dritte

Denkbar ist, dass der Verbraucher mit über RFID gekennzeichneten Objekten („getagten Objekte“) ein beliebiges Geschäft betritt, in dem das Lesesystem des Geschäftsinhabers ihn an Hand seiner Kunden- oder Zahlungskarte identifiziert und während seines Aufenthaltes auch die Kennnummern der getagten Objekte erfasst, ausliest und speichert. Problematisch ist dies vor allem im Hinblick auf nicht deaktivierte RFID-Tags in Produkten, die bereits im Eigentum des Kunden stehen.

Der Geschäftsbetreiber würde in diesem Fall der Person des Kunden die Objektnummern von Produkten zuordnen können, sobald sich der Kunde ihm gegenüber bspw. über seine Kunden- oder Zahlungskarte authentifiziert hat. Unter der Voraussetzung, dass das System des Geschäftsbetreibers diese Kennnummern interpretieren kann[252], verfügt das Unternehmen über die Informationen zu den Dingen, die der einzelne Verbraucher bei sich trägt. An der Auswertung dieser Informationen wird der Geschäftsbetreiber auch ein wirtschaftliches Interesse haben, weil er auf diese Weise ein individuelles Profil über Vorlieben und Eigenschaften, aber auch die finanzielle Leistungsstärke der Person erstellen kann. Aber selbst wenn der Geschäftsbetreiber keine der Objektnummern interpretieren kann, so ermöglichen ihm diese Informationen, den Verbraucher bei seinem nächsten Besuch im Geschäft anhand der von ihm bereits gespeicherten Objektinformationen zu identifizieren.

Für diese Erhebung von fremden Objektinformationen und ihre Zuordnung zur Person ihres Trägers bedarf der Geschäftsbetreiber als der hierfür verantwortlichen Stelle einer Einwilli-

[252] Was insbesondere durch einen Zugriff auf die standardisierte EPC Global-Datenbank unproblematisch möglich ist.

gung des Verbrauchers.[253] Mangels eines Vertragsverhältnisses über diese Objekte scheidet § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Rechtsgrundlage aus. Auch § 28 Abs. 1 Satz 1 Nr. 2 dieser Vorschrift ist nicht einschlägig, weil die schutzwürdigen Interessen des Betroffenen im Fall einer heimlichen Erfassung seiner Objekte und ihre Zuordnung zu seiner Person in jedem Fall die Interessen des Geschäftsbetreibers überwiegen. Die gesetzlichen Tatbestände der Datenerhebung und -verarbeitung rechtfertigen keine heimliche und automatisierte Erhebung von fremden Objektinformationen an dem Betroffenen vorbei.

## 6.3 Transparenz

Im Hinblick auf die kontakt- und im Unterschied zu Barcodes auch sichtverbindungslose Erhebung und Verarbeitung personenbezogener Daten beim RFID-Einsatz gelten besondere Anforderungen an die Transparenz der Datenverarbeitung.[254]

### 6.3.1 Unterrichtung des Betroffenen

Im Fall einer Erhebung personenbezogener Daten beim Betroffenen ist dieser von der verantwortlichen Stelle nach § 4 Abs. 3 Satz 1 BDSG über seine Identität (Nr. 1), die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung (Nr. 2) und die Kategorien von Empfängern zu unterrichten (Nr. 3) (s.o. S. 46). Verantwortliche Stelle ist im Anwendungsbeispiel des Einkaufes von Produkten mit RFID-Tags der Betreiber des Ladengeschäftes, in dessen Hintergrundsystem die Informationen über das Einkaufsverhalten des Verbrauchers zusammengeführt werden. Entsprechendes gilt für den Betreiber der Veranstaltungsräume, in dessen System die Kennnummern der Tickets mit den Informationen über seinen Inhaber zusammengeführt werden.

Die Informationen aus den RFID-Tags können allerdings unter der Voraussetzung, dass sie nach Verlassen des Geschäftes bzw. der Veranstaltung nicht gelöscht worden sind, auch von Lesegeräten Dritter erfasst, ausgelesen und gespeichert werden. Soweit auf dem Tag lediglich eine Kennnummer gespeichert ist, die das Objekt mit einer eigenen Nummer versieht, fehlt es an der Eigenschaft des personenbezogenen Datums, so dass eine Verpflichtung zur Unterrichtung des Betroffenen nicht besteht. Der Personenbezug besteht jedoch, wenn die Objektinformationen im Zusammenhang mit Informationen über die Person von einem Dritten erhoben werden. Letzteres wird im Konsumentenbereich der Regelfall sein.

Werden Objektinformationen heimlich ausgelesen und mit der Person ihres Trägers zusammengeführt, so hat der Geschäftsbetreiber als der für die Lesegeräte und das Hintergrundsystem verantwortlichen Stelle, den Betroffenen über diese personenbezogene Erhebung im oben genannten Umfang nach § 4 Abs. 3 Satz 1 BDSG zu unterrichten.

---

[253] Holznagel/Bonnekoh, MMR 2006, 21.

[254] Zur Tansparenzanforderung beim RFID-Einsatz siehe Roßnagel/Müller, CR 2004, 625 (628).

### 6.3.2 Besondere Informationspflichten

Besondere Informationspflichten können sich aus § 6 c BDSG ergeben, wenn es sich bei der RFID-Anwendung um mobile personenbezogene Speicher- und Verarbeitungsmedien handelt. Der Begriff des mobilen personenbezogenen Speicher- und Verarbeitungsmediums ist vom Gesetzgeber in § 3 Abs. 10 BDSG definiert worden. Voraussetzung für ein solches Medium ist, dass es an den Betroffenen ausgegeben wird, auf ihm personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden und der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann. [255]

Die Anwendung der Transparenzregelungen des § 6 c BDSG setzt voraus, dass das Medium an den Betroffenen ausgegeben worden ist (§ 3 Abs. 10 Nr. 1 BDSG). Hierzu genügt es, wenn das Objekt, auf dem der Tag aufgebracht ist, dem Betroffenen ausgehändigt wird.[256] Betroffener ist allerdings nur, wessen Daten auf dem Medium gespeichert werden. Dies ist nicht der Fall, wenn lediglich Objektinformationen auf dem RFID-Tag abgelegt werden.

Auf RFID-Tags sind in der Regel Kennnummern der Objekte gespeichert, die über einen elektronischen Impuls von Lesegeräten ausgelesen werden. Soweit lediglich auf dem RFID-Tag gespeicherte Informationen ausgelesen werden, erfüllt das RFID-Tag nicht die Voraussetzung eines mobilen Speicher- und Verarbeitungsmediums im Sinne des § 3 Abs. 10 BDSG.[257] Diese Voraussetzung ist erst dann erfüllt, wenn es sich bei dem Tag um einen Prozessorchip handelt, auf dem personenbezogene Daten „über die Speicherung hinaus“ automatisiert verarbeitet werden können.[258] „Dumme“ Speicherkarten erfüllen diese Voraussetzung nicht,[259] denn der Begriff der automatisierten Verarbeitung setzt nach § 3 Abs. 2 Satz 1 BDSG vielmehr eine „Datenverarbeitungsanlage“ voraus, mit deren Hilfe personenbezogene Daten verarbeitet werden. Eine derartige automatisierte Datenverarbeitung erfolgt bei einfachen, mit einer Kennnummer versehenen Tags nicht auf dem Medium selbst, sondern im Hintergrundsystem, das den Auslesevorgang auslöst, die Daten erhebt, speichert und mit den Daten des Kunden zusammenführt. In diesem Fall gelten die Transparenzpflichten des Betreibers des Hintergrundsystems, der zur Information der betroffenen Verbraucher verpflichtet ist.

RFID-Tags erfüllen die Voraussetzungen des § 3 Abs. 10 BDSG, wenn sie über einen Prozessorchip verfügen, der eine aktive Verarbeitung personenbezogener Daten ermöglicht. Unter dieser Voraussetzung ist die Stelle, die sie in Verbindung mit anderen Objekten ausgibt, nach § 6 c Abs. 1 BDSG verpflichtet, den Betroffenen über ihre Identität und Anschrift,

---

[255] Zu den Einzelheiten vgl. Bizer in: Simitis, BDSG, § 3, Rn. 273 ff.

[256] Bizer in: Simitis, BDSG, § 3, Rn. 276.

[257] Bizer in: Simitis, BDSG, § 3, Rn. 277; Holznagel/Bonnekoh, MMR 2006, 21.

[258] Bizer in: Simitis, BDSG, § 3, Rn. 277.

[259] Bizer in: Simitis, BDSG, § 3, Rn. 277

über die Funktionsweise des Mediums und die Art der zu verarbeitenden personenbezogenen Daten sowie über seine Auskunfts-, Berichtigungs- und Löschungsrechte nach § 34 und § 35 BDSG und die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen zu informieren.

Von besonderer praktischer Bedeutung ist für die Verbraucher im Anwendungsbeispiel der RFID-gestützten Eintrittskarten die Anforderung nach § 6 c Abs. 1 Nr. 4 BDSG, über Maßnahmen bei Verlust oder Zerstörung des Mediums zu unterrichten. In diesem Fall entfällt die Funktionalität der Eintrittskarte als Zugangsberechtigung und damit die Gegenleistung des Verbrauchervertrages. Diese Informationspflicht unterstützt den Verbraucher also auch für den Fall eines Technikversagens, damit er seine vertragsmäßigen Rechte geltend machen kann.

Der besonderen Intransparenz der kontakt- und sichtverbindungslosen Funktechnik begegnet § 6 c Abs. 3 BDSG mit einer Hinweispflicht der verantwortlichen Stelle, dem Betroffenen die einzelnen Kommunikationsvorgänge anzuzeigen, die auf dem Medium eine Datenverarbeitung auslösen. Diese Hinweispflicht durch eine optische oder akustische Signalisierung bezieht sich auf Verarbeitungsvorgänge personenbezogener Daten auf dem Medium. Sie soll verhindern, dass eine Verarbeitung personenbezogener Daten von dem Betroffenen unbemerkt, z.B. beim Vorbeigehen an einem Terminal, ausgelöst wird.[260] Werden also Daten über den Betroffenen aus dem RFID-Tag bspw. ausgelesen, gespeichert oder verändert, so ist nach § 6 c Abs. 3 BDSG eine entsprechende Signalisierung vorzusehen.[261]

### 6.3.3 Auskunftsanspruch

Dem Betroffenen einer personenbezogenen Datenverarbeitung steht ein Auskunftsrecht gegen die verantwortliche Stelle nach § 34 Abs. 1 BDSG zu. Dabei ist über die zur Person des Betroffenen gespeicherten Daten, die Herkunft der Daten, die Empfänger oder Kategorien von Empfängern dieser Daten und den Zweck der Verarbeitung in der Regel unentgeltlich Auskunft zu erteilen.

Für den Fall des Einsatzes mobiler personenbezogener Speicher- und Verarbeitungsmedien hat die verpflichtete Stelle nach § 6 c Abs. 2 BDSG dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte und Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.[262]

Für den RFID-Einsatz bedeutet die Ausübung des Auskunftsrechts insbesondere, dass den Betroffenen Einblick in die in den Hintergrundsystemen über sie gespeicherten Informationen Einblick gewährt und deren weitere Nutzung und Weiterverarbeitung deutlich wird. Für das zusammenhängende Verständnis ist dabei auch die Möglichkeit einzuräumen, über ein Lesegerät die tatsächlich auf einem RFID gespeicherten Informationen auslesen zu können.

---

[260] Vgl. BT-Drs. 14/5793, S. 64.

[261] Bizer in: Simitis, BDSG, § 6 c, Rn. 71 ff.

[262] Bizer in: Simitis, BDSG, § 6 c, Rn. 57 ff.

Insbesondere gehört dazu auch, die Zugangsmöglichkeit zu möglicherweise verschlüsselt oder gegen Zugriff geschützten, auf dem RFID abgelegten Informationen zu eröffnen.

## 6.4 Risiken für den Verbraucher

Die Risiken des RFID-Einsatzes bestehen insbesondere in der Intransparenz der Technik, die es dem Systembetreiber erlaubt, einen erheblichen Informationsvorsprung gegenüber dem Verbraucher zu erreichen und so das Marktverhältnis einseitig zu beeinflussen.

Das verbraucherrechtliche Leitbild des mündigen Verbrauchers ist damit in besonderem Maße gefährdet, da detaillierte Verbraucherprofile in Hintergrundsystemen gebildet und ausgewertet werden können und die gewonnenen Informationen zur Steuerung des weiteren Konsums einsetzbar sind.

# 7 Empirische Untersuchung

## 7.1 Befragungen

Der Frage, ob und in welchem Umfang die Verbraucher die im rechtsanalytischen Teil dargestellten Rechte auch wahrnehmen, ging das ULD durch die vier folgenden Befragungen auf den Grund:

- **Befragung von Verbrauchern**
  Es wurden 500 Verbraucher in einer repräsentativen Telefonbefragung zu ihren Kenntnissen der Datenschutzrechte interviewt.
- **Befragung von betrieblichen Datenschutzbeauftragten**
  Es wurden 1.800 Fragebögen an betriebliche Datenschutzbeauftragte verschickt sowie darüber hinaus im Internet zum Download bereitgestellt. Das Ziel der Befragung bestand darin, die Wahrnehmungsdichte von Datenschutzrechten zu ermitteln.
- **Befragung von Verbraucherberaterinnen und -berater**
  In der dritten Befragung wurden 710 Verbraucherberaterinnen und Verbraucherberater zum Informationsgrad der Verbraucher und deren Wahrnehmung der Datenschutzrechte befragt.
- **Befragung der Aufsichtsbehörden als qualitative Experteninterviews**
  In einer vierten und letzten Befragung wurden zur Ergänzung und Überprüfung der Ergebnisse aus den vorgenannten Befragungen die Aufsichtsbehörden der Bundesländer zum Kenntnisstand der anfragenden Verbraucher und der Unternehmen befragt.

Nachfolgend werden zunächst die gewonnenen Erkenntnisse der jeweiligen Befragung je für sich dargestellt, abschließend wird ein Fazit über alle vier Befragungen gezogen. Im Kern zeigt die Verbraucherbefragung, dass die Verbraucher über Informationspflichten der Unternehmen und über ihre Auskunfts- bzw. Widerspruchsrechte relativ gut informiert sind, nach den Ergebnissen der Befragung der betrieblichen Datenschutzbeauftragten, ihre Rechte allerdings in nur geringem Maße wahrnehmen. Aus den Befragungen der Verbraucherberaterinnen und -berater und den Erkenntnissen der aufsichtsbehördlichen Experteninterviews lässt sich entnehmen, dass die Kenntnisse der Verbraucher im datenschutzrechtlichen Bereich relativ niedrig eingeschätzt werden.

## 7.2 Befragung der Verbraucher

Um Erkenntnisse zu erlangen, inwieweit die Verbraucher über ihre Datenschutzrechte informiert sind, beauftragte das ULD das Marktforschungsinstitut Produkt + Markt[263], eine exklu-

[263] Produkt + Markt, Markforschung Marketingberatung, Otto-Lilienthal-Straße 15, 49134 Wallenhorst.

sive, repräsentative telefonische Verbraucherbefragung durchzuführen. Produkt + Markt fungiert als Marktforschungsunternehmen mit langjähriger Erfahrung im Bereich von telefongestützten Befragungen. Es werden pro Jahr ca. 300.000 telefongestützte Befragungen durchgeführt. Damit zählt es laut „Context Magazin“[264] zu den Top 20 der deutschen Marktforschungsinstitute. Methodisch erfolgte die Befragung im Rahmen von CATI-Interviews (Computer Aided Telephone Interview), d.h. durch computer-gestützte Telefoninterviews, bei denen die Fragen vom Computerbildschirm abgelesen und die Antworten direkt digital erfasst werden. Aus der Grundgesamtheit der telefonisch Erreichbaren im Alter von 18 bis 70 Jahren (Haushalte mit mindestens einem Festnetzanschluss) wurde eine repräsentative, mehrstufig geschichtete Zufallsstichprobe nach Alter, Geschlecht, Bundesland und Ortsgrössenklasse mit 500 Teilnehmerinnen und Teilnehmern gezogen. Dabei wurde die Repräsentativität beim Alter, Geschlecht und bei der Ortsgrößenklasse durch die Einhaltung von Quoten gewährleistet.[265] Grundsätzlich wird die Repräsentativität durch die sog. Last-Birthday-Methode gewahrt, d.h. diejenige Person wird als Ansprechpartnerin bzw. Ansprechpartner für die Befragung ausgewählt, die im angerufenen Haushalt als letzte Geburtstag hatte. Inzwischen sind bei den Festnetzanschlüssen ältere Menschen allerdings überrepräsentiert, so dass Quotenkorrekturen deshalb nötig sind. Das Bundesland der befragten Verbraucher wurde über die Vorwahl ausgewählt und gesteuert.

Der Fragebogen[266] war so konzipiert, dass es bei den inhaltlichen Fragen – mit Ausnahme der offenen Fragen – meist drei Antwortvorgaben gab, die von den Interviewern am Telefon vorgelesen wurden.

Um sich von der Qualität des Verfahrens zu überzeugen, besuchten zwei Mitarbeiter des ULD zum Befragungsbeginn die CATI-Studios. Die für die Befragung vorgesehenen Telefoninterviewerinnen und Telefoninterviewer erhielten dabei eine kurze Einleitung in die Thematik des Datenschutzes und zu den Hintergründen der Studie. Außerdem wurden die einzelnen Fragen des Fragenkataloges inhaltlich durchgesprochen und Rückfragen der Interviewer geklärt. Die Mitarbeiter des ULD hatten dann die Möglichkeit, den ersten Interviews beizuwohnen und Verbesserungsvorschläge zur Formulierung des Einleitungstextes des Interviews einzuarbeiten. Die Interviews wurden innerhalb von drei aufeinander folgenden Tragen durchgeführt.

### 7.2.1 Die Befragung

Die Fragen des Telefoninterviews wurden vom ULD mit Unterstützung durch Produkt + Markt entwickelt. Die Befragung umfasste 13 Fragen und war auf eine Gesprächsdauer von ca. acht bis zehn Minuten angelegt. Über die so genannten „Screening-Fragen“ nach Alter, Ge-

[264] Context magazin, Jan. 2004.

[265] Die Repräsentativität wurde durch Quotenbildung beim Alter, Geschlecht und Ortsgrößenklasse auf der Grundlage von Angaben aus dem statistischen Jahrbuch hergestellt.

[266] Der Fragebogen befindet sich im Anhang S. A14 ff.

schlecht, Wohnortgröße wurde die quotenorientierte Repräsentativität der Studie abgesichert.

Zum Einstieg in den inhaltlichen Teil wurden die Verbraucher befragt, was ihnen spontan zum Thema Datenschutz einfiele und wo sie sich informierten, wenn sie Fragen zum Datenschutz hätten. Beide Fragen waren als offene Fragen ausgestaltet. Anschließend wurden die Befragten gebeten, drei Stichworte zu nennen, die sie mit Datenschutz assoziierten. Den Kern der Befragung stellte ein Szenario dar, in dem die Verbraucher gebeten wurden, sich vorzustellen, die Kundenkarte eines Handelsunternehmens zu nutzen. Es wurde beschrieben, welche Daten zu diesem Zweck vom Befragten erhoben würden, dass die gekauften Artikel auf einem elektronischen Konto zusammengetragen und dass die Nutzungsgewohnheiten ausgewertet werden könnten. Die Kundenkarte wurde als Anwendungsbeispiel gewählt, weil viele Verbraucher bereits eine Kundenkarte besitzen und sich daher einfach in die beschriebene Lage hineinversetzen können. Das Ziel bestand darin, die Kenntnisse der Verbraucher zu Informationspflichten der Unternehmen und ihren Auskunfts- bzw. Widerspruchsrechten zu ermitteln. Zu Beginn sollten die Befragten erklären, ob sie grundsätzlich Bedenken gegen die Nutzung einer Kundenkarte hegen. Zum Abschluss wurde den Verbrauchern mit einem weiteren Beispiel die Situation eines „cold calls“[267] geschildert. Der Sachbearbeiter einer Bank, bei der die/der Verbraucher/in ihr/sein Konto führt, bietet während eines Telefonanrufs einen Versicherungsvertrag an. Dabei wurde die Frage gestellt, ob die Bank zuvor hätte fragen müssen, ob diese mit einem solchen Anruf einverstanden sind. Bei den Antworten mussten sich die Verbraucher entscheiden, ob sie eine Zustimmung für erforderlich oder für nicht erforderlich hielten. Als dritte Möglichkeit konnten die Verbraucher angeben, dass eine vorherige Zustimmung zwar nicht erforderlich sei, im Verlaufe des Gesprächs allerdings darauf hingewiesen werden könnte, dass kein weiterer Anruf dieser Art erfolgen soll.

Für die Auswertung der Befragung hat das Marktforschungsunternehmen Produkt + Markt die Antworten der offenen Fragen typologisiert, dann sämtliche Antworten zur Erfassung kodiert und den Datensatz anschließend dem ULD zur Auswertung zur Verfügung gestellt. Die Auswertungen sämtlicher Befragungen sind mit Hilfe des Softwareprogrammes SPSS[268] durchgeführt worden.

[267] Ein zu Werbezwecken durchgeführter Anruf beim Verbraucher ohne dessen vorherige Zustimmung.

[268] Statistical Package for the Social Sciences.

### 7.2.2 Ergebnisse und Interpretation[269]

#### 7.2.2.1 Demografische Daten

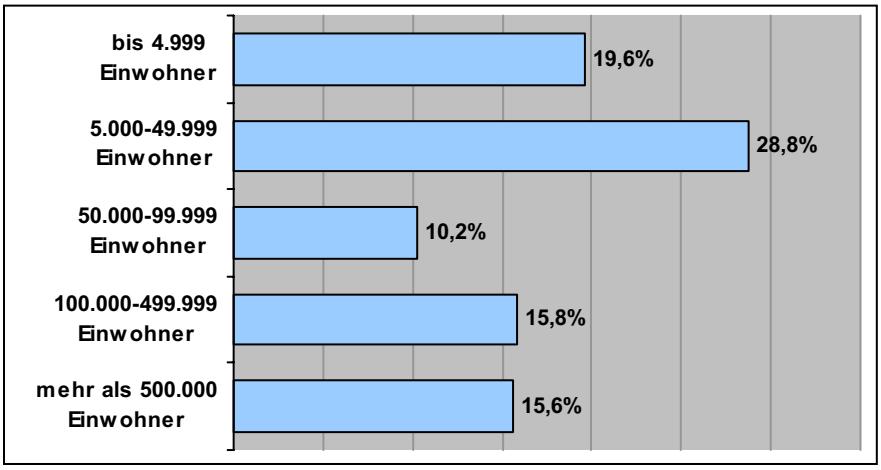
Die Alters- und Geschlechtsverteilung der Befragten setzte sich dabei wie folgt zusammen:

Tabelle 1: Alters- und Geschlechtsverteilung der Befragten

| Altersverteilung | | Geschlechtsverteilung | |
|---|---|---|---|
| Altersklasse | in % | Geschlecht | in % |
| 18 – 29 Jahre | 16,2 % | Frauen | 49,6 % |
| 30 – 44 Jahre | 35,6 % | Männer | 50,4 % |
| 45 – 59 Jahre | 28,2 % | | |
| 60 – 70 Jahre | 20,0 % | | |

Die Ortsgrößenverteilung der Befragten setzt sich dabei wie folgt zusammen:

Abbildung 1: Verteilung der Befragten auf die einzelnen Ortsgrößenklassen




[269] Die Auswertungen befinden sich im Anhang S. A19 ff.

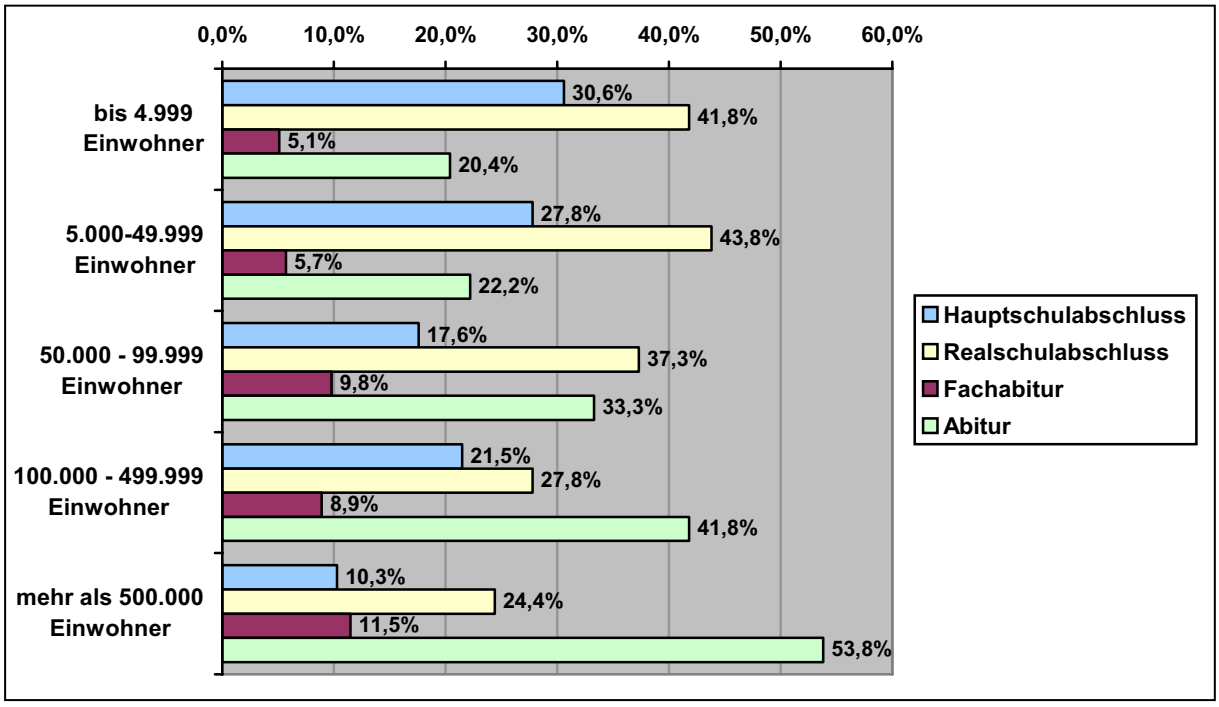
Die Schulbildung der Befragten setzt sich wie folgt zusammen:

Tabelle 2: Schulbildung der Befragten

| Schulbildung | in % |
|---|---|
| Keine Schulbildung | 0,4 % |
| Hauptschulabschluss | 23,6 % |
| Realschulabschluss | 37,2 % |
| Fachabitur | 7,4 % |
| Abitur | 31,0 % |
| Sonstige | 0,4 % |

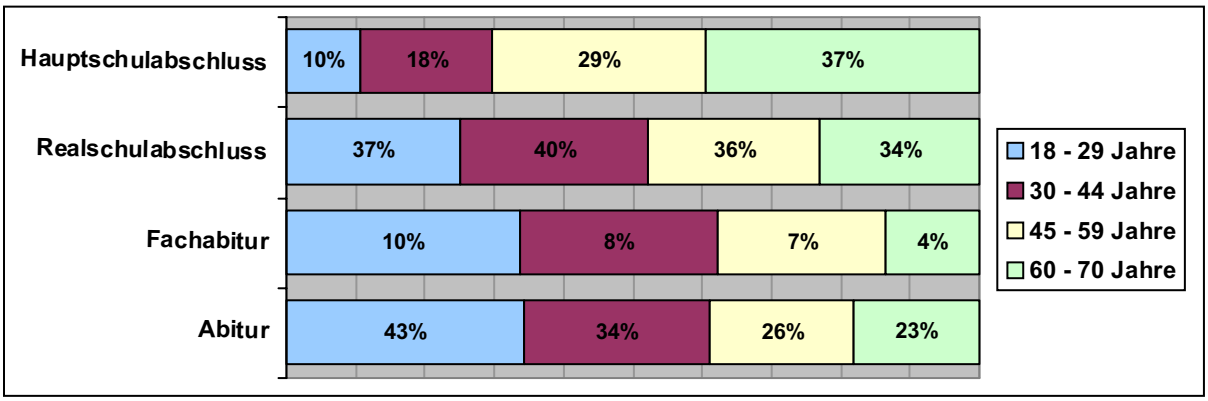
Die Verteilung der Befragten nach Schulabschluss und Ortsgrößen setzt sich wie folgt zusammen:

Abbildung 2: Schulabschlussverteilung je Ortsgrößenklasse



Die Altergruppen der Befragten verteilen sich dabei auf die Bildungsklassen wie folgt:

Abbildung 3: Altersgruppenverteilung je Bildungsklasse

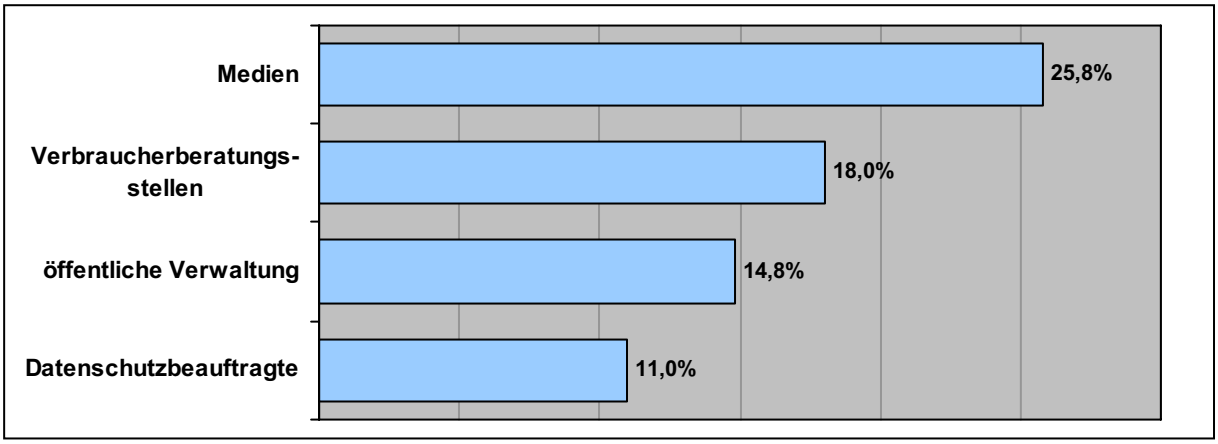



Die demografischen Angaben entsprechen aufgrund der quotenorientierten Befragung der allgemeinen statistischen Verteilung in der Bundesrepublik.

### 7.2.2.2 Assoziationen zum Thema Datenschutz und zuständige Stelle

Bei der Frage, wo sich die Verbraucher informieren würden, wenn sie Fragen zum Thema Datenschutz hätten, wird von den meisten Befragten das Stichwort „Medien“ genannt. So gaben 25,8% an, sich über Internet, Zeitungen oder Fernsehen zu informieren. Für 18% der Befragten seien die Verbraucherzentralen Anlaufstellen. 14,8% der Befragten würden sich an die öffentliche Verwaltung (Gemeinde, Ämter und Polizei) wenden. Nur 11% der Befragten nannten hingegen den Datenschutzbeauftragten, wobei hier die Angaben nach Bundes- und Landesdatenschutzbeauftragten sowie betrieblichen Datenschutzbeauftragten zusammengefasst wurden. 27% der Befragten machten keine Angaben zu dieser Frage.

Abbildung 4: Assoziationen zu möglichen Anlaufstellen im Falle von Datenschutzfragen



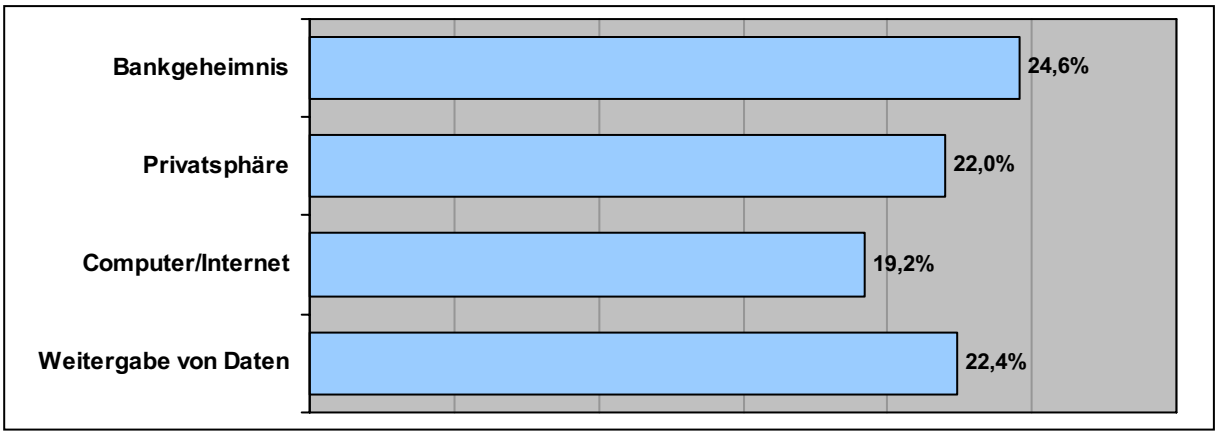

Die Verbraucher wurden ferner gebeten, drei Stichworte zu nennen, die ihnen spontan zum Thema Datenschutz einfielen.

Rund einem Viertel (24,6%) der Befragten fiel das Stichwort Bank im Zusammenhang mit dem Thema Datenschutz ein. Dabei ging es um das Bankgeheimnis, um Bankdaten, Konto-

nummer, Kreditkarten u.ä. In 22% der Fälle gaben die Befragten an, dass sie mit dem Thema Datenschutz persönliche Daten, Schutz personenbezogener Daten und Privatsphäre assoziierten. Für 19,2% der befragten Verbraucher ist das Thema Datenschutz mit dem Stichwort Computer, insbesondere Internet, Viren und E-Mail verknüpft. Auch die Übermittlung oder Weitergabe von Daten beschäftigen die befragten Verbraucher, wenn sie auf das Thema Datenschutz angesprochen werden. 8,4% der Befragten fielen spontan die Stichworte Weitergabe von Adressen bzw. Telefonnummern ein. 7,6% assoziierten „keine Weitergabe von Daten“ oder „Daten sind geschützt“. 6,4% nannten die (unerwünschte) Zusendung von Werbung bzw. unerwünschte Anrufe. Von 5,6% der Befragten wurde „Datenweitergabe“ bzw. „Verbreitung persönlicher Daten“ genannt. 1,6% der Verbraucher konstatierten „ohne Einwilligung keine Weitergabe von Daten bzw. Adressen“. Werden diese Zahlen zusammengefasst, so lässt sich feststellen, dass in 22,4% der Fälle Stichworte genannt wurden, die mit der Weitergabe von Daten zu tun haben.

Weitere Stichworte wurden aus den Bereichen Werbung, Kundenbindungssysteme und Auskunfteien geäußert. 2,4% der befragten Verbraucher fiel die ärztliche Schweigepflicht und 1,8% das Stichwort „Schufa“ als datenschutzrechtlich besonders sensible Bereiche ein. Weitere 2,4% nannten als Stichworte „Kundenkarte bzw. Einkaufsverhalten“. 2% äußerten sich zu unnötiger Datensammlung. Knapp 1% der Befragten teilten mit, dass sie mit Datenschutz das Sammeln von Adressen durch Preisausschreiben verbinden. 9,2 % der Befragten machten keine Angaben zu dieser Frage.

Abbildung 5: Assoziationen zum Thema Datenschutz




Man kann also konstatieren, dass Verbraucher beim Datenschutz vornehmlich an Aspekte des Bankgeheimnisses, an das Bewahren ihrer Privatsphäre ganz allgemein, an Gefährdungen der Sicherheit ihrer Computer sowie auch an die Weitergabe von Daten denken. Die ärztliche Schweigepflicht oder Kundenkarten spielten dagegen eine weitaus geringere Rolle. Wenn Verbraucher auf Datenschutzprobleme stoßen, dann informieren sie sich zunächst offenbar vor allem über das Internet.

Auffällig ist der Befund, dass den Verbrauchern die Datenschutzbeauftragten wenig bekannt sind. 1998 hatten bei einer repräsentativen Umfrage, die auch die Frage, an wen sie sich bei

einem Datenschutzverstoß wenden würden, nur 7% angegeben, dass sie den Datenschutzbeauftragten einschalten wollten.[270] In einer weiteren repräsentativen Umfrage gaben sogar 75% an, noch nie etwas vom Datenschutzbeauftragten gehört zu haben.[271] Ganz offensichtlich muss die öffentliche Darstellung der Aufgabe der Datenschutzbeauftragten bzw. Aufsichtsbehörden erheblich verbessert werden.

#### 7.2.2.3 Kenntnisse über Informationspflichten, Auskunfts- und Widerspruchsrecht

Die Verbraucher sind über die Informationspflichten der Unternehmen bei Datenverarbeitungen im Zusammenhang mit der Kundenkarte überwiegend gut informiert. 63,6% der Befragten gingen zutreffend davon aus, dass das Unternehmen sie über die Auswertung ihrer Kundendaten zum Zwecke der zielgerichteten Werbung informieren muss. Unter den Befragten, die in Großstädten zwischen 100.000 bis 499.999 Einwohnern leben, war der Anteil derjenigen, die die Frage richtig beantworteten, im Vergleich zu den anderen Ortsgrößenklassen mit knapp 70% am größten.

Bei der Frage, ob die Verbraucher beim Verkauf der Daten an Dritte zu informieren seien, lagen über Dreiviertel der Befragten mit ihrer Einschätzung richtig. So gingen 77,6% der Befragten davon aus, dass das Unternehmen zur Information verpflichtet sei. Dabei wussten die Befragten der Altersgruppe der 18- bis 29-Jährigen am besten Bescheid. Hier gaben sogar 87,7% die richtige Beurteilung ab. Dagegen waren die 60- bis 70-Jährigen von allen Altersgruppen am unsichersten. 26% vermuteten, dass das Unternehmen nicht zur Information verpflichtet sei. Für die Frage, ob ein Unternehmen beim Verkauf von Daten an Dritte auch den Namen des Dritten preisgeben muss, sind die Ergebnisse weniger eindeutig, 48,4% der Befragten nahmen zutreffend an, dass keine Informationspflicht besteht.

58,8% der Befragten gaben zutreffend an, dass sie gegen die Zusammenfassung ihrer Daten zum Zwecke des Überblicks über die Einkäufe, Widerspruch einlegen können. Das datenschutzrechtliche Instrument „Widerspruch“ wurde von den Befragten dabei allerdings nicht selbst genannt. Vielmehr enthielt eine der vorgegebenen Antwortmöglichkeiten die Formulierung, dass Widerspruch eingelegt werden könnte.

Am besten wussten die Verbraucherinnen und Verbraucher bei der Frage nach ihrem Auskunftsrecht Bescheid. 85,2% der Befragten gingen davon aus, dass das Unternehmen die Auskunft über die gespeicherten Daten nicht verweigern darf. Über den Auskunftsanspruch waren die Befragten der mittleren bis großen Städten (100.000 bis 499.999 Einwohner) am besten informiert. 91,1% lagen hier richtig. Die Befragten aus der Altersgruppe der 45- bis 59-Jährigen kannten sich am wenigsten aus. In dieser Altersgruppe nahmen fast 85% der Befragten an, dass das Unternehmen die Auskunft erteilen müsse.

Im Gegensatz zum Auskunftsanspruch kannten sich die Verbraucher bei der Frage zum Bankanruf als „cold call“ weniger gut aus. 9% hielten ihre vorherige Zustimmung zu einem

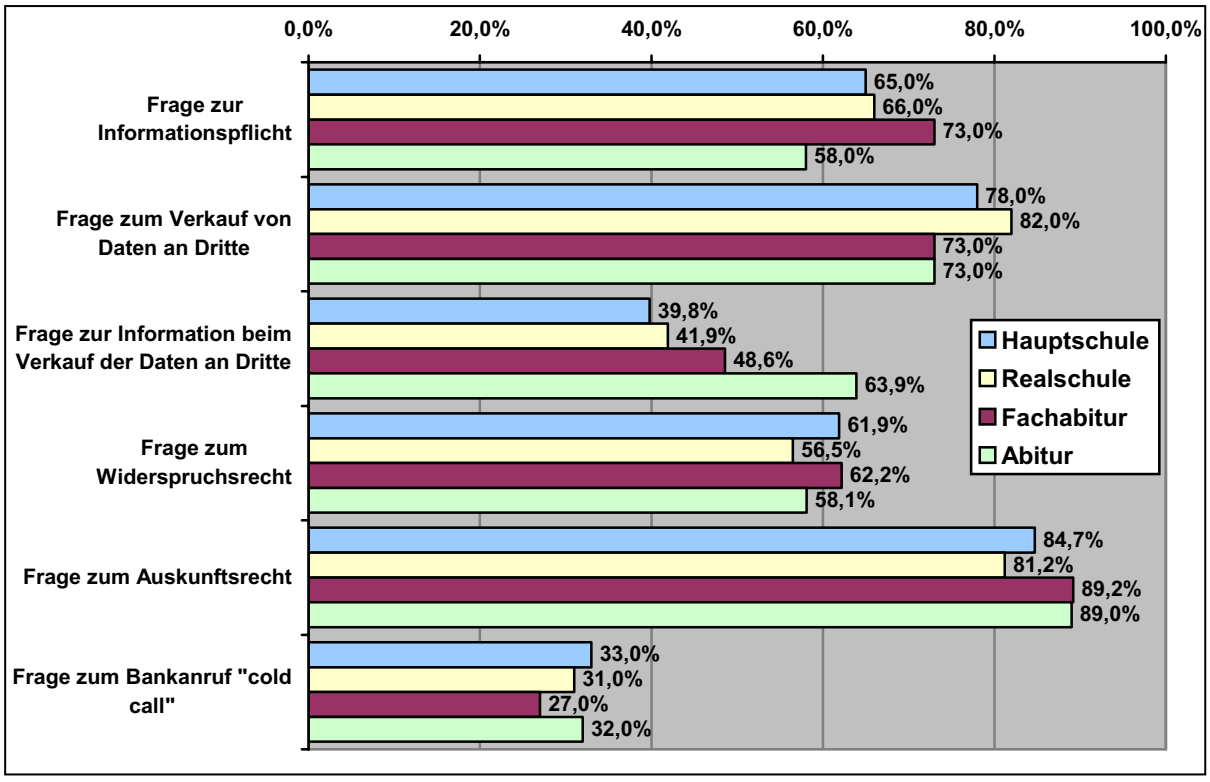
[270] Opaschowski, DuD 1998, 656

[271] Opaschowski, DuD 2001, 680

derartigen Anruf für nicht erforderlich. 57,6% gingen ebenfalls davon aus, dass die Zustimmung nicht erforderlich sei, die Verbraucher den Anrufer allerdings darauf hinweisen könnten, weitere Anrufe dieser Art zu unterlassen. 31,8% nahmen zutreffend an, dass sie zuvor ihre Einwilligung zu dem Anruf hätten erteilen müssen. Die Befragten zwischen 60 und 70 Jahren wussten in diesem Fall am besten Bescheid. Mit 40% gingen sie zutreffend davon aus, dass sie vorher in einen derartigen Anruf einwilligen müssen. Bei den 18- bis 29-Jährigen lagen 22% richtig.

Der Bildungsstand spielt für die Kenntnisse der Verbraucherinnen und Verbraucher im Bereich der datenschutzrechtlichen Informationspflichten und der Auskunfts- bzw. Widerspruchsrechte keine Rolle. Bei den Fragen nach den Pflichten zur Information über die Auswertung der Kundendaten und den Verkauf der Daten an Dritte wussten die Befragten mit Haupt- und Realschulabschluss tendenziell besser Bescheid als solche mit Abitur oder Fachabitur. Bei den Fragen nach der Pflicht zur Information über den Namen des Dritten und nach dem Anspruch auf Auskunft waren die Befragten mit dem höheren Bildungsstand tendenziell besser informiert. Für die Fragen nach dem Widerspruchsrecht und dem Zustimmungserfordernis beim Anruf der Bank lassen sich keine entsprechenden Unterschiede ausmachen.

Abbildung 6: Häufigkeit der zutreffenden Antworten in den einzelnen Bildungsklassen



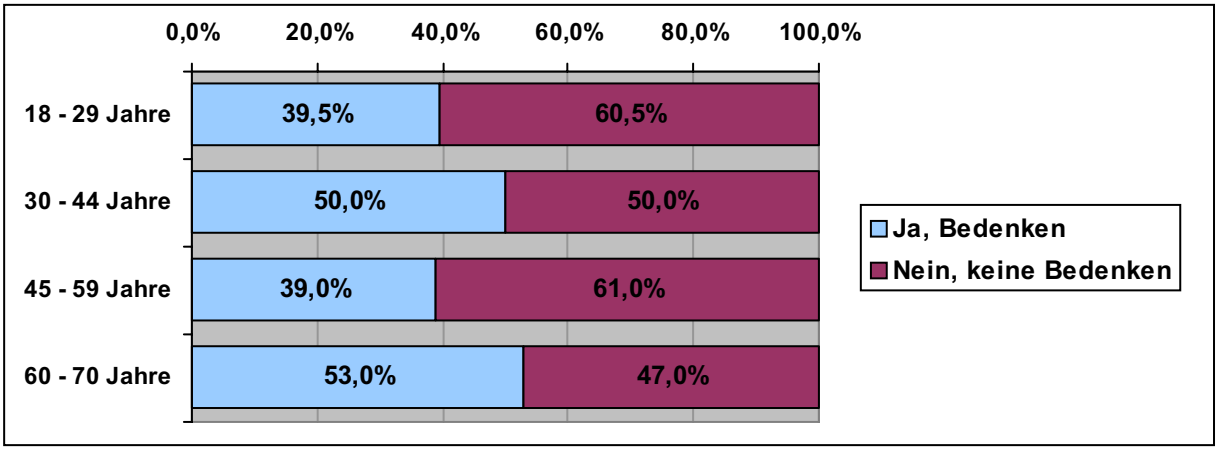

Man kann somit festhalten: Die Verbraucher sind über die Informationspflichten der Unternehmen und über das Widerspruchsrecht ganz überwiegend gut, über ihren Auskunftsanspruch sogar sehr gut informiert. Das allein besagt aber noch nicht, dass die Kenntnis über die Datenschutzrechte auch zu ihrer Einforderung führt. Die Kenntnis der Datenschutzrechte

ist von Unterschieden im Einzelnen abgesehen nicht an die Bildung der Verbraucher gebunden.

#### 7.2.2.4 Bedenken gegen die Nutzung einer Kundenkarte

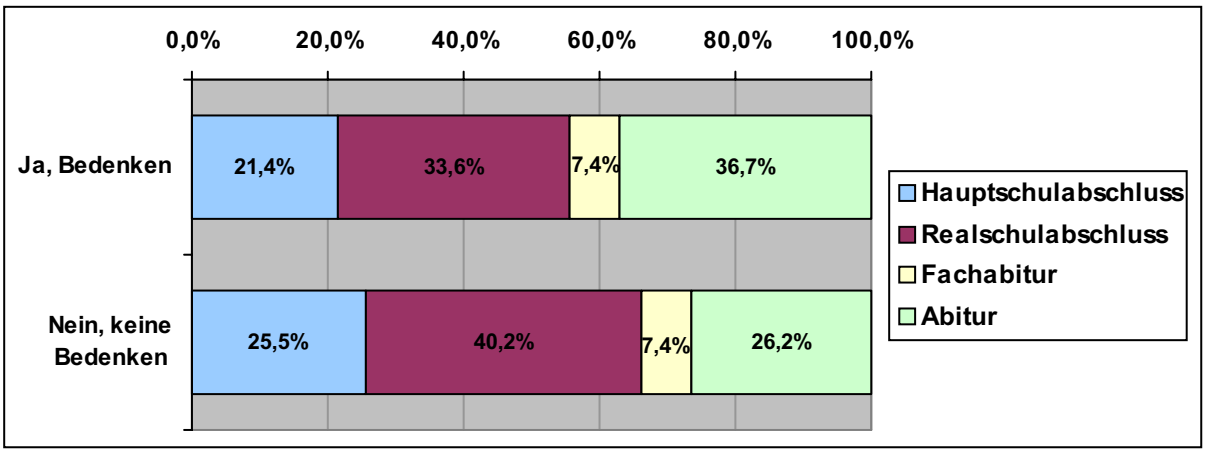
In Bezug auf die Nutzung einer Kundenkarte hegen 54,2% der Befragten keine grundsätzlichen datenschutzrechtlichen Bedenken. Die geringsten Bedenken haben die Verbraucher im Alter zwischen 18 und 29 sowie zwischen 45 und 59 Jahren. Hier antworteten 60,5% bzw. 61% der Teilnehmer, dass sie keine Bedenken hätten. Die Befragten der Altersgruppe zwischen 60 und 70 Jahren stehen der Kundenkarte in der Mehrheit eher zögerlich gegenüber. Hier äußerten 53%, dass sie Bedenken gegen deren Nutzung hegen. Hierbei darf man vermuten, dass ältere Verbraucher tendenziell weniger von Datenschutzbedenken getragen sind als von einer Zurückhaltung bzw. eher skeptischen Haltung gegenüber allem, was sie nicht schon länger kennen. Bewohner größerer Städte äußerten sich tendenziell eher skeptischer als Bewohner kleinerer Städte, ebenso wie Männer leicht skeptischer als Frauen eingestellt sind.

Abbildung 7: Verteilung der Antworten bei der Frage nach den Bedenken gegen die Nutzung einer Kundenkarte je Altersgruppe




Bei den Bedenken gegen die Kundenkarte zeigt sich in Bezug auf den Ausbildungshintergrund ein etwas klareres Bild. 36,7% derjenigen, die Bedenken hegen, haben Abitur; 33,6% der Befragten, die Bedenken haben, besitzen einen Realschulabschluss, 21,4% mit zögerlicher Haltung haben einen Hauptschulabschluss.

Abbildung 8: Häufigkeit der einzelnen Schulabschlüsse bei denjenigen, die Bedenken gegen die Nutzung einer Kundenkarte haben und bei denjenigen, die keine haben




Sowohl innerhalb der Gruppe der Hauptschüler als auch bei den Realschülern sind diejenigen Befragten eindeutig in der Mehrheit, die keine Vorbehalte gegen eine Kundenkarte haben (58,5% bzw. 58.6%).

### 7.2.3 Zusammenfassung der Ergebnisse der telefonischen Verbraucherbefragung

Die Verbraucherinnen und Verbraucher sind relativ gut bzw. tendenziell sogar sehr gut über ihre Auskunftsrechte, über die Möglichkeit zum Widerspruch sowie über die Informationspflichten der Unternehmen informiert. Der Kenntnisstand der Verbraucher, die in den großen Städten mit 100.000 Einwohnern und mehr leben, ist im Vergleich zu den Bewohnern anderer Ortsgrößen am höchsten. Die jüngeren Befragten, insbesondere in der Altersgruppe zwischen 18 und 29 Jahren, wissen häufig etwas besser Bescheid über ihre Rechte als die Älteren.

Der Bildungsstand der Befragten wirkt sich dagegen eher nicht auf die rechtlichen Kenntnisse der Befragten aus. Es ist keine klare Tendenz zu erkennen, dass die Befragten mit einem höheren Bildungsniveau – Abiturienten und Fachabiturienten – sich bei ihren Datenschutzrechten besser auskennen. Vielmehr wussten mal die Befragten mit Hauptschul- und Realschulabschluss, mal die Abiturienten und Fachabiturienten besser Bescheid. Der Schwierigkeitsgrad der einzelnen Fragen ist in etwa gleich, so dass auch kein Rückschluss gezogen werden kann, dass die Befragten mit höherem Bildungsstand im Bereich der schwierigeren Fragen besser informiert waren.

Das Bildungsniveau der Befragten macht sich allerdings dann doch leicht bemerkbar, wenn konkret nach der Nutzung von Kundenkarten gefragt wird. Die vergleichsweise etwas größere Vorsicht der Befragten mit höherem Bildungsstand in Bezug auf die Kundenkarte ließe sich möglicherweise darauf zurückführen, dass diese eher eine Vorstellung davon entwickeln, wie herausgegebene Daten möglicherweise für andere, unter Umständen auch für nachteilige Zwecke im Gegensatz zu der als Vorteil wahrgenommenen Rabattgewährung, genutzt werden könnten.

Nicht zuletzt zeigt diese Befragung, dass der Datenschutzbeauftragte bzw. die Aufsichtsbehörde als erste Anlaufstelle für Datenschutzkonflikte relativ unbekannt ist.

## 7.3 Befragung der betrieblichen Datenschutzbeauftragten (bDSB-Befragung)

Bei der Befragung der betrieblichen Datenschutzbeauftragten ging es im Schwerpunkt um die Frage der Wahrnehmung der Datenschutzrechte bei den Unternehmen durch die Verbraucher. Als für datenschutzrechtliche Anfragen der Kunden zuständige Stelle im Unternehmen boten sich die betrieblichen Datenschutzbeauftragten als Ansprechpartner für eine derartige Befragung an.

### 7.3.1 Durchführung

Die Befragung wurde vermittels eines Fragebogens durchgeführt. Sowohl bei der Entwicklung des Fragebogens als auch bei der Ausführung der Befragung stand die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)[272] dem ULD mit Anregungen und Hilfestellung zur Seite.

Die GDD unterstützt als gemeinnütziger Verein die im Sinne des BDSG verantwortlichen Stellen, insbesondere die betrieblichen Datenschutzbeauftragten bei der Bewältigung der datenschutzrechtlichen Anforderungen im Umgang mit personenbezogenen Daten. Die Gesellschaft wurde 1977 gegründet und hat inzwischen mehr als 1.700 Mitglieder. Damit betreut sie eine große Anzahl von betrieblichen Datenschutzbeauftragten und war somit ein idealer Partner, um die Zielgruppe der Befragung zu erreichen.

Um den Mitgliedern aktuelle und praxisbezogene Informationen zu Datenschutz und Datensicherheit zukommen zu lassen und über die aktuelle Arbeit der GDD zu berichten, gibt die Gesellschaft ein Mitteilungsblatt (GDD-Mitteilungen) heraus. Der Fragebogen des ULD wurde als Beilage zu der GDD-Mitteilung 3-4/2005 1.800-mal an die Mitglieder verschickt.

Zusätzlich wurde der Fragebogen zusammen mit einer Kurzinformation zur Studie im Internet unter der Seite http://www.datenschutzzentrum.de/verbraucherdatenschutz/ zum Download bereitgestellt.

Darüber hinaus wies der Vorstand des Berufsverbands der Datenschutzbeauftragten Deutschlands e.V. (BvD)[273] als Interessenvertretung der Datenschutzbeauftragten seine Mitglieder im Rahmen einer Rundmail auf den Fragebogen im Internet hin.

Der Einsendeschluss für den Fragebogen wurde zunächst auf den 15. Juli 2005 festgelegt. Aufgrund des relativ geringen Rücklaufs bis zu diesem Zeitpunkt, bedingt durch die Zeit der Sommerferien, verlängerte das ULD die Möglichkeit zur Abgabe der Fragebögen. Die letzten

[272] Gesellschaft für Datenschutz und Datensicherung e.V., Pariser Str. 37, 53117 Bonn.

[273] Berufsverband der Datenschutzbeauftragten Deutschlands e.V., Geschäftsstelle Gladbeck, Hegemannsweg 32, 45966 Gladbeck.

berücksichtigten Fragebögen gingen am 2. September 2005 ein, d.h. der Datenbestand für die Auswertung wurde auch nach dem Zwischenbericht noch einmal erweitert.

Bis zu diesem endgültig letzten Termin der Einsendung beträgt der Rücklauf 192 Fragebögen.

### 7.3.2 Fragebogen

Der Fragebogen[274] zur Befragung der betrieblichen Datenschutzbeauftragten enthält insgesamt 22 Fragen und wurde vom ULD mit Unterstützung der GDD entwickelt.

Der Fragebogen lässt sich inhaltlich in fünf Teile unterteilen. Mit den ersten fünf Fragen wird die Art des befragten Unternehmens ermittelt, d.h. Größe, Kundenzahl, Tätigkeitsbereich, Branche sowie die Funktion der Person des Befragten (Fragen 1-5).

Beim zweiten Teil (Fragen 6-10) geht es um den Kernpunkt der Befragung, die Wahrnehmung der Datenschutzrechte durch die Verbraucher. Mit insgesamt fünf Fragen wird ermittelt, in welcher Häufigkeit die befragten Unternehmen Anfragen auf Auskunft, Widersprüche oder Löschungsbegehren jeweils erhalten und welche weiteren Anfragen bzw. Beschwerden die Kunden an die Unternehmen richten. Außerdem sollen die betrieblichen Datenschutzbeauftragten auf einer Skala von 1-5 den Informationsgrad der Kunden bezogen auf ihre Datenschutzrechte einschätzen (Frage 18).

Mit den nächsten drei Fragen (Fragen 11-13) werden nur solche Unternehmen angesprochen, die Kundendaten auf der Grundlage einer Einwilligung erheben, verarbeiten und nutzen. Die anderen Befragten sollten diese Fragen überspringen. Inhaltlich werden Erkenntnisse über die Gestaltung der Einwilligung als Opt-In- bzw. Opt-Out Lösung und über den Anteil der Kunden angestrebt, die eine Einwilligung verweigern bzw. widerrufen. Unter dem Begriff Opt-In werden im Fragebogen solche Gestaltungen erfasst, bei denen die betroffenen Personen aktiv dem Verarbeitungsprozess zustimmen müssen. Wird die Zustimmung verweigert, ist keine Einwilligung gegeben. Als Opt-Out wird im Fragebogen eine solche Gestaltung bezeichnet, bei der die Einwilligung automatisch mit Unterschrift als erteilt gilt. Wollen die Kunden nicht in die Verarbeitung einwilligen, müssen sie mit Durchstreichen oder Setzen eines Kreuzes der Einwilligung widersprechen.

Im vierten Teil (Fragen 14-17) geht es um die interne Organisation beim Umgang mit Datenschutzanfragen. Es werden die Zuständigkeiten für die Bearbeitung von Auskunftsanfragen, Widersprüchen, Löschungsbegehren und widerrufenen Einwilligungen erfragt. Außerdem wird der Grad der Beteiligung der betrieblichen Datenschutzbeauftragten an der Gestaltung von Einwilligung, Allgemeinen Geschäftsbedingungen und Datenschutzhinweisen ermittelt (Frage 19).

Zuletzt (Fragen 20-22) wird den befragten betrieblichen Datenschutzbeauftragten die Gelegenheit gegeben, zu Verbesserungsmöglichkeiten im Verbraucherdatenschutz Stellung zu beziehen. Erfragt werden der wirkungsvollste Zeitpunkt der Belehrung und Information der

[274] Der Fragebogen befindet sich im Anhang S. A43 ff.

Kunden, die Bedeutung bestimmter Informationen für einen guten Verbraucherdatenschutz, die sinnvollsten Instrumente und Maßnahmen zur Erreichung eines guten bzw. zur Verbesserung des Verbraucherdatenschutzes.

In den meisten Fällen enthält der Fragebogen Antwortvorgaben zum Ankreuzen. Bei insgesamt neun Fragen bestand für die Befragten die Möglichkeit, eine freie Antwort zu geben.

### 7.3.3 Methoden der Auswertung

Von den 192 zurückgeschickten Fragebögen wurden diejenigen aussortiert, deren Bearbeitung sich nicht auf die Verarbeitung von Verbraucherdaten bezog. Drei der befragten Unternehmen gaben an, keine Verbraucher sondern fast ausschließlich juristische Personen als Kunden zu haben. Die Antworten wurden nicht mit in die Auswertung einbezogen, um die Ergebnisse nicht zu verfälschen. Die Angaben aus 189 ausgefüllten Fragbögen stellen danach die Grundlage für die Auswertung dar.

#### 7.3.3.1 Keine Angabe

Nichtbeantwortete Fragen – mit Ausnahme der fehlenden Antworten auf die Fragen zur Nutzung der Einwilligung (Fragen 11-13) – wurden als „keine Angabe“ gewertet. Bedeutung erlangt diese Bewertung bei der Berechnung der Prozentanteile. Die im Rahmen des Gutachtens genannten Prozentangaben beziehen sich immer auf die „valid percentage“, d.h. die Antwort „keine Angabe“ wird bei der Anzahl der Fälle, von der für die Berechnung des Prozentanteils ausgegangen wird, nicht mitberücksichtigt.

Im Falle der Fragen 11-13, die sich auf die Verarbeitung von Kundendaten auf der Grundlage einer Einwilligung beziehen, wurde die Nichtbeantwortung als „keine Nutzung einer Einwilligung“ gewertet. Der Fragebogen enthielt zur Einleitung der Fragen 11-13 den Hinweis, dass die Teilnehmer, in deren Verantwortungsbereich Kundendaten nicht auf Grund einer Einwilligung verarbeitet werden, die folgenden Fragen auslassen und mit Frage 14 fortfahren sollten. Die Nichtbeantwortung der Fragen 11-13 lässt daher den Rückschluss zu, dass die Teilnehmer die Einwilligung nicht als Verarbeitungsgrundlage nutzen.

#### 7.3.3.2 Offene Fragen

Der Fragebogen enthält neun Möglichkeiten zur freien Antwort. Inhaltlich gleichartige Antworten auf diese offenen Fragen wurden jeweils in Gruppen zusammengefasst, die Gruppen mit Schlagwörtern der Antworten benannt und als eigene Antwortkategorie kodiert. Unter „Sonstiges“, „Andere“ bzw. „Weitere“ wurden die Antworten gesammelt, die zu selten genannt wurden, um eine eigene Gruppe zu eröffnen und sich zu sehr von anderen Antworten unterschieden, um einer anderen Gruppe zugeordnet werden zu können.

Bei der Frage nach der Funktion des ausfüllenden Teilnehmers (Frage 5) ist neben den Antwortvorgaben auch ein Feld „Keine der vorangegangenen Funktionen, sondern …“ vorgese-

hen. Hier wurden alle verschiedenen Antworten als eigenständige Gruppe erfasst und damit insgesamt 15 Gruppen gebildet.

Bei der Frage 9 zu „weiteren Anfragen/Beschwerden … im Hinblick auf die Verarbeitung von Kundendaten“ wurden elf Gruppen gebildet, wobei eine Gruppe als „Sonstiges“ und eine Gruppe als „Keine“ bezeichnet wurde. In die Kategorie „Keine“ wurde sowohl eingeordnet, wer in der Antwort das Wort als solches niedergeschrieben hatte, als auch diejenigen, die mit einem Strich kenntlich machten, derartige Anfragen bisher nicht erhalten zu haben.

Bei Frage 10 bestand für die Teilnehmer die Möglichkeiten, den jeweiligen Anteil der einzelnen vorgegebenen Arten von Anfragen – Auskunft, Widerspruch, Löschung – und den Anteil „weiterer“ datenschutzrechtlichen Anfragen an der Gesamtheit aller datenschutzrechtlichen Anfragen in Prozent zu bestimmen. Bei der Auswertung dieser Frage wurden nur die Antworten berücksichtigt, bei denen die Prozentangaben rechnerisch auf 100% summiert werden konnten. Trugen die Befragten anstelle einer Prozentangabe einen Strich in das dafür vorgesehen Feld ein, so wurde der Strich als „0%“ gewertet. Ebenfalls mit „0%“ wurde erfasst, wer die Frage mit „N/A“ (d.h. „nicht anwendbar“) kennzeichnete. Diese Teilnehmer konnten die Frage nicht beantworten, da sie im Rahmen ihrer Tätigkeit offensichtlich bisher noch keine Anfragen mit datenschutzrechtlicher Relevanz erhalten hatten. Für die freie Antwort im Textfeld „Weitere“ wurden zwei Gruppen gebildet. Die Antworten mit dem Wort „Keine“ wurden in gleichnamiger Gruppe erfasst. Alle anderen Antworten ließen sich nicht in Gruppen mit inhaltlich konformen Antworten einteilen, sondern nur unter dem Oberbegriff „Weitere Anfragen“ sammeln.

Bei den Fragen nach der Zuständigkeit für die Bearbeitung einzelner Datenschutzanfragen (Auskunft, Widerspruch, Löschung und Widerruf der Einwilligung) Fragen 14-17 bestand neben den Antwortvorgaben auch die Möglichkeit, in dem Textfeld „Andere“ eine offene Antwort zu geben. Die Fragen 14-17 wurden im Hinblick auf die Gruppierung zusammengefasst und insgesamt 28 Gruppen gebildet. Erfasst wurden hier nicht nur die offenen Antworten. Auch Mehrfachnennungen der Antwortvorgaben wurden je nach Kombination in zusätzlichen Gruppen zusammengefasst und so als weitere Antworten kodiert.

Für die Frage 20 nach dem wirkungsvollsten Zeitpunkt der Information der Kunden war eine Zusammenfassung der Antworten unter dem Aspekt der inhaltlichen Gleichartigkeit nicht möglich. Die Antworten konnten nur unter „Andere“ gesammelt werden.

Bei Frage 22 nach dem besten Instrument zur Erreichung eines guten Verbraucherdatenschutzes wurden insgesamt drei Gruppen gebildet, wobei eine Gruppe mit „Andere“ gekennzeichnet wurde und eine andere Gruppe Mehrfachnennungen der Antwortvorgaben erfasst.

#### 7.3.3.3 Mehrfachnennungen

Wie bereits beschrieben, wurden Mehrfachnennungen bei solchen Fragen, die auch eine offene Antwort zulassen, als eigene Gruppe kodiert und ausgewertet.

Mehrfachnennungen bei anderen Fragen wurden unter einer der Antwortvorgaben subsumiert, entsprechend kodiert und ausgewertet. Es ergaben sich nachfolgend dargestellte Einzelfälle:

Bei Frage 4 gab einer der Befragten an, dass das Unternehmen aus dem Bereich Einzelhandel komme, wobei er das Wort „Einzelhandel“ ausstrich und mit den Worten „Groß- und Außenhandel“ überschrieb. Diese Antwort wurde so gewertet als käme das befragte Unternehmen aus keinem der vorgegebenen Bereiche.

Im Rahmen der Frage 6 nach der Anzahl der Anfragen auf Auskunft unterschied ein Teilnehmer zwischen Kundenanfragen und Mitarbeiteranfragen und setzte deshalb zwei Kreuzchen. Hier wurde nur die Antwort gewertet, die sich auf die Kundenanfragen bezog.

Bei Frage 7 nach der Anzahl der Widersprüche wurde in zwei Fällen sowohl die Antwortvorgabe „Trotz der Möglichkeit zum Widerspruch keine“ als auch die Vorgabe „Diese Frage ist für unser Unternehmen nicht relevant“ angekreuzt. Bei diesen Fällen der Mehrfachnennung wurde davon ausgegangen, dass für die Unternehmen kein Widerspruch in Frage kommt und deswegen die Antwort unter der zweiten hier genannten Antwortmöglichkeit subsumiert. Die erste Antwort sollte nur solche Fälle erfassen, bei denen ein Widerspruch grundsätzlich möglich ist.

Im Rahmen der Frage nach der Ausgestaltung der Einwilligungserklärung (Frage 11) wurde die Mehrfachnennung sowohl „Opt-In“ als auch „Opt-Out“ mit einer neuen Antwortkategorie „Beides wird genutzt“ kodiert und ausgewertet.

#### 7.3.3.4 Einzelfälle besonderer Kodierung

Bei den Prozentangaben in Frage 10 nach den Anteilen der einzelnen Kundenbegehren wurden keine Prozentangaben mit Kommastelle kodiert. In zwei Fällen wurde das Ergebnis daher schon bei der Kodierung interpretiert. In einem Falle hatte die/der Befragte angegeben, dass 99,9% Auskunftsbegehren und 0,01% sonstige Anfragen geltend gemacht werden. Kodiert wurden diese Angaben mit 100% und 0%, da eine nähere differenzierte Erfassung nicht möglich war. Mit der Frage sollte festgestellt werden, von welchen Datenschutzrechten die Verbraucher tendenziell am häufigsten Gebrauch machen. In diesem Sinne wurde die Frage auch von den meisten Teilnehmerinnen und Teilnehmern verstanden und entsprechend mit geschätzten, d.h. ungefähren runden Prozentangaben beantwortet. Diese Prozentangaben wurden zur Grundlage der Auswertung gemacht, so dass der in Rede stehende Einzelfall angepasst und in der Tendenz kodiert wurde.

In einem weiteren Fall hatte die/der Befragte Prozentangaben in Höhe von 0,5% gemacht. Auch hier wurde unter Berücksichtigung der Tendenz kodiert, d.h. die Angaben wurden auf 1% aufgerundet.

Bei zwei Fragebögen wurde Frage 10 beantwortet, ohne dass die Summe der Prozentangaben 100% oder 0% ergab. Aus den Antworten war jedoch ersichtlich, was die/der Befragte mit ihrer/seiner Angabe zum Ausdruck bringen wollte, so dass nach diesen Vorgaben die Zahlen auf 100% aufgerechnet und so kodiert werden konnten.

Wurde bei Frage 10 – wie in einem Fall – in dem Textfeld „Weitere“ „Keine“ eingetragen, allerdings ohne die Felder für die Prozentangaben auszufüllen, so wurde diese Angabe als 100% „Keine“ kodiert.

Im umgekehrten Fall, wenn bei Frage 10 zwar Prozentangaben gemacht wurden, auch vor dem Textfeld „Weitere“ eine Prozentzahl eingetragen wurde, ohne jedoch das Textfeld auszufüllen, wurde die Angabe als „Sonstiges“ kodiert.

### 7.3.4 Ergebnisse und Interpretation[275]

#### 7.3.4.1 Art und Größe der befragten Unternehmen

Die Anzahl der Mitarbeiter und Kunden in den befragten Unternehmen setzen sich wie folgt zusammen:

Tabelle 3: Anzahl der Mitarbeiter der befragten Unternehmen

| Klassen der Mitarbeiteranzahl | in % |
|---|---|
| 1 – 50 Mitarbeiter | 12,2 % |
| 51 – 200 Mitarbeiter | 12,2 % |
| 201 – 500 Mitarbeiter | 22,1 % |
| 501 – 1.000 Mitarbeiter | 19,3 % |
| mehr als 1.000 Mitarbeiter | 34,3 % |

Tabelle 4: Anzahl der Kunden der befragten Unternehmen

| Klassen der Kundenanzahl | in % |
|---|---|
| weniger als 10 Kunden | 2,3 % |
| zwischen 10 und 100 Kunden | 8,5 % |
| zwischen 100 und 1.000 Kunden | 17,5 % |
| zwischen 1.000 und 10.000 Kunden | 16,9 % |
| zwischen 10.000 und 100.000 Kunden | 23,7 % |
| mehr als 100.000 Kunden | 31,1 % |

Die befragten Unternehmen verteilten sich auf die folgenden Branchen:

Tabelle 5: Branchen der befragten Unternehmen

| Branchen | in % |
|---|---|
| Dienstleistung | 55,0 % |
| produzierendes Gewerbe | 17,2 % |
| verarbeitendes Gewerbe | 1,1 % |
| Verwaltung | 5,6 % |
| andere Branchen | 21,1 % |

[275] Die Auswertungen befinden sich im Anhang S. A51 ff.

Die befragten Unternehmen verteilten sich auf die folgenden Tätigkeitsbereiche:

Tabelle 6: Tätigkeitsbereiche der befragten Unternehmen

| Tätigkeitsbereiche | in % |
|---|---|
| Einzelhandel | 3,3 % |
| Finanzdienstleistungen | 13,9 % |
| Versicherungen | 7,2 % |
| Auskunfteien | 0,6 % |
| Telekommunikation | 3,9 % |
| Finanzdienstleistung und Versicherung | 1,1 % |
| Keine der Vorgenannten | 70,0 % |

#### 7.3.4.2 Wahrnehmung der Rechte – Auskunftsanspruch, Widerspruch und Löschung

Das Ergebnis der Befragung, wie häufig die befragten Unternehmen Anfragen mit datenschutzrechtlichem Hintergrund erhalten, ist recht eindeutig: Die Kunden der Unternehmen machen den Auskunftsanspruch, Widerspruch bzw. Löschungsanspruch äußerst selten geltend.

Von 189 gaben 50 Befragte an, dass sich bisher noch nie ein Kunde mit einer Auskunftsanfrage, mit einem Widerspruch[276], mit einem Löschungsbegehren bzw. mit einer sonstigen Anfrage/Beschwerde in Bezug auf die Verarbeitung von Kundendaten an das Unternehmen gewandt hat. Das sind mehr als ein Viertel der Befragten (26,45%). Bei insgesamt 170 Befragten sind bisher entweder nie Auskunftsanfragen, Widersprüche und Löschungsbegehren eingegangen oder derartige Anfragen werden von weniger als 1% der Kunden[277] im Jahr geltend gemacht. Bei fast 90% der Befragten ist also das Aufkommen von datenschutzrelevanten Anfragen entweder nicht vorhanden oder liegt zumindest so niedrig, dass weniger als 1% der Kunden im Jahr Ansprüche geltend machen.

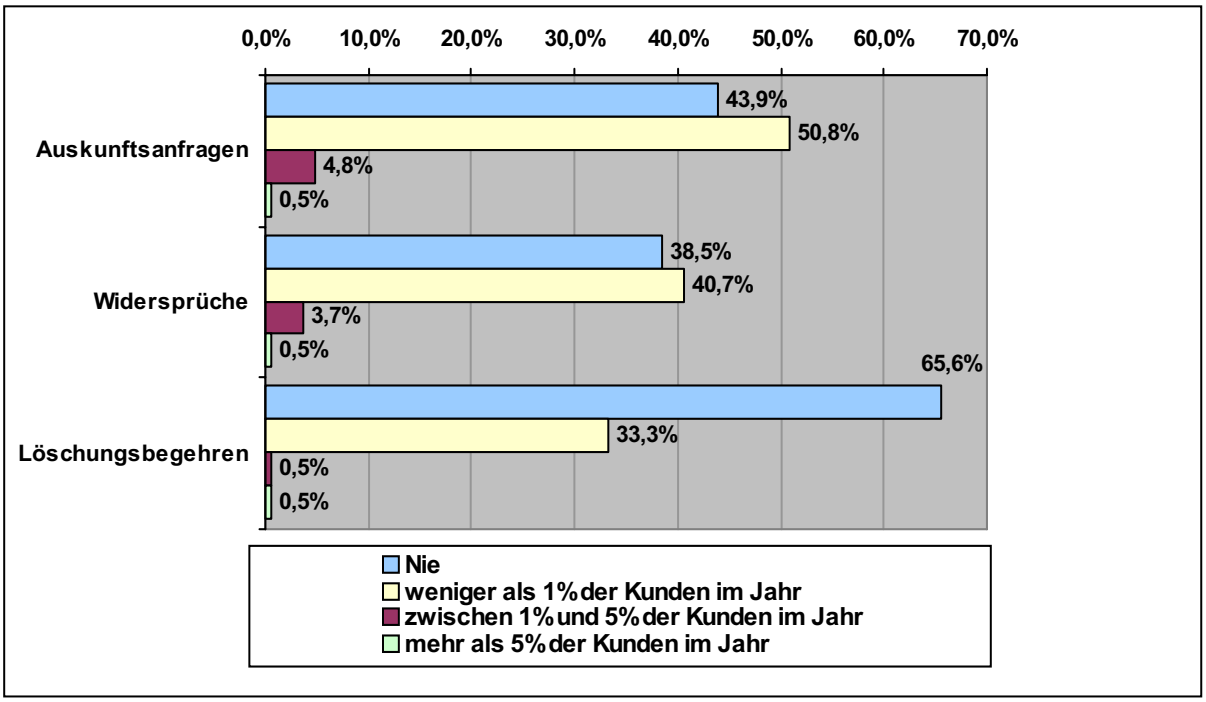
Auch wenn die drei abgefragten Arten der datenschutzrechtlichen Inanspruchnahme einzeln betrachtet werden, ergeben sich keine relevanten Abweichungen von diesem Ergebnis. An 43,9% der befragten Unternehmen wurden noch nie Anfragen auf Auskunft gerichtet und bei gut 50% fragen weniger als 1% der Kunden im Jahr an. Kumuliert ergibt dies einen Prozentanteil von fast 95% (94,7%). Bei 36,5% der Befragten ist noch nie ein Widerspruch eingegangen und bei 40,7% der Befragten widersprechen weniger als 1% der Kunden im Jahr, zusammengenommen ergibt das gut 77% der Befragten. Der Anspruch auf Löschung wird in

[276] Hier sind auch diejenigen Befragten erfasst, die angaben, dass die Frage des Widerspruchs für ihr Unternehmen irrelevant sei. Ein Widerspruch käme nicht in Frage, da entweder das Unternehmen keine Kundendaten zu Werbe- und Marktforschungszwecken nutzt oder diese Nutzung auf Grund einer expliziten Einwilligung erfolgt.

[277] Gemessen an der Zahl der Kunden des befragten Unternehmens.

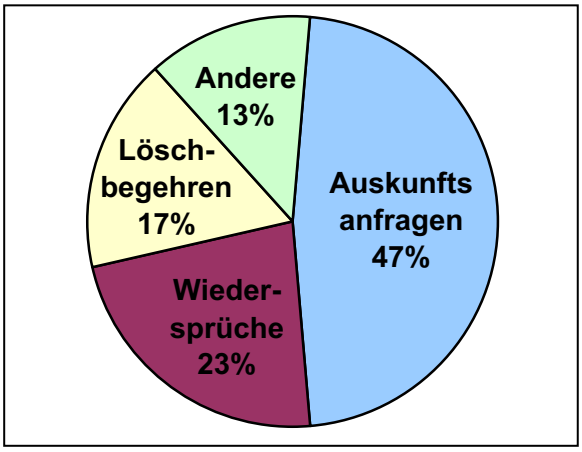
einem noch geringeren Maße geltend gemacht. Bei fast 99% der Befragten sind Löschungsanfragen entweder noch nie (65,6%) vorgekommen oder weniger als 1% der Kunden im Jahr beanspruchen die Löschung ihrer Daten (33,3%). Jeweils ein Befragter gab an, dass zwischen 1% und 5% bzw. mehr als 5% der Kunden im Jahr die Löschung begehren.

Abbildung 10: Häufigkeit der Auskunftsanfragen, Widersprüche und Löschungsbegehren




Es lässt sich erkennen, dass die Verbraucher – wenn überhaupt – häufiger die Geltendmachung eines Auskunftsanspruches in Betracht ziehen als Widersprüche einzulegen oder Löschung zu begehren. Von den Anfragen, die die Befragten erhielten, liegt der Anteil der Auskunftsansprüche bei gut 47%. Widersprüche nehmen einen Anteil von fast 23% ein, Löschungsbegehren werden bei 17% und „weitere“ Anfragen bei 13% der datenschutzrelevanten Anfragen geltend gemacht.

Abbildung 11: Aufteilung der Anfragen nach Auskunft, Widerspruch, Löschung und andere Anfragen



Für die einzelnen Tätigkeitsbereiche und Branchen der Unternehmen ergibt sich dabei folgendes Bild:

Bei den Dienstleistungsunternehmen erhalten 37,4% der Befragten nie Anfragen auf Auskunft. Bei 53,4% der Befragten fragen weniger als 1% der Kunden pro Jahr an und bei immerhin 9,1% der befragten Dienstleister fragen 1% der Kunden oder mehr an.

Die Mehrzahl, 64,5%, der Befragten aus der Branche des produzierenden Gewerbes erhalten nie Anfragen auf Auskunft. Bei 35,5% des produzierenden Gewerbes fragen weniger als 1% der Kunden im Jahr an. Für die Häufigkeit der Widersprüche ergibt sich ein ähnliches Bild. Bei der Mehrzahl der Dienstleister legen die Kunden – wenn auch weniger als 1% im Jahr – einen Widerspruch ein. Die meisten produzierenden Gewerbe (51,6%) erhalten nie einen Widerspruch ihrer Kunden. Für die Frage nach der Häufigkeit der Löschungsbegehren stellt sich eine Veränderung im Dienstleistungsbereich heraus, denn in diesem Zusammenhang geben auch die Dienstleister in der Mehrzahl an, dass sie nie Anfragen erhalten (58,6%).

Bei den Tätigkeitsbereichen erhalten etwa die Hälfte aller Finanzdienstleister gar keine Anfragen auf Auskunft und bei der anderen Hälfte fragen weniger als 1% der Kunden an. Genauso verhält es sich für die Geltendmachung von Widersprüchen. Bei den Löschungsbegehren gaben die Mehrzahl der Finanzdienstleister an, nie Anfragen zu erhalten.

Bei den Versicherungen hingegen, war der Anteil derjenigen, bei denen weniger als 1% der Kunden pro Jahr Auskunft anfragen, Widerspruch einlegen oder Löschung begehren immer größer als der Anteil der befragten Versicherungen, die nie Anfragen dieser Art erhalten.

Auf die Frage, welche „weiteren“ Begehren neben Auskunft, Widerspruch und Löschung von den Verbrauchern gestellt werden, spielt vor allen Dingen die „Übermittlung von Daten an Dritte“ eine große Rolle. 42 der befragten Stellen gaben an, dass sich andere Anfragen/Beschwerden der Verbraucher auf die Weitergabe von Daten bezögen. In jeweils neun Fällen werden von den Befragten Nachfragen bzw. Beschwerden zu den Themen „Speicherung und Fristen“ sowie „Herkunft und Erhebung der Daten“ genannt. Ein spezieller Fall der Datenübermittlung, die Weitermeldung an die Schufa, d.h. Übermittlung zur Bonitätsauswertung, wird 7-mal von den Befragten angegeben.

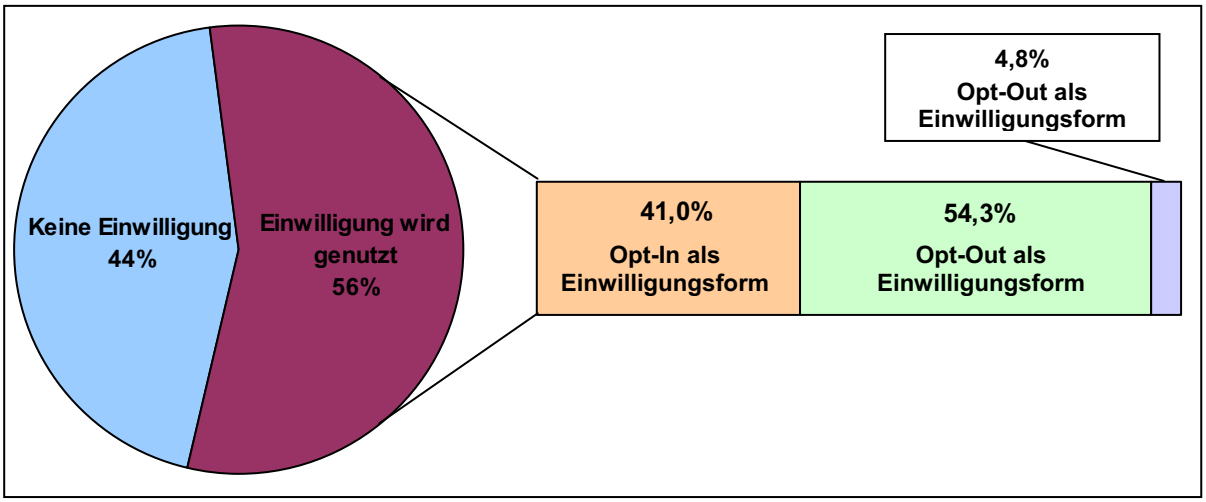
Bei der Frage nach dem datenschutzrechtlichen Kenntnisstand ihrer Kunden beurteilen die Befragten in der Mehrzahl den Informationsgrad als befriedigend bis gut. Die meisten der Befragten (36,6%) schätzen den Informationsstand der Kunden in Bezug auf ihre Datenschutzrechte als befriedigend ein. Fast 35% gehen davon aus, dass ihre Kunden gut oder sehr gut informiert sind. Eine deutlich kleinere Gruppe (22,3%) hat den Eindruck, dass die Kunden wenig oder gar nicht informiert sind.

#### 7.3.4.3 Einwilligung als Verarbeitungsgrundlage – Gestaltung, Verweigerung, Widerruf

Im Fragebogen wurde abgefragt, wie die datenschutzrechtliche Einwilligung des Kunden ausgewiesen, d.h. rechtstechnisch gestaltet, wird und ist. Zur Antwort wurden die ausdrückliche Einwilligung (Opt-In) bzw. eine Widerspruchslösung (Opt-out) Lösung angeboten.

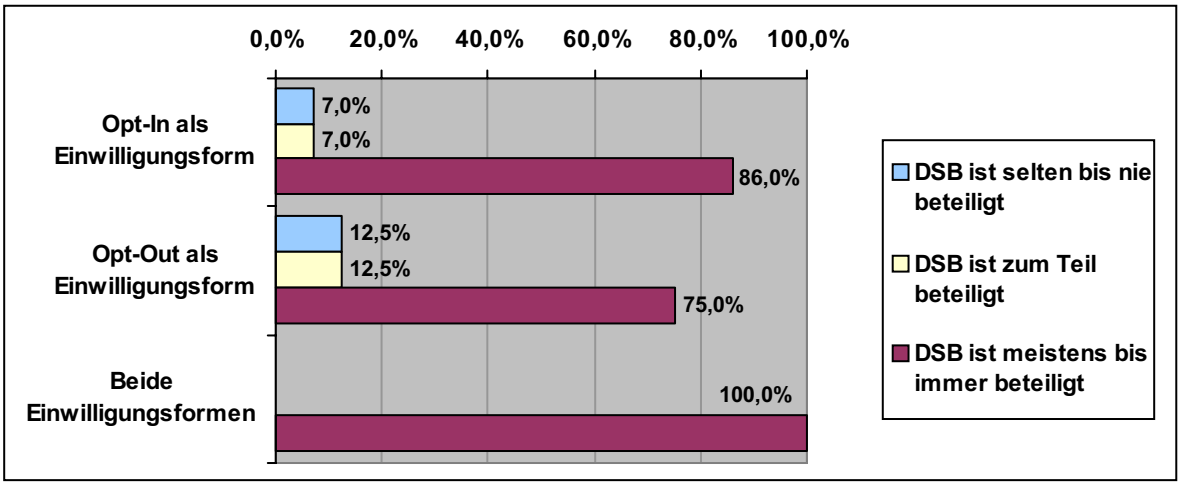
In 105 von 189 Fällen, d.h. in fast 56% der Fälle, erheben, verarbeiten und nutzen die Befragten Kundendaten auf der Grundlage einer Einwilligung. Davon gestalten gut 54% die Einwilligungserklärung als Opt-Out Lösung, d.h. die Datenverarbeitung gilt über den Vertragsabschluss als konsentiert, aber der Kunde hat die Möglichkeit der Verarbeitung zu widersprechen, indem er beispielsweise eine vorformulierte Einwilligungserklärung durchstreichen muss oder den Widerspruch durch setzen eines Kreuzes zu einem entsprechenden Text erklärt. Bei 41% der Befragten, die eine Einwilligung als Legitimationsgrundlage verwenden, ist die Erklärung als Opt-In ausgestaltet, d.h. die Einwilligung muss gesondert und ausdrücklich erteilt werden. Fast 5% der befragten Einwilligungsnutzer verwenden sowohl Opt-In als auch Opt-Out Lösungen.

Abbildung 12: Häufigkeit der Nutzung der Einwilligung und Häufigkeit der Gestaltung als Opt-In bzw. Opt-Out Einwilligung




Für die Gestaltung der Einwilligungserklärung macht es kaum einen Unterschied, in welchem Maße die oder der Datenschutzbeauftragte an der Gestaltung von Einwilligungserklärungen, Allgemeinen Geschäftsbedingungen oder Datenschutzhinweisen im Unternehmen beteiligt wird. 86% der Befragten, die eine Opt-In Einwilligungserklärung nutzen, gaben an, dass die/der Datenschutzbeauftragte meistens oder immer beteiligt ist. Dreiviertel der Befragten, die eine Opt-Out Lösung verwenden, beteiligen die/den Datenschutzbeauftragte/n nach eigenen Angaben ebenfalls meistens bis immer. Innerhalb der Gruppe der Befragten, die/den Datenschutzbeauftragte/n immer oder meistens beteiligen, verwendet die Hälfte der einwilligungsnutzenden Unternehmen eine Opt-Out Erklärung. Der Anteil der Opt-In Nutzer liegt hier bei 44%.

Abbildung 13: Verteilung der Beteiligungsgrade der betrieblichen Datenschutzbeauftragten unterschieden nach Ausgestaltung der Einwilligung




Bezogen auf die einzelnen Branchen ergibt sich folgendes Bild: Fast 68% der Dienstleister nutzen eine Einwilligung als Grundlage zur Verarbeitung von Kundendaten. Von diesen verwenden 61,2% ein Opt-Out und 35,8% ein Opt-In. Beim produzierenden Gewerbe liegt der Anteil derjenigen, die eine Einwilligungserklärung zur Verarbeitung einholen, bei 29%, d.h. in 9 von 21 Fällen. Fünf dieser neun Einwilligungsnutzer verwenden ein Opt-In und vier ein Opt-Out. Bei den Befragten, die eine Einwilligung nutzen, ist die Dienstleistungsbranche mit über 64% am häufigsten vertreten. 21% von den Befragten, die sich einer Einwilligung bedienen, kommen aus anderen nicht näher spezifizierten Branchen und 8,7% aus dem produzierenden Gewerbe. Im Zusammenhang mit den einzelnen Tätigkeitsbereichen ist insbesondere der Finanzdienstleistungsbereich als besonders verbraucherrelevant für die Auswertung interessant. 76% der Finanzdienstleister verarbeiten Verbraucherdaten auf der Grundlage einer Einwilligung. Von diesen gestalten fast 74% die Einwilligungserklärung als Opt-Out. In vier von 19 Fällen (21,1%) nutzen die Unternehmen eine Opt-In Lösung und in einem Fall werden beide Varianten verwendet.

Nach den Ergebnissen der Befragung gibt es kaum Verbraucher, die eine Einwilligung verweigern oder im Nachhinein widerrufen. Bei 92% der Befragten verweigern weniger als 5% der Kunden die Erklärung. Noch weniger Verbraucher machen von der Möglichkeit des Widerrufs einer einmal erteilten Einwilligung Gebrauch. Bei fast allen befragten Einwilligungsnutzern (96%) widerrufen weniger als 1% der Kunden ihre einmal erteilte Einwilligungserklärung.

Tabelle 7: Anzahl derjenigen, die eine Einwilligung verweigern

| Anzahl der Kunden im Jahr, die die Einwilligung verweigern | in % |
|---|---|
| weniger als 5% | 92,2 % |
| zwischen 5% und 9% | 4,9 % |
| zwischen 10% und 24% | 2,9 % |

Tabelle 8: Anzahl derjenigen, die eine Einwilligung widerrufen

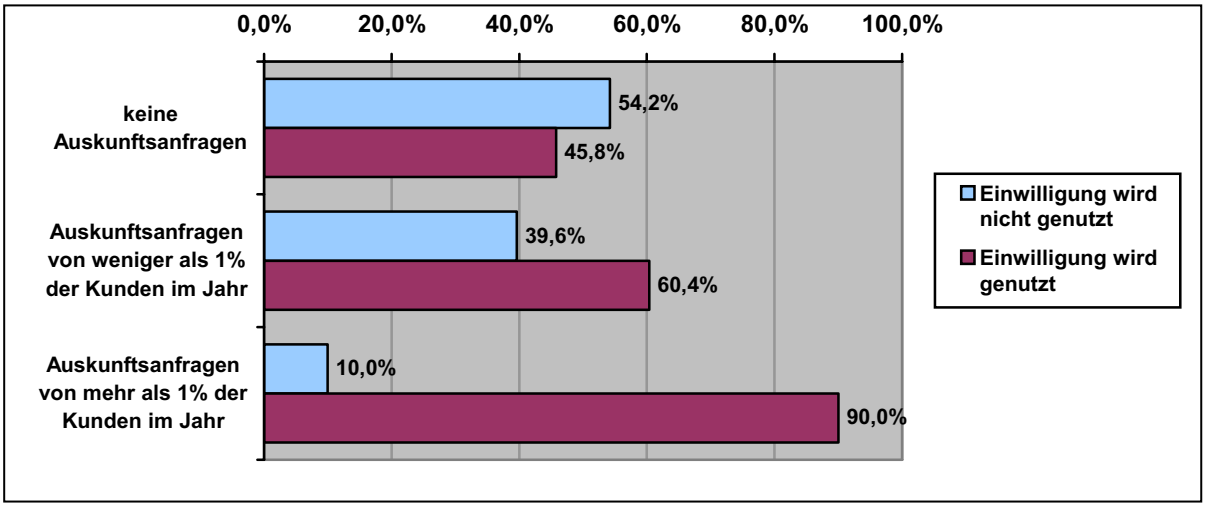
| Anzahl der Kunden im Jahr, die eine Einwilligung widerrufen | in % |
|---|---|
| weniger als 1% | 96,2 % |
| zwischen 1% und 4 | 1,9 % |
| zwischen 5% und 10% | 1,9 % |

Die Gestaltung der Einwilligung als Opt-In oder Opt-Out hat keinen nennenswerten Einfluss auf den Anteil der Verbraucher, die eine Einwilligung verweigern bzw. widerrufen. Die Unterschiede sind hier tendenziell gering: Von den Befragten, deren Kunden in weniger als 5% der Fälle eine Einwilligung verweigern, nutzen gut 40% eine Opt-In Lösung und 54% ein Opt-Out. Für die Befragten, die die Einwilligung als Opt-In gestalten, liegt die Verweigerungsrate in fast 98% der Fälle unter 5%. Ähnliches ergibt sich innerhalb der Opt-Out Nutzer. Bei über 91% derjenigen, die die Einwilligung als Opt-Out ausgestalten, verweigern weniger als 5% der Kunden die Einwilligung.

Ein fast identisches Ergebnis wurde bei der Frage nach der Auswirkung der Gestaltung der Einwilligungserklärung auf den Anteil derjenigen ermittelt, die eine Einwilligung im Nachhinein widerrufen. Innerhalb der Gruppe der Befragten, bei denen weniger als 1% der Kunden die Einwilligung widerrufen, nutzen 54% eine Opt-Out Gestaltung und 41% ein Opt-In. Von den Teilnehmern, die ihre Einwilligungserklärung als Opt-In gestalten, liegt die Widerrufsrate in fast 98% der Fälle unterhalb von 1%. Bei den Opt-Out Nutzern trifft dies in fast 95% der Fälle zu.

Die Ergebnisse zeigen, dass die Gestaltung der Einwilligung als Opt-In oder Opt-Out kaum Einfluss auf die Höhe der Verweigerungsrate hat. Es wird allerdings deutlich, dass die Nutzung einer Einwilligung als solcher - als Opt-In oder Opt-Out – tendenziell geeignet ist, den Verbraucher für seine Datenschutzbelange zu sensibilisieren und „aufzurütteln“. Ein Zusammenhang zwischen der Nutzung einer Einwilligung als Verarbeitungsgrundlage durch die Daten verarbeitende Stelle und der Häufigkeit der Auskunftsanfragen der Betroffenen kann hergestellt werden. Aus dem Kreise der Befragten, die nie Auskunftsanfragen erhalten, nutzen 45,8% eine Einwilligung und 54,2% nutzen keine. Bei denjenigen, die weniger als 1% der Anfragen pro Jahr erhalten, liegt der Anteil der Einwilligungsnutzer bei 60,4% und der Anteil derjenigen, die keine Einwilligung verwenden, bei 39,6%. Von den zehn Befragten, bei denen 1% und mehr Kunden pro Jahr Auskunftsbegehren geltend machen, bedienen sich neun (90%) Unternehmen einer Einwilligung zur Kundendatenverarbeitung und ein Unternehmen nutzt keine Einwilligung. Zwar ist die Anzahl der Fälle gerade in der letzten Gruppe sehr gering. Aus den Zahlen lässt sich aber zumindest eine steigende Tendenz ablesen und der Rückschluss, dass die Häufigkeit der Auskunftsanfragen und die Nutzung einer Einwilligung in einem gewissen Zusammenhang stehen könnten, ist möglich.

Abbildung 14: Zusammenhang zwischen der Einwilligungsnutzung und der Häufigkeit der Auskunftsanfragen

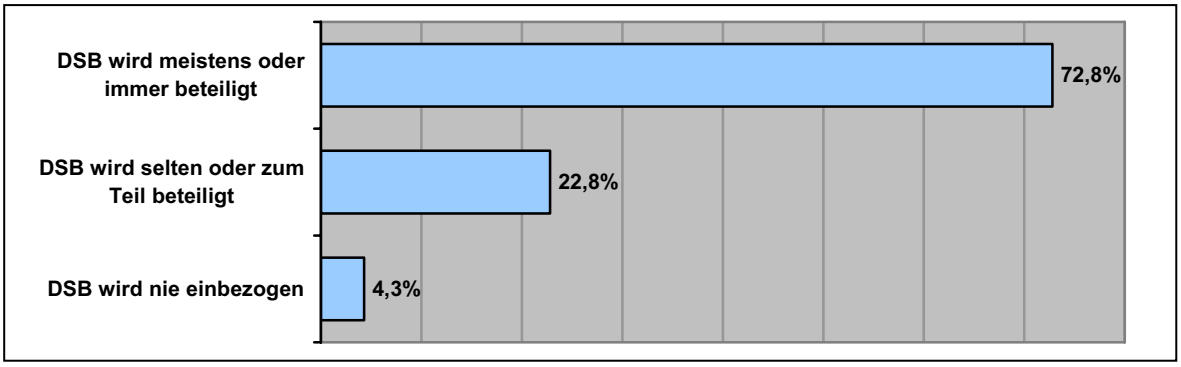



### 7.3.4.4 Bearbeitung von Datenschutzanfragen – Zuständigkeiten, Beteiligung des betrieblichen Datenschutzbeauftragten

Für die Bearbeitung von Auskunftsanfragen, Widersprüchen, Löschungsbegehren und den Widerrufen von Einwilligungen sind jeweils bei mindestens 53% der Befragten die betrieblichen Datenschutzbeauftragten zuständig. Als zweithäufigste Anlaufstelle wird von den Befragten mit 11% bis fast 20% der Kundenservice genannt. Auch eine Kombination aus betrieblichem Datenschutzbeauftragten und Kundendienst ist im Vergleich zu anderen Angaben relativ häufig die zuständige Stelle. Ansonsten ergibt sich ein sehr uneinheitliches Bild. Die angegebenen Stellen sind breit gefächert. Bei den Auskunftsersuchen und den Löschungsbegehren werden bis zu 23 verschiedene Stellen genannt, denen die Bearbeitung der jeweiligen Anfragen im Unternehmen zugewiesen ist.

An der Gestaltung von Einwilligungserklärungen, Allgemeinen Geschäftsbedingungen und Datenschutzhinweisen wird der betriebliche Datenschutzbeauftragte nach Auskunft der Befragten häufig beteiligt. 72,8% der Befragten geben an, dass der betriebliche Datenschutzbeauftragte entweder meistens oder immer beteiligt ist. 13% beteiligen den betrieblichen Datenschutzbeauftragten selten oder nie und 14% geben eine teilweise Beteiligung an.

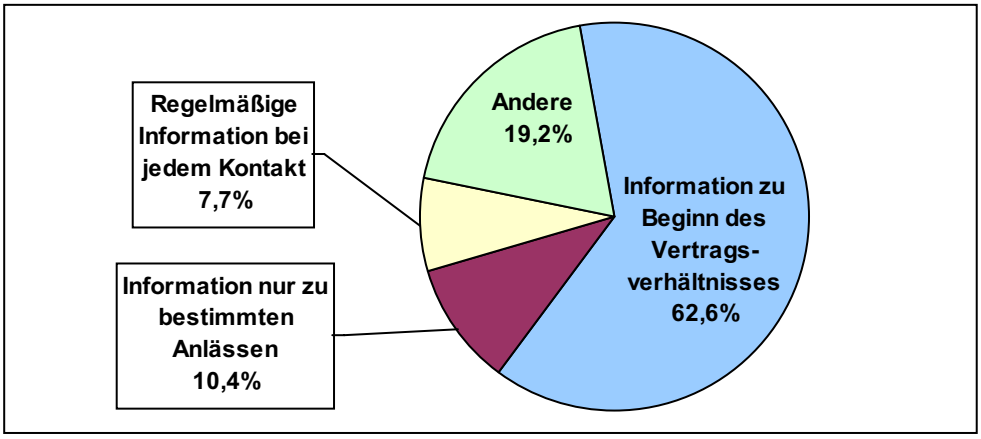
Abbildung 15: Beteiligung des betrieblichen Datenschutzbeauftragten



#### 7.3.4.5 Verbesserung des Verbraucherdatenschutzes

Fast 63% der Teilnehmer halten den Beginn des Vertragsverhältnisses für den wirkungsvollsten Zeitpunkt, um die Kunden über die Verarbeitung von Daten und Rechte zu informieren. Eine regelmäßige Information zu jedem Kundenkontakt schätzen 7,7% als sinnvoll ein.

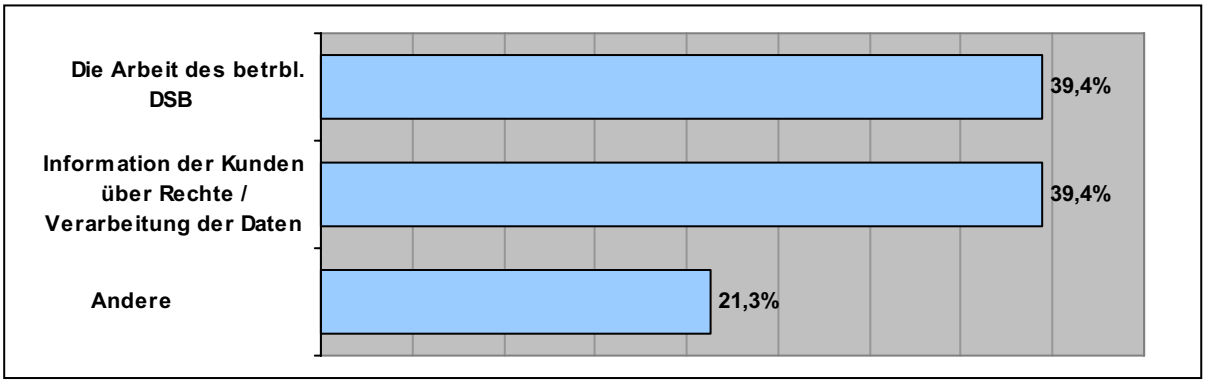
Abbildung 16: Wirkungsvollster Zeitpunkt zur Information der Kunden nach Einschätzung der Befragten




Bei der Frage, welcher Information im Rahmen eines guten Verbraucherdatenschutzes am meisten Bedeutung zukommt, schätzte die Mehrheit der Befragten die Information über die Übermittlung von Kundendaten am wichtigsten ein. Auf einer Skala von 1-5, wobei 1 mit „unwichtig“ und 5 mit „sehr wichtig“ gekennzeichnet war, wurde die Information über die Weitergabe mit durchschnittlich 4,40 bewertet. Auch die gesetzlichen Informationspflichten, wie die Unterrichtung über Zweckbestimmung der Erhebung, Verarbeitung und Nutzung von Kundendaten und die Identität der verantwortlichen Stelle wurden ebenfalls hoch eingeschätzt. Mit durchschnittlich 4,38 bzw. 4,33 gewichteten die Befragten diese Information als tendenziell wichtig. Die Information der Kunden über ihre Datenschutzrechte wie Auskunftsanspruch und Widerspruchsrecht werden von den Befragten mit durchschnittlich 4,18 und 4,30 ebenfalls als wichtig beurteilt. Die Informationen über die Existenz und Erreichbarkeit des betrieblichen Datenschutzbeauftragten und über die Aufbewahrungsdauer der gespeicherten Daten waren den Befragten weniger wichtig. Diese wurden im Durchschnitt mit 3,78 bzw. 3, 32 bewertet.

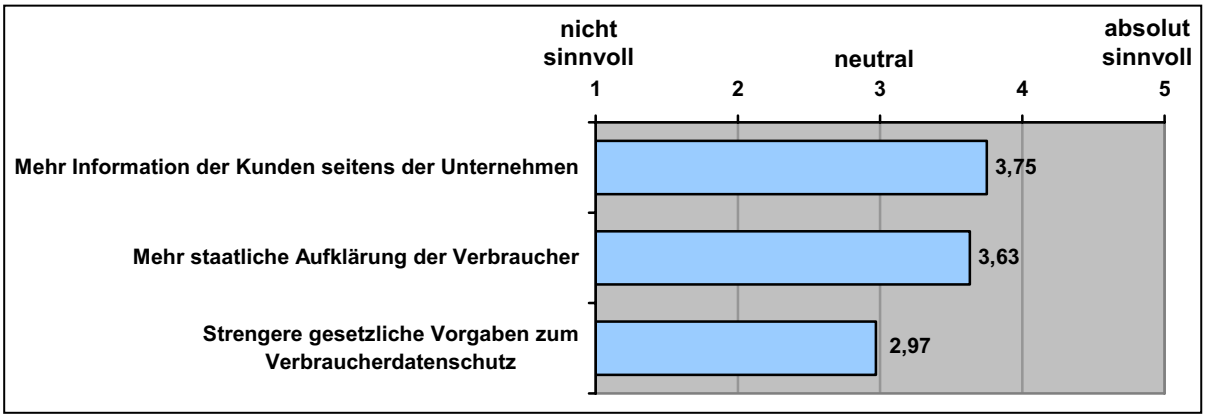
Jeweils fast 40% der Befragten halten die Arbeit des betrieblichen Datenschutzbeauftragten bzw. die Information der Kunden über ihre Rechte sowie zur Verarbeitung ihrer Daten als am besten geeignet, um die Situation des Verbraucherdatenschutzes zu verbessern. Drei der Befragten sahen in der Sensibilisierung und Schulung der Mitarbeiter sowie der Führungskräfte ein sinnvolles Instrument zur Verbesserung des Verbraucherdatenschutzes. Ein Erklärungsansatz für die relativ geringe Zahl ist, dass die Arbeit des betrieblichen Datenschutzbeauftragten und die Information der Kunden über ihre Rechte als Antworten vorgegeben waren und zudem die Befragten aus methodischen Gründen gebeten wurden, nur eine Antwort anzukreuzen. Die Befragten hielten diese Instrumente folglich als für noch geeigneter als die Schulung und Sensibilisierung der eigenen Mitarbeiter.

Abbildung 17: Am besten geeignete Instrumente zur Verbesserung der Situation des Verbraucherdatenschutzes nach Einschätzung der Befragten




Für die Frage nach der sinnvollsten Maßnahme zur Verbesserung des Verbraucherdatenschutzes gewichteten die betrieblichen Datenschutzbeauftragten die vorgegebenen Maßnahmen in folgender Reihenfolge: Auf einer Skala von 1-5, wobei 1 mit „nicht sinnvoll“ bzw. 5 mit „absolut sinnvoll“ gekennzeichnet wurde, bewerteten die Befragten eine erhöhte Information der Kunden seitens der Unternehmen mit durchschnittlich 3,75 und damit als sinnvollste Maßnahme. Die verstärkte staatliche Aufklärung der Verbraucher beurteilten die Befragten mit einer durchschnittlichen Bewertung von 3,63 als zweitwichtigste Maßnahme. Am wenigsten sinnvoll erschienen den betrieblichen Datenschutzbeauftragten mit einer durchschnittlichen Bewertung von 2,97 die strengeren gesetzlichen Vorgaben zum Verbraucherdatenschutz.

Abbildung 18: Bewertung von Maßnahmen zur Verbesserung des Verbraucherdatenschutzes auf einer Skala von 1-5




### 7.3.5 Zusammenfassung der Ergebnisse der Befragung der betrieblichen Datenschutzbeauftragten

Trotz der geringen Rücklaufquote mit 189 Fragebögen, d.h. 10,5%, lässt sich aufgrund der Eindeutigkeit des Ergebnisses die Aussage treffen, dass die Verbraucher ihre Datenschutzrechte gegenüber der Daten verarbeitenden Stelle in äußerst geringem Maße wahrnehmen. Von den wenigen datenschutzrelevanten Anfragen, die die Unternehmen erhalten, nehmen die Auskunftsbegehren im Gegensatz zu Widersprüchen oder Löschungsanfragen den größten Anteil ein. Erhalten die Unternehmen „weitere“ Anfragen mit datenschutzrechtlichem Hin-

tergrund, so handelt es sich dabei in der Hauptsache um Anfragen zur Übermittlung von Daten an Dritte.

Die Einwilligung wird bei über der Hälfte der Unternehmen als Grundlage für die Verarbeitung von Kundendaten genutzt. Es stellt sich in diesem Zusammenhang die Frage, ob allein die Verwendung einer Einwilligung als Rechtsgrundlage der Datenverarbeitung als positives Zeichen gewertet werden kann, denn für die datenschutzkonforme Verwendung der Daten kommt es auch immer auf die konkrete Ausgestaltung der Einwilligung an. Die Unternehmen könnten die Einwilligung als Legitimationsgrundlage ihrer Datenverarbeitung anbieten, um sich einen möglichst weiten Verarbeitungsspielraum zu eröffnen, der durch eine kundenunfreundliche Gestaltung der Erklärung dem betroffenen Verbraucher verborgen bleibt oder dessen Ausnutzung von ihm nicht zu kontrollieren ist.

Auf der anderen Seite markiert die Verwendung einer Einwilligung unter dem Gesichtspunkt der Transparenz für die Verbraucher eine positive Entwicklung. Dies lässt sich auch an dem Umstand ablesen, dass die Unternehmen, die Daten auf der Grundlage einer Einwilligung verwenden, mehr datenschutzrelevante Auskunftsanfragen erhalten als solche, die auf gesetzlicher Grundlage Daten verarbeiten. Die Einwilligungserklärung, so ist zu vermuten, rückt den Verbrauchern die Preisgabe ihrer Daten und deren Verwendung in einem erhöhten Maße ins Bewusstsein und Gedächtnis – mehr als ein einfacher Datenschutzhinweis bei der Erhebung personenbezogener Daten. In der Konsequenz stärkt die Einwilligung das Bedürfnis, den Schutz der persönlichen Daten durch die Ausübung der Datenschutzrechte abzusichern.

Die Gestaltung der Erklärung als Opt-In oder Opt-Out wirkt sich nach den Ergebnissen der Befragung nicht nachhaltig auf die Sensibilisierung der Verbraucher aus. Zumindest macht es keinen Unterschied für die Anzahl der verweigernden oder widerrufenden Kunden, ob die Einwilligung eine Opt-In Erklärung ist oder als Opt-Out genutzt wird. Eine Opt-In Gestaltung ist aus Transparenzgründen allerdings immer noch vorzuziehen.

Die meisten betrieblichen Datenschutzbeauftragten schätzen den Informationsstand der Kunden über die Datenschutzrechte zwar als befriedigend bis sehr gut ein, halten häufig allerdings die Information über die Datenschutzrechte sowie zur konkreten Verarbeitung der Daten weiterhin für eine besonders geeignete Maßnahme zur Verbesserung des Verbraucherdatenschutzes. Aufschlussreich ist in diesem Zusammenhang, dass die Befragten die Informationen zur Weitergabe von Daten an Dritte, zur Zweckbestimmung der Verarbeitung und zur Identität der verarbeitenden Stelle als besonders wichtig einschätzen. Jedenfalls bewerten sie diese Informationen sogar im Durchschnitt als noch bedeutsamer als die Information über Widerspruchs- und Auskunftsrecht. In diesen Zusammenhang passen auch die Angaben der Befragten zu den weiteren datenschutzrechtlichen Anfragen: Wenn überhaupt neben Auskunftsanspruch, Widerspruch oder Löschungsbegehren noch weitere Anfragen mit datenschutzrechtlichem Inhalt geltend gemacht werden, so handelt es sich dabei überwiegend um Anfragen zur Übermittlung von Daten. Das Informationsinteresse der Verbraucher deutet darauf hin, dass ihnen gerade solche Informationen zum Zeitpunkt der Erhebung ihrer Daten fehlen. Auch die Bewertung der Befragten deutet darauf hin, dass hier möglicherweise ein Informationsdefizit auf Seiten der Verbraucher besteht, so dass die Inkennt-

nissetzung der Verbraucher durch die verantwortlichen Daten verarbeitende Stelle über die Weitergabe von Daten besonders wichtig ist, um diese Lücke zu schließen.

Eine Erklärung für den hohen Bedeutungsgrad, den die Befragten der Information über die Weitergabe von Daten beimessen, könnte allerdings auch sein, dass es sich hierbei um eine gesetzliche Informationspflicht handelt, zumindest in der Form, dass nach § 4 Abs. 3 BDSG über Empfängerkategorien unterrichtet werden muss. Die gesetzlichen Unterrichtungspflichten nach § 4 Abs. 3 BDSG, wie Zweckbestimmung und Identität der verantwortlichen Stelle, schneiden allesamt auf der Wichtigkeitsskala der Befragten überdurchschnittlich hoch ab. Allerdings hatten die Befragten auch andere gesetzliche Informationspflichten zu bewerten, wie die Information über das Widerspruchsrecht, Information über die Freiwilligkeit der Einwilligung (Einwilligung verweigern zu können) oder die Widerrufsmöglichkeit, die sie als weniger wichtig einschätzten. Die Bewertung der Information über die Weitergabe von Daten an Dritte als wichtigste Information kann folglich nicht allein auf die Tatsache gestützt werden, dass es sich hier um eine gesetzliche Pflicht handelt.

Für datenschutzrechtliche Anfragen sind überwiegend die betrieblichen Datenschutzbeauftragten zuständig. Häufig besteht auch eine geteilte Zuständigkeit zwischen dem Datenschutzbeauftragten und dem Kundenservice oder zwischen diesem und der Marketingabteilung.

## 7.4 Befragung der Verbraucherberaterinnen und Verbraucherberater (vzbv-Befragung)

Die Befragung der Verbraucherberaterinnen und –berater erfolgte mit dem Ziel, Informationen über die Wahrnehmung der Datenschutzrechte durch die Verbraucher in Erfahrung zu bringen sowie als Basis für geeignete Vorschläge zur Verbesserung des Verbraucherdatenschutzes zu dienen. Die Verbraucherberatungen sind bei den Verbrauchern allgemein bekannt und einer der häufigsten Anlaufstellen, um sich über Rechte und Pflichten in verbrauchertypischen Situationen zu informieren oder Hilfe zu suchen. Es war davon auszugehen, dass die Beraterinnen und Berater auch in Fragen mit datenschutzrechtlicher Relevanz vielfach konsultiert werden.

Erkenntnisse aus der Beratungspraxis der Verbraucherschützer ergänzen daher die Informationen der betrieblichen Datenschutzbeauftragten zur Wahrnehmung der Rechte auf Seiten der Verbraucher. Die Beraterinnen und Berater können vermittels ihrer Erfahrung im Beratungsbereich zudem fundierte und kompetente Anregungen zur Verbesserung der Situation des Verbraucherdatenschutzes geben.

### 7.4.1 Durchführung

Die Durchführung der Befragung der Verbraucherberaterinnen und –berater erfolgte mit Hilfe eines Fragebogens. Bei der Konzipierung des Fragebogens stand die Verbraucherzentrale

Bundesverband e.V. (vzbv)[278] dem ULD beratend zur Seite und auch bei der Ausführung der Befragung wurde das ULD intensiv durch den vzbv unterstützt.

Die Fragebögen wurden über die Verbraucherzentralen der Landesverbände verteilt. Letztere vermittelten die Fragebögen weiter an ihre örtlichen Beratungsstellen. Der Vorstand der Verbraucherzentrale Bundesverband e.V. empfahl die Teilnahme an der Befragung in einem Begleitschreiben an die Landesverbände. Es wurden insgesamt 710 Fragebögen an die einzelnen Landesstellen versendet. Die Aufteilung erfolgte anhand der Anzahl von örtlichen Beratungsstellen in den 16 Bundesländern und der Anfrage über die Landesstellen, wie viel Mitarbeiter in den jeweiligen Beratungsstellen durchschnittlich tätig sind.

Der Einsendeschluss für die bearbeiteten Fragebögen wurde auf den 15. Juli 2005 festgelegt. Der Rücklauf beträgt 170 ausgefüllte Fragebögen, d.h. eine Rücklaufquote von 24% wurde erzielt. Dieser Rücklauf ist positiv zu bewerten, weil die Verbraucherberaterinnen und –berater nach fachlichen Schwerpunkten tätig sind, also bei weitem nicht alle Verbraucherberaterinnen und –berater Themenfelder beraten, die datenschutzrelevant sind.

### 7.4.2 Fragebogen

Der Fragebogen[279] zur Befragung der Verbraucherberaterinnen und –berater umfasst acht Fragen und ist in drei Teile untergliedert.

Im ersten Teil (Fragen 1-6) werden die Beraterinnen und Berater zu ihren Erfahrungen mit datenschutzrechtlichen Anfragen in der Beratungspraxis befragt. Ermittelt wird, in welchem Maße Anfragen mit datenschutzrechtlichem Hintergrund in der Beratungspraxis eine Rolle spielen (Frage 1) und ob sich die Anzahl derartiger Anfragen in den letzten Jahren verändert hat (Frage 2). Stellen die Beraterinnen und Berater eine Veränderung fest, sollen sie die Gründe dafür aus ihrer Sicht darstellen (Frage 3). Es wird zudem erfragt, in welchen Bereichen sich die Anzahl der Anfragen verändert hat (Frage 4). Bei der Frage 5 geht es um die Themengebiete, auf die sich Fragen mit datenschutzrechtlichem Hintergrund am häufigsten beziehen. Dabei sind sieben Antworten vorgegeben, die Teilnehmerinnen und Teilnehmer haben zudem die Möglichkeit der freien Antwort. Bei den vorgegebenen Antworten handelt es sich um die Bereiche „Auskunfteien“; „Versicherungen“, „Banken“, „Einzelhandel“, „Techniken zur Markierung von Waren (z.B. RFID)“, „Telekommunikation (incl. Mobilfunk)“, „Internetdienste (z.B. ebay, amazon) und Internetprovider“. Mehrfachnennungen waren hier erlaubt. Im Rahmen der Frage 6 sollen die Teilnehmerinnen und Teilnehmer schätzen, wie viele der Verbraucher vor der Anfrage bereits eigene Schritte zur Lösung ihres Problems unternommen, d.h. Datenschutzrechte gegenüber dem Unternehmen geltend gemacht haben.

In einem weiteren Teil des Fragebogens werden die Beraterinnen und Berater nach ihrer Einschätzung befragt, warum die Verbraucher die Datenschutzrechte in relativ geringem

[278] Verbraucherzentrale Bundesverband e.V., Markgrafenstraße 66, 10969 Berlin.

[279] Der Fragebogen befindet sich im Anhang S. A86 ff.

Maße wahrnehmen (Frage 7). Die Befragten konnten hier zwischen vier Antworten auswählen oder eine eigene Antwort eintragen. Die vorgegebenen Antworten lauten:

- „Dem Verbraucher ist nicht bewusst, dass sein Problem einen datenschutzrechtlichen Bezug hat."
- „Der Verbraucher ist über seine Rechte (z.B. Auskunft, Widerspruch oder Löschung) nicht informiert."
- „Dem Verbraucher ist die Ursache seines Problems (Verarbeitung seiner Daten) bewusst, er ist auch über die entsprechenden Rechte unterrichtet, verspricht sich von deren Wahrnehmung aber keinen Erfolg."
- „Der Verbraucher ist mit der Lösung seines Problems überfordert."

Mit der letzten Frage (Frage 8) wird den Teilnehmerinnen und Teilnehmern die Gelegenheit gegeben, Maßnahmen zur Verbesserung der Situation des Verbraucherdatenschutzes vorzuschlagen.

### 7.4.3 Methoden und Auswertung

#### 7.4.3.1 Keine Angabe

Nichtbeantwortete Fragen wurden als „keine Angabe" gewertet. Bedeutung erlangt diese Bewertung bei der Berechnung der Prozentanteile. Die im Rahmen des Gutachtens genannten Prozentangaben beziehen sich immer auf die „valid percentage", d.h. die Antwort „keine Angabe" wird bei der Anzahl der Fälle, von der für die Berechnung des Prozentanteils ausgegangen wird, nicht mitberücksichtigt.

#### 7.4.3.2 Prozentangaben

Bei den Prozentangaben in Fragen 1 und 6 wurden zum Teil „von-bis-Angaben" gemacht. In diesen Fällen wurde jeweils der höchste Wert erfasst. Die Prozentangaben wurden mit einer Stelle hinter dem Komma kodiert.

#### 7.4.3.3 Offene Fragen

Der Fragebogen enthält fünf Möglichkeiten zur freien Antwort. Inhaltlich gleichartige Antworten auf diese offenen Fragen wurden jeweils in Gruppen zusammengefasst, die Gruppen mit Schlagwörtern der Antworten benannt und als eigene Antwortkategorie kodiert. Unter „Sonstiges" wurden die Antworten gesammelt, die zu selten genannt wurden, um eine eigene Gruppe zu eröffnen und sich zu sehr von anderen Antworten unterschieden, um in eine andere Gruppe eingeteilt werden zu können.

Bei Frage 3 wurden insgesamt zehn verschiedene Gruppen gebildet, wobei eine dieser Gruppen als „Sonstiges“ kodiert wurde. Bei Frage 4 ergaben sich zwölf Gruppen, inklusive einer als „Sonstiges“ gekennzeichneten Gruppe.

Für Frage 5 kam neben den vorgegebenen Antworten in dem Textfeld „Andere“ auch eine freie Angabe in Betracht. Hier wurden zwei Gruppen gebildet. Eine dieser Gruppen wurde als „Sonstiges“ kodiert. Ähnlich wurde bei Frage 7 vorgegangen. Auch hier bestand neben den vier vorgegebenen Antworten die Möglichkeit „Andere Gründe“ anzugeben. Es wurde die Gruppe „Sonstiges“ gebildet. Unter „Sonstiges“ wurden sowohl zwei freie Angaben als auch Mehrfachnennungen der vorgegebenen Antworten zusammengefasst. Mehrfachnennungen waren durch den Zusatz in der Frage „Bitte nur eine Antwort ankreuzen“ vorliegend nicht zugelassen, so dass diese auch nicht in den vorgegebenen Antwortkategorien gewertet werden können.

Bei Frage 9 wurden insgesamt 10 Gruppen gebildet. Auch hier ist eine Gruppe als „Sonstiges“ kodiert.

#### 7.4.3.4 Mehrfachnennungen

Bei Frage 5 waren Mehrfachnennungen durch den Zusatz „Bitte maximal 3 Antworten ankreuzen“ ausdrücklich zugelassen, so dass Mehrfachnennungen hier in den jeweiligen Antwortkategorien gewertet wurden.

Bei Frage 7 war – wie bereits beschrieben – nur eine Antwort vorgesehen. Mehrfachnennungen wurden als eine Antwort im Rahmen der Gruppe „Sonstiges“ gewertet. Eine mehrmalige Wertung in den jeweiligen Antwortkategorien hätte unberücksichtigt gelassen, dass diejenigen Befragten, die nach den Anweisungen nur eine Antwort gaben, möglicherweise mehrere Nennungen gemacht hätten. Zudem stellt Frage 7 einen Schwerpunkt der Befragung der Beraterinnen und Berater dar. Es ging darum, den Hauptgrund für die geringe Wahrnehmung der Rechte zu isolieren, so dass Mehrfachnennungen hier aus methodischen Gründen nicht gewertet werden konnten.

### 7.4.4 Ergebnisse und Interpretation[280]

#### 7.4.4.1 Datenschutzrechtliche Anfragen in der Beratungspraxis

Im Rahmen der Beratungspraxis der Verbraucherberaterinnen und –berater spielen datenschutzrechtliche Anfragen tendenziell eine untergeordnete Rolle. Im Durchschnitt beinhalten 11% der Anfragen Datenschutz-Themen. Dabei gaben 123 der Befragten (fast 77%) an, dass bei 0% bis 10% der Anfragen der Datenschutz eine relevante Rolle spielt. 27 der Befragten ordneten die Anzahl der Anfragen mit datenschutzrechtlicher Relevanz bei 10,1% bis

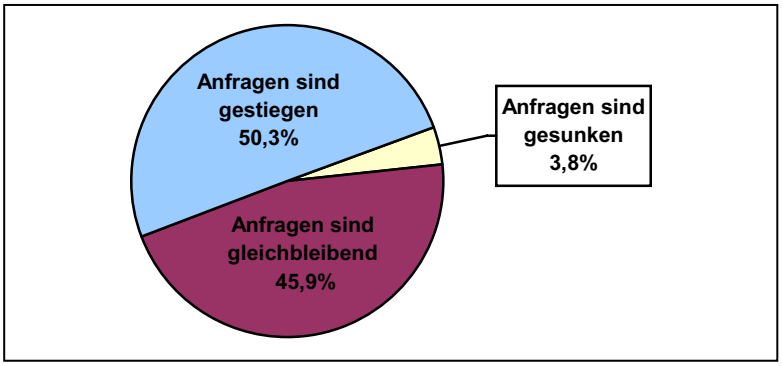
[280] Die Auswertungen befinden sich im Anhang S. A90 ff.

30%, fünf Befragten nannten Prozentangaben im Bereich von 30,1% bis 60% und weitere fünf Befragte gingen von 70% und mehr aus.

Die Anfragen mit Datenschutzrelevanz beziehen sich dabei am häufigsten auf die Themenbereiche Auskunfteien, Telekommunikation und Einzelhandel. 101 der Befragten, d.h. fast 60%, gaben zum Teil neben anderen Themengebieten den Bereich Auskunfteien an. Die Themen Telekommunikation und Einzelhandel wurden insgesamt von 80 bzw. 51 der Befragten genannt. Auf den Bereich der Versicherungen beziehen sich die Anfragen bei 20% der Befragten. Techniken zur Markierung von Waren (wie z.B. RFID) wurden insgesamt sechsmal genannt. Im Rahmen der offenen Antwort gaben insgesamt 37 Befragte Themenbereiche an, die mit einer Adressweitergabe im Zusammenhang stehen. Dabei wurden die Stichworte Adresshandel, ungebetene Werbung und Gewinnspiele angeführt.

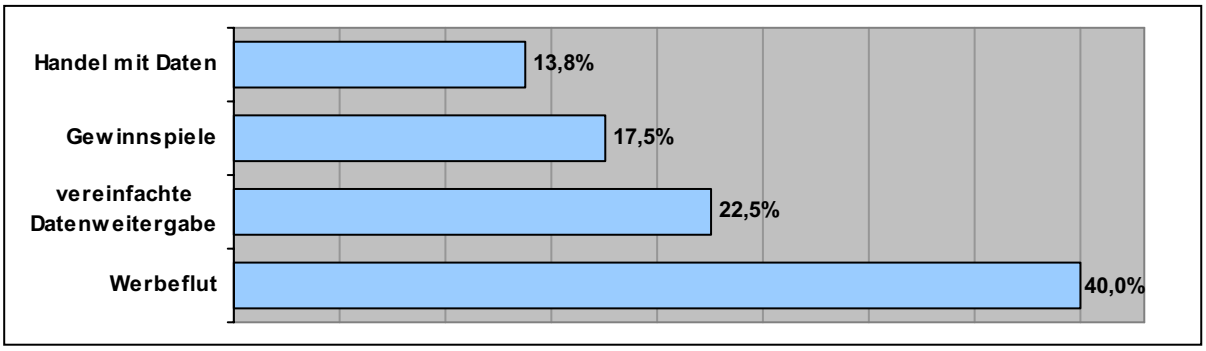
In den letzten Jahren ist die Zahl der Anfragen mit datenschutzrechtlichem Inhalt bei den Verbraucherberaterinnen und –beratern eher gestiegen. Insgesamt 80 (über 50%) der Befragten gaben an, dass die Anzahl derartiger Anfragen gestiegen bzw. stark gestiegen ist. Fast 46% stellten keine Veränderung in der Häufigkeit datenschutzrelevanter Anfragen fest. Bei sechs der Befragten ist die Anzahl derartiger Anfragen in den letzten Jahren gesunken oder stark gesunken.

Abbildung 19: Veränderung der Anfragen mit datenschutzrelevantem Inhalt




Den Anstieg von Anfragen mit datenschutzrechtlichem Inhalt führen die meisten Befragten – neben anderen Gründen – auf die erhöhte Werbeflut, d.h. die spürbare Belästigung bzw. Verwunderung über die Fülle an ungebetener Werbung zurück. Insgesamt 32 Befragte, d.h. 40% der Befragten, die einen Anstieg feststellten, gaben als Begründung unter anderem Werbeflut, Belästigung/Verärgerung/Verwunderung durch/über ungebetene Werbung, massivere Werbung, verstopfte Briefkästen etc. an. 18 (22,5%) der Befragten verwiesen u.a. auf die erhöhte bzw. vereinfachte Datenweitergabe im Bereich neuer Medien/Internet als Grund für die erhöhte Anzahl von Datenschutzanfragen in den letzten Jahren. Die Zunahme des Adresshandels bzw. des Handels mit Daten im Allgemeinen wurde insgesamt elfmal, d.h. in ca. 14% der Fälle, als Begründung genannt. Auch andere Methoden der Adresssammlung und die Zunahme von Kundenbindungssystemen wurden von den Befragten als Gründe für den Zuwachs der datenschutzrelevanten Anfragen genannt. Die zunehmende Werbung durch Gewinnspiele bzw. –mitteilungen, sog. Verbraucherumfragen bzw. das Thema Kundenkarte wurde insgesamt von 14 Befragten (fast 18%) angegeben.

Abbildung 20: Gründe für den Anstieg der Anfragen von Verbrauchern nach Einschätzung der Befragten




Von den Befragten wird ein Zusammenhang zwischen der Sensibilität der Verbraucher und einer Veränderung der datenschutzrelevanten Anfragen in den letzten Jahren hergestellt. Wie sich das Problembewusstsein der Verbraucher verändert hat und welche Auswirkung dies auf die Anzahl der Datenschutzanfragen hat, wird von den Befragten allerdings nicht einheitlich gesehen. Sowohl eine erhöhte als auch eine nachlassende Sensibilität der Verbraucher werden als Gründe für eine Veränderung genannt. 25% der Befragten, die einen Anstieg der Datenschutzanfragen festgestellt haben, führen diesen darauf zurück, dass die Verbraucher kritischer bzw. sensibler geworden sind. Dabei wurde zum Teil darauf verwiesen, dass die Verbraucher durch Insolvenzen, Verschuldung, Auskunfteiabfragen z.B. bei Handyverträgen Datenschutzprobleme in stärkerem Maße wahrnehmen. Andererseits wurde die leichtfertige/kritiklose Weitergabe von Daten bzw. eine nachlassende Sensibilität der Verbraucher von sechs Befragten als Grund für eine Veränderung der Anzahl der Datenschutzanfragen identifiziert. Die Auswirkung dieser Tendenzen wurde unterschiedlich beurteilt. Vier Befragte gaben an, dass die nachlassende Sensibilität der Grund für eine Verringerung der Anfragen mit datenschutzrechtlicher Relevanz sei. Zwei Befragte erkannten in der nachlassenden Sensibilität den Grund für einen Anstieg derartiger Anfragen.

Nach den Angaben der Befragten vollzog sich die Veränderung der Anzahl der datenschutzrelevanten Anfragen hauptsächlich in den Bereichen Gewinnspiele, neue Medien und Telefonmarketing. Jeweils fast 15% der Befragten gaben an, dass ein Anstieg derartiger Anfragen u.a. im Zusammenhang mit Gewinnbenachrichtigungen, Gewinnspielen bzw. Preisausschreiben sowie im Bereich der neuen Medien bzw. Telekommunikation zu verzeichnen ist. Insgesamt 14% der Befragten beobachteten einen Zuwachs an Anfragen mit datenschutzrechtlichem Bezug im Bereich von (belästigender) Telefonwerbung, unerwünschten Faxen, „cold calling“ und Call-Center Aktivitäten. Eine Erhöhung derartiger Anfragen findet nach den Angaben von 17 Befragten, d.h. 10%, außerdem im Bereich der Kundenbindungssysteme statt.

Zum Themenfeld Finanzdienstleistung/Auskunfteien stellten fast 9% der Befragten eine Veränderung der Anzahl von Datenschutzanfragen fest. Dabei gab eine bzw. einer der Befragten an, dass sich die datenschutzrelevanten Anfragen in diesem Bereich verringert hätten.

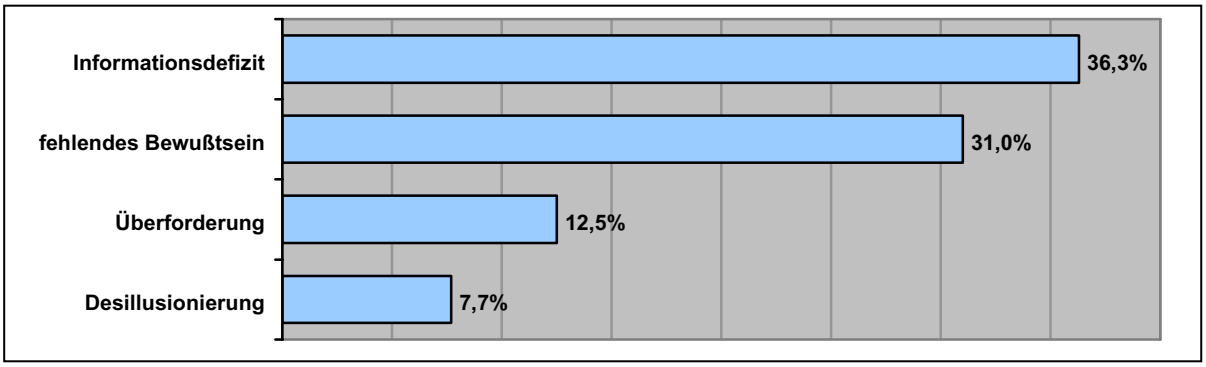
Der Bereich des Gesundheitswesens/ärztliche Schweigepflicht ist relativ selten von einem Anstieg der Anfragen mit datenschutzrechtlichem Hintergrund erfasst. Sechs Befragte stellten auf diesem Gebiet eine Veränderung fest.

#### 7.4.4.2 Wahrnehmung von Datenschutzrechten

Auch die Verbraucherberaterinnen und Verbraucherberater beobachten in ihrer Beratungspraxis eine tendenziell geringe Wahrnehmung von Datenschutzrechten gegenüber dem verantwortlichen Unternehmen. Die Befragten gaben an, dass nur durchschnittlich 10% der Verbraucher, die sich mit Fragen zum Datenschutz an die Beratungsstelle wenden, zuvor eigene Schritte zur Lösung ihres Problems unternommen haben. In mehr als 20% der Fälle haben die Verbraucher sich vor der Beratung gar nicht an das Unternehmen gewandt. In 22% der Fälle machen etwa 1%, in 15% der Fälle etwa 5% der anfragenden Verbraucher zuvor Datenschutzrechte geltend. Rund 12% der Befragten geben an, dass 10% der Verbraucher sich vor der Anfrage bei der Beratungsstelle an das Unternehmen gewandt haben. 7% gehen davon aus, dass die Hälfte der anfragenden Verbraucher vorher eigene Schritte zur Lösung ihres Problems unternehmen. Insgesamt führen fast 79% der Befragten an, dass höchstens 10% der Verbraucher vor der Beratung Datenschutzrechte gegenüber dem verantwortlichen Unternehmen wahrnehmen.

Die meisten Befragten sehen den Hauptgrund für eine geringe Wahrnehmung der Datenschutzrechte darin, dass die Verbraucher über ihre Rechte nicht informiert sind. 36,5% machen ein Informationsdefizit für die geringe Wahrnehmung primär verantwortlich. Fast ebensoviel, 31% der Befragten gehen davon aus, dass den Verbrauchern nicht bewusst ist, dass ihr Problem einen datenschutzrechtlichen Bezug hat. Für fast 13% der Befragten sind die Verbraucher mit der Lösung ihrer Probleme überfordert. Eine Desillusionierung der Verbraucher halten die Verbraucherberaterinnen und –berater hingegen tendenziell weniger für die Hauptursache einer geringen Wahrnehmung der Rechte. Nur knapp 8% der Befragten gaben an, dass die Verbraucher sich zwar der Ursache ihrer Probleme bewusst und auch über die entsprechenden Rechte informiert sind, sich aber von der Wahrnehmung keinen Erfolg versprechen.

Abbildung 21: Gründe für die geringe Wahrnehmung der Datenschutzrechte nach Einschätzung der Befragten



#### 7.4.4.3 Maßnahmen zur Verbesserung des Verbraucherdatenschutzes

Die Verbraucherberaterinnen und –berater schlugen mit Abstand am Häufigsten eine bessere bzw. stärkere Aufklärung und Information der Verbraucher zur Verbesserung des Verbraucherdatenschutzes vor. 106 der Befragten, d.h. 62%, gaben bei der Frage nach den Maßnahmen zur Verbesserung Aufklärung und Information an. Für fast 16% der Befragten stellten verstärkte bzw. strengere Kontrollen und Sanktionen Instrumente zur Verstärkung des Datenschutzes dar. In jeweils 12% der Fälle wurden Hinweis- und Belehrungspflichten bzw. strengere und bessere gesetzliche Regelungen als Verbesserungsvorschläge genannt. Jeweils zehn Verbraucherberaterinnen und –berater, knapp 6%, führten die Sensibilisierung der Verbraucher sowie das Verbot bzw. eine Einschränkung von Adresshandel und –verkauf als Maßnahme zur Verbesserung an. Das Erfordernis einer deutlichen und ausdrücklichen Einwilligung befürworteten fünf Befragte; für das Verbot einer Weitergabe von Daten ohne ausdrückliche Zustimmung plädieren insgesamt sieben der befragten Beraterinnen und Berater.

### 7.4.5 Zusammenfassung der Ergebnisse der Befragung der Verbraucherberaterinnen und -berater

Im Rahmen der Beratungspraxis der Verbraucherberaterinnen und –berater nehmen die Anfragen mit datenschutzrechtlichem Hintergrund einen geringen Anteil ein. Mehr als die Hälfte der Verbraucherberaterinnen und –berater geht allerdings davon aus, dass die datenschutzrelevanten Anfragen in den letzten Jahren zugenommen haben. Als Begründung für einen Anstieg wird insbesondere auf die spürbare Beeinträchtigung, die Verärgerung oder Verwunderung über eine erhöhte Werbeflut verwiesen. Außerdem wird die vermehrte und erleichterte Datenweitergabe im Zusammenhang mit Internet und neuen Medien als Begründung angegeben. Als Bereiche, auf die sich ein solcher Anstieg bezieht, werden vornehmlich die Bereiche Gewinnspiele, neue Medien und Telefonmarketing benannt.

Aus den Angaben der Verbraucherberaterinnen und –berater aus ihrer Beratungspraxis ist zu erkennen, dass auch die Verbraucher, die ein datenschutzrechtliches Problem haben, ihre Datenschutzrechte äußerst selten gegenüber dem Unternehmen geltend machen. Den Hauptgrund für eine derartig geringe Wahrnehmung der Rechte sehen die meisten Beraterinnen und Berater in der mangelnden Information der Befragten über ihre Rechte. Fast eben soviel Beraterinnen und Berater gehen allerdings davon aus, dass die Verbraucher noch nicht einmal erkennen, dass ihr Problem datenschutzrechtlicher Natur ist. Diese Annahme korrespondiert mit den Beobachtungen der Beraterinnen und Berater zum Anstieg der datenschutzrelevanten Anfragen in den letzten Jahren. Die Verbraucher erscheinen mit Problemen in den Beratungsstellen, die vordergründig mit dem Label „Werbeflut“ oder „Gewinnmitteilungen“ beschrieben werden. Dahinter verstecken sich datenschutzrelevante Vorgänge, wie z.B. die Übermittlung von Daten an Dritte oder die Sammlung von Adressen durch Adresshändler, die von den Verbrauchern als solche zunächst nicht erkannt werden.

In einer Frustration bzw. Desillusionierung der Verbraucher sehen die Verbraucherberaterinnen und –berater tendenziell selten den Grund, warum die Verbraucher ihre Datenschutzrechte in einem so geringen Maße geltend machen. Für die Verbraucherberaterinnen und –berater stellt insbesondere eine verstärkte Aufklärung und Information der Verbraucher eine geeignete Maßnahme zur Verbesserung des Verbraucherdatenschutzes dar. Zur Verbesserung werden außerdem häufig strengere Kontrollen und verstärkte Sanktionen sowie die Verstärkung von Informations- und Belehrungspflichten vorgeschlagen.

## 7.5 Befragung der Aufsichtsbehörden der Bundesländer für die Einhaltung des Datenschutzes im nichtöffentlichen Bereich

Auf Anregung einiger Vertreterinnen und Vertreter der Datenschutzaufsichtsbehörden aus anderen Bundesländern führte das ULD in Abstimmung mit dem Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft zusätzlich eine Befragung der einzelnen Aufsichtsbehörden der Bundesländer mit Hilfe eines Fragebogens durch.

### 7.5.1 Fragebogen

Der Fragebogen[281] enthält insgesamt 15 Fragen und lässt sich in drei Teile aufteilen. Die ersten drei Fragen befassen sich mit der Organisation der Datenschutzaufsichtsbehörde. Es wird nach der Einbindung in die Verwaltung, der Mitarbeiteranzahl und danach gefragt, ob die Datenschutzaufsichtsbehörde über eine Statistik der Eingänge verfügt.

Im zweiten Teil geht es um datenschutzrechtliche Anfragen. Dabei werden die Häufigkeit von Anfragen pro Woche, die Themengebiete zu denen angefragt wird, Veränderungen der Häufigkeit von Anfragen und die Veränderung der Anfragen zu gewissen Themenbereichen abgefragt.

Der Schwerpunkt der Befragung liegt im dritten und letzten Teil. Die Aufsichtsbehörden werden nach ihren Einschätzungen zu den Kenntnissen der Petenten über ihre Datenschutzrechte, den Kenntnissen der Verbraucher im allgemeinen über die in den einzelnen Branchen genutzten operativen Verarbeitungsprozesse, den Kenntnissen zu den in der Praxis anzutreffenden operativen Verwendungen sowie zu den Kenntnissen der Unternehmen über ihre Datenschutzpflichten befragt. Dabei mussten die Befragten die Kenntnisse auf einer Skala von 1-5 bewerten, wobei 1 als „sehr gut“ und 5 als „sehr schlecht“ gekennzeichnet war. Auch sollten die Befragten einschätzen, wie viele der anfragenden Verbraucher vor der Eingabe eigene Schritte zur Lösung ihres Problems unternommen haben. Die befragten Aufsichtsbehörden werden zudem aufgefordert, zu der These Stellung zu nehmen, dass die Verbraucher im Großen und Ganzen über die Auskunftspflichten der Unternehmen und ihren Auskunftsanspruch informiert sind, sie ihre Rechte aber nur zu einem verschwindend geringen Anteil wahrnehmen. Mit den letzten beiden Fragen erhielten die Befragten die Gelegen-

[281] Der Fragebogen befindet sich im Anhang S. A106 ff.

heit, Maßnahmen zur Verbesserung des Verbraucherdatenschutzes vorzuschlagen und sonstige Kommentare abzugeben.

### 7.5.2 Durchführung

Die Fragebögen wurden in der Sitzung des Düsseldorfer Kreises vom 10. bis 11.11.2005 an die vertretenen Aufsichtsbehörden mit der Bitte verteilt, diesen spätestens bis zum 23.11.2005 ausgefüllt zurückzusenden. Die Aufsichtsbehörden der Bundesländer, die an der Herbsttagung des Düsseldorfer Kreises nicht teilgenommen hatten, erhielten den Fragebogen in elektronischer Form.

Von den 16 ausgegebenen Fragebögen erhielt das ULD Rückantwort aus 11 Bundesländern. Ein Bundesland sendete drei ausgefüllte Fragebögen zurück. In diesem Fall sind die datenschutzrechtlichen Aufsichtsbehörden für den nichtöffentlichen Bereich auf mittelbehördlicher Ebene organisiert. Es gibt drei Regionen, für die jeweils drei unterschiedliche Aufsichtsbehörden bestehen.

### 7.5.3 Methoden der Auswertung

#### 7.5.3.1 Allgemeines

Diese vierte Befragung verfolgte das Ziel, durch die Befragung von Experten in der datenschutzrechtlichen Beratungspraxis die Erkenntnisse aus den bisherigen Befragungen abzugleichen und zu ergänzen. Die Erkenntnisse aus den vorhergehenden Befragungen flossen bei der Konzipierung der Fragen für die Aufsichtsbehörden mit ein, d.h. der Fragenbereich wurde speziell auf die Kernfrage zum Informationsstand der Verbraucher abgestimmt. Zudem wurde eine auf Grundlage der Vorbefragungen gebildete These durch eine gezielte Frage getestet.

Die Befragung erfolgte somit in Form standardisierter Experteninterviews, wobei die Daten in Teilbereichen aggregiert ausgewertet wurden und es bei anderen Fragen auf die einzelnen konkreten Antworten ankam.

Beim ersten Teil der Befragung zur Einbindung der Aufsichtsbehörde in die Verwaltung wurden die Antworten – bis auf die Frage nach der Statistik – qualitativ ausgewertet.

Für den zweiten Teil der Befragung wurden die Befragten, die eine Statistik nutzen und solche, die keine führen, sowohl zusammen als auch getrennt von einander in aggregierter Form ausgewertet. Die Frage nach der Häufigkeit der Anfragen spielt für die Ermittlung des Informationsstandes der Verbraucher keine große Rolle und blieb damit unberücksichtigt. Dies wäre die einzige Frage gewesen, deren Auswertung eine Beachtung der Einwohnerzahlen der einzelnen Bundesländer bedurft hätte. Die anderen Fragen zu Themenbereichen der Anfragen und Veränderung der Zahl der Anfragen konnten wiederum in aggregierter Form ausgewertet werden. Für den zweiten Teil der Befragung wurde allerdings das Bundesland mit drei zurückgesandten Fragebögen außer Acht gelassen. Da zwei der mittelbe-

hördlichen Aufsichtsbehörden Statistiken führen und eine Aufsichtsbehörde keine führt, war eine Zusammenfassung für den zweiten Teil der Befragung nicht möglich. Eine Zusammenfassung wäre allerdings erforderlich geworden, da diese Fragen auch nach den Parametern mit Statistik/ohne Statistik getrennt ausgewertet wurden.

Die Fragen zur Einschätzung des Informationsstandes des Verbrauchers im dritten Teil konnten ebenfalls ohne länderspezifische Gewichtung als Expertenkenntnisse in aggregierter Form ausgewertet werden. Aufgrund des Charakters der Fragen als Einschätzungsfragen spielte das Führen einer Statistik hier keine Rolle. Es konnten alle Rückantworten – auch die drei Fragebögen aus einem einzigen Bundesland – zusammen ausgewertet werden. Bei den Fragen zu Vorschlägen zur Verbesserung des Verbraucherdatenschutzes wurde dann wiederum eine qualitative Auswertung gewählt. Insgesamt war es für die Auswertung daher nicht erforderlich, die Antworten nur entsprechend ihrer Gewichtung nach der Einwohneranzahl der einzelnen Bundesländer zu berücksichtigen.

Alle fehlenden Angaben wurden als „keine Angabe“ gewertet.

Bei „von-bis“-Angaben wurde der Durchschnittswert kodiert und bei der Auswertung berücksichtigt.

#### 7.5.3.2 Einzelfälle

In zwei Fällen wurde der Kenntnisstand zu einzelnen Themenbereichen auf einer Skala von 1-5 zum Teil mehrfach bewertet. Bei einer dieser beiden Rückantworten war diese mehrfache Bewertung nicht kommentiert, und es ließen sich Spuren auf dem Papier erkennen, dass jeweils ein Kreuzchen unkenntlich sein sollte. Durch die Übermittlung per Fax war das entfernte Kreuzchen allerdings wieder sichtbar geworden. In diesem Fall wurde das spurenfreie Kreuzchen gewertet. In dem zweiten Fall waren bei der Frage nach dem Kenntnisstand der Verbraucher über die in den einzelnen Branchen genutzten operativen Verarbeitungsprozesse bei der Branche „Freie Berufe“ und „Dienstleistungsunternehmen“ wegen „branchenspezifischen Unterschieden“ mehrfache Bewertungen gewählt. Diese Bewertungen wurden als neue Kategorie z.B. „zwischen mittelmäßig und schlecht“ berücksichtigt und bei der Mittelwertberechnung als Mittelwert miteinbezogen.

In einem Fall wurde bei der Frage nach den Anfragen in den einzelnen Themengebieten in das Textfeld „Andere“ das Stichwort „Arbeitnehmerdatenschutz“ und „Internationaler Datenschutz“ eingetragen und zusammen mit 11,1% gewichtet. Die Kodierung erfolgte hälftig mit jeweils 5,55% pro Kategorie.

In einem Fall wurden bei der Frage nach einer Veränderung der Anfragen in bestimmten Themenbereichen die Stichworte „elektronische Dienste und Medien, insbes. SPAM-Beschwerden“ in das Textfeld „Andere“ eingetragen. Diese Angabe wurde unter die vorgegebene Kategorie „Telekommunikation und neue Medien, Internetsicherheit“ subsumiert und in dieser Kategorie gezählt.

### 7.5.4 Ergebnisse und Interpretationen[282]

#### 7.5.4.1 Verwaltungsorganisation

Die Einbindung der datenschutzrechtlichen Aufsichtsbehörden für den nichtöffentlichen Bereich in die Verwaltung ist in den einzelnen Bundesländern unterschiedlich geregelt. Die Aufsichtsbehörde ist entweder in das Innenministerium eingegliedert (als Referat oder Teil eines Referates), an dieses angegliedert, unterliegt der Rechts- und Fachaufsicht des Innenministeriums oder untersteht als unabhängige Behörde bzw. Anstalt des öffentlichen Rechts der Rechtsaufsicht des zuständigen Innenministeriums, des Senats bzw. der Landesregierung. In manchen Bundesländern sind die Aufsichtsbehörden auch auf mittelbehördlicher Ebene organisiert und zum Teil dem Landesinnenministerium nachgeordnet.

Die Anzahl der Mitarbeiterinnen und Mitarbeiter im nichtöffentlichen Bereich bewegt sich zwischen 1,5 und 25 Arbeitskräften, wobei in fast allen Aufsichtsbehörden höchstens neun Mitarbeiterinnen und Mitarbeiter die Kontrolle im nicht-öffentlichen Sektor ausüben. Nur in einem einzigen Fall beschäftigen sich ca. 25 Personen mit dem Datenschutz im nichtöffentlichen Bereich. In diesem Fall war allerdings keine feste Zahl in Höhe von 25 Mitarbeiterinnen und Mitarbeitern angegeben. Vielmehr sind die Zuständigkeiten im fraglichen Bundesland nicht nach öffentlichem und nichtöffentlichen Bereich, sondern nach Lebensbereichen aufgeteilt. Es wurde angegeben, dass insgesamt fast 50 Personen beschäftig seien, wobei mindestens die Hälfte der Arbeitskraft auf den nicht-öffentlichen Bereich entfalle.

Mehr als die Hälfte der Aufsichtsbehörden führen eine Statistik über die Eingaben, die speziell den nicht-öffentlichen Bereich betreffen.

#### 7.5.4.2 Datenschutzrechtliche Anfragen

Die Anfragen je Woche sind nach Bundesland – auch aufgrund der unterschiedlichen Einwohneranzahl – sehr unterschiedlich. Die von den Aufsichtsbehörden angegebenen Werte lagen zwischen 2 und 110 Anfragen pro Woche. Die befragten Aufsichtsbehörden erhalten zu „Adresshandel und Direktwerbung“ mit durchschnittlich mehr als 16% die meisten Anfragen. Danach folgen die Themengebiete „Telekommunikation und neue Medien, Internetsicherheit“, „Auskunfteien, zentrale Warndateien und Inkassounternehmen“ sowie „Industrie, Handel und Handwerk“ mit rund 14%, 12% sowie 11%. Die Themen „Wohnungswirtschaft“ und „freie Berufe“ werden mit jeweils rund 10% angefragt. Kaum eine Rolle in der aufsichtsbehördlichen Praxis spielt das Thema „Versandhandel“. Hier erhalten die Aufsichtsbehörden mit fast 3% durchschnittlich die geringste Anzahl von Anfragen. Auch das Thema „Schufa“ wird mit etwas mehr als 3% kaum angefragt. Hier bleibt allerdings zu vermuten, dass die

[282] Die Auswertungen befinden sich im Anhang S. A115 ff.

Befragten die Anfragen zum Thema Auskunfteien unter die gleichgenannte Kategorie zusammenfassten und die Schufa nicht als Einzelkategorie berücksichtigten.

Auch die Auswertung bezogen auf die Länder, die eine Statistik führen, weist im Unterschied zur Gesamtauswertung keine großen Unterschiede auf. Hier sind ebenfalls die am häufigsten angefragten Themengebiete „Telekommunikation und neue Medien, Internetsicherheit“ (15%), „Adresshandel und Direktmarketing“ (13%), „Industrie, Handel und Handwerk“ (12%), „Wohnungswirtschaft“ (12%), „Freie Berufe“ (12%), „Auskunfteien, zentrale Warndateien und Inkassounternehmen“ (10%). Am wenigsten wurden nach dieser Auswertung die „Schufa“ mit knapp 2% und das Thema „Versandhandel“ mit fast 3% angefragt.

Bei der Auswertung der Antworten der Länder ohne Statistik ergibt sich ein etwas anderes Bild. Zwar werden „Adresshandel und Direktmarketing“ (25%), „Auskunfteien, zentrale Warndateien und Inkassounternehmen“ (17%) sowie „Telekommunikation und neue Medien, Internetsicherheit“ (12%) auch nach dieser Auswertung am häufigsten angefragt. Ebenso wird die Thematik „ Videoüberwachung, Videoaufzeichnung“ (11%) als häufig angefragter Bereich genannt. „Wohnungswirtschaft“ (8%) und „Freie Berufe“ (4%) spielen bei den Ländern ohne Statistik dagegen keine so große Rolle. Anfragen zum „Versandhandel“ werden in diesem Zusammenhang überhaupt nicht genannt.

Tabelle 9: Durchschnittliche Anzahl der Anfragen in den einzelnen Themengebieten in Prozent

| Themengebiete | Gesamt | Länder mit Statistik | Länder ohne Statistik |
|---|---|---|---|
| Anfragen zu Adresshandel und Direktwerbung | 16,3 % | 13,3 % | 25,0 % |
| Anfragen zu Telekommunikation und neue Medien, Internetsicherheit | 14,4 % | 15,3 % | 13,0 % |
| Anfragen zu Auskunfteien, zentrale Warndateien und Inkassounternehmen | 12,4 % | 10,0 % | 17,1 % |
| Anfragen zu Industrie, Handel und Handwerk | 11,2 % | 12,3 % | 5,8 % |
| Anfragen zur Wohnungswirtschaft | 10,2 % | 12,0 % | 7,5 % |
| Anfragen zu freien Berufen | 10,0 % | 11,5 % | 4,2 % |
| Anfragen zur Videoüberwachung und Videoaufzeichnung | 8,9 % | 7,6 % | 11,1 % |

Die Befragten gehen insgesamt von einem Anstieg der Anzahl der Anfragen gegenüber dem Vorjahr in den wichtigsten Themenbereichen um durchschnittlich 9,5% aus. Dabei verzeichnen zwei Befragte keinen Zuwachs, die anderen Befragten geben einen Zuwachs von 5% bis 20% an. Auch bei der Auswertung der Antworten der Länder, die eine Statistik führen, wird im Durchschnitt von einem Anstieg von 9% ausgegangen. Die Länder, die keine Statistik führen, halten durchschnittlich einen Zuwachs von 10% für realistisch.

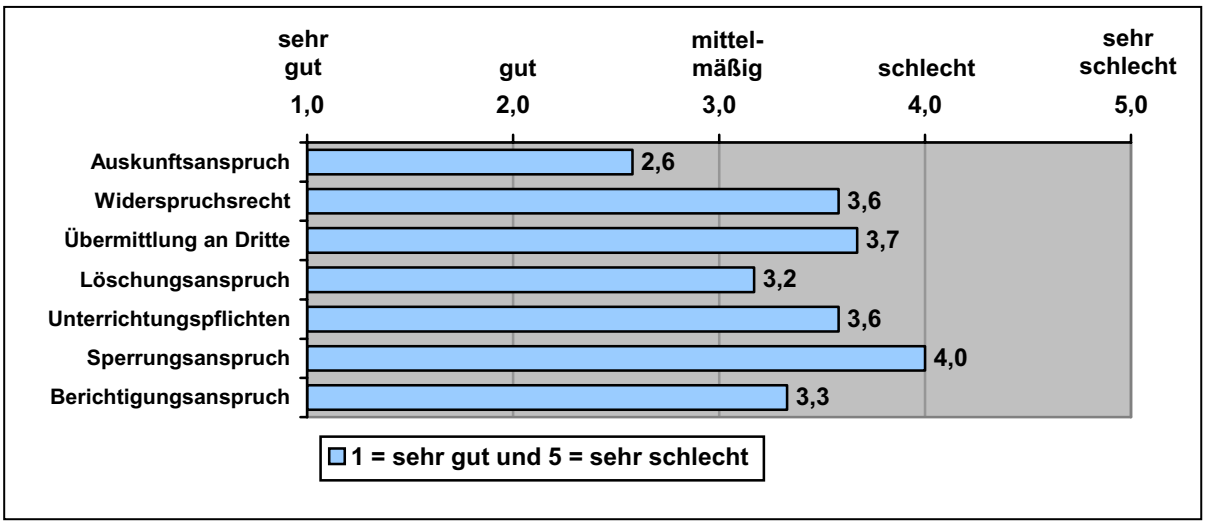
Die größten Zuwächse werden dabei in den Themenbereichen „Auskunfteien, zentrale Warndateien und Inkassounternehmen“ sowie „Videoüberwachung, Videoaufzeichnung“ verzeichnet.

#### 7.5.4.3 Einschätzungen zu Datenschutzkenntnissen und Datenschutzpflichten

Zunächst wurden die Befragten nach ihrer Einschätzung zum Kenntnisstand der Verbraucher über ihre Datenschutzrechte befragt. Die Bewertung erfolgte auf einer Skala von 1-5 wobei 1 mit „sehr gut“ und 5 mit „sehr schlecht“ gekennzeichnet war. Dabei wurden als Datenschutzrechte der Auskunftsanspruch, das Widerspruchsrecht, die Übermittlung der eigenen Kundendaten an Dritte, der Löschungsanspruch, die Unterrichtungspflichten der Unternehmen (Identität der verantwortlichen Stelle, Zweckbestimmung, Übermittlung an Dritte), der Sperrungsanspruch und der Berichtigungsanspruch abgefragt.

Die Befragten schätzten den Informationsstand der Petenten im Hinblick auf diese einzelnen Rechte sehr unterschiedlich ein. Der Auskunftsanspruch scheint danach relativ bekannt zu sein. Insofern gingen die Aufsichtsbehörden im Durchschnitt davon aus, dass die Verbraucher gut bis mittelmäßig über den Anspruch informiert sind. Hingegen werden die Kenntnis des Löschungsanspruches bzw. die Information über die Übermittlung von Kundendaten an Dritte als schlecht bzw. mittelmäßig bis schlecht eingestuft. Auch die Kenntnisse der Verbraucher über das Widerspruchsrecht und die Information über Unterrichtungspflichten werden im Durchschnitt als eher schlecht denn mittelmäßig bewertet. Beim Löschungsanspruch und Berichtigungsanspruch gehen die Befragten durchschnittlich von einem eher mittelmäßigen Kenntnisstand aus.

Abbildung 22: Durchschnittliche Einschätzung des Kenntnisstandes der Verbraucher bezogen auf einzelne Datenschutzrechte auf einer Skala von 1-5

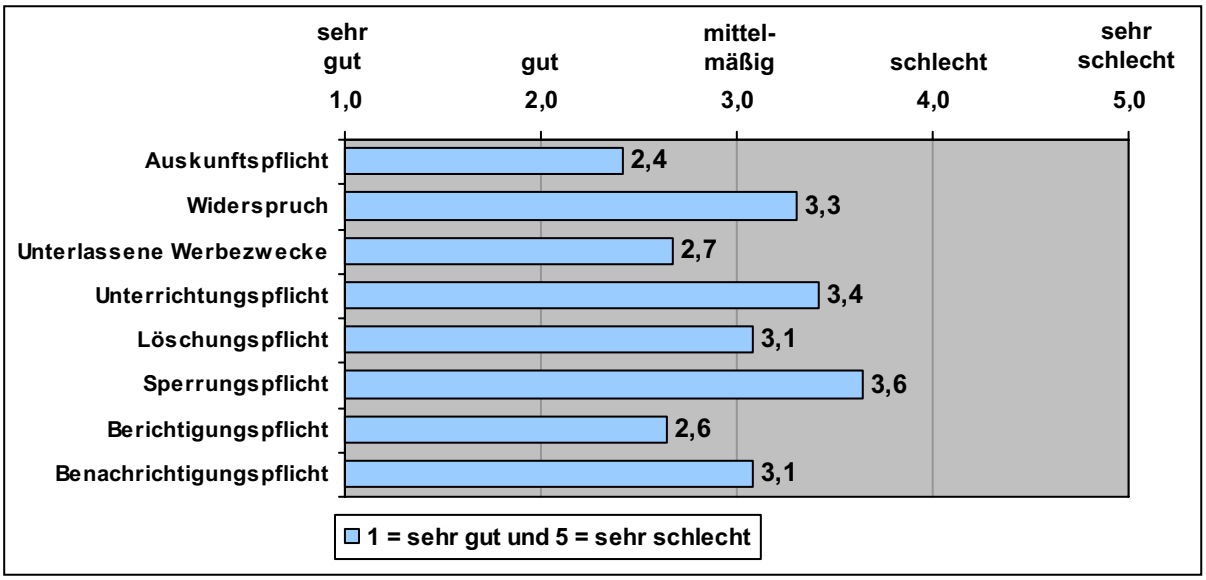



Spiegelbildlich zum Informationsstand der Petenten wurde auf der anderen Seite nach der Einschätzung der Kenntnisse der Unternehmen in Bezug auf ihre Datenschutzpflichten gefragt, wobei u.a. auch die Rechte der Verbraucher in Form der Verpflichtung für die Unternehmen abgefragt wurden. Insofern sollten die Befragten einschätzen, inwieweit die Unternehmen die Auskunftspflicht, die Pflicht zur Information über das Widerspruchsrecht bei

Verwendung zu Werbezwecken, die Pflicht, die Verwendung zu Werbezwecken bei Widerspruch zu unterlassen, die Unterrichtungspflichten nach § 4 Abs. 3 BDSG, die Löschungspflicht, die Sperrungspflicht sowie die Berichtigungspflicht und die Benachrichtigungspflicht bei Speicherung von Daten ohne Kenntnis des Betroffenen kennen.

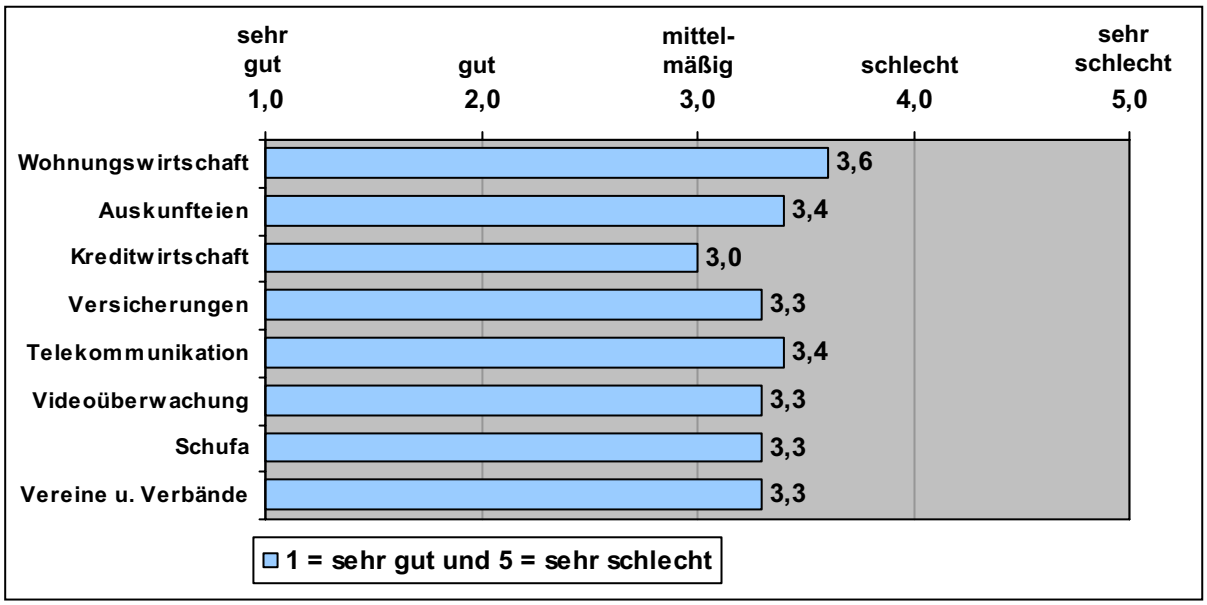
Insgesamt bewerteten die Befragten die Kenntnisse der Unternehmen bezüglich der einzelnen Pflichten als gut bis mittelmäßig und damit besser als den Informationsstand der Petenten. Nach Einschätzung der Aufsichtsbehörden besteht hier folglich eine Informationsasymmetrie. Als durchschnittlich eher schlecht wurde bei den Unternehmen nur die Kenntnis über die Sperrungspflicht identifiziert. Die Kenntnisse über Auskunftspflicht, Berichtigungspflicht und Unterlassen der Verwendung zu Werbezwecken bei Widerspruch wurde dagegen durchschnittlich zwischen gut und mittelmäßig eingeordnet. Das Wissen der Unternehmen in Bezug auf die Pflicht zur Information über das Widerspruchsrecht, die Löschungspflicht, die Benachrichtigungspflicht und die Unterrichtungspflichten wurde im Durchschnitt als mittelmäßig bewertet, wobei die Bewertung der Kenntnis über die Unterrichtungspflichten noch am schlechtesten ausfiel und eher von mittelmäßig bis schlecht eingeschätzt wurde.

Abbildung 23: Durchschnittliche Einschätzung des Kenntnisstandes der Unternehmen bezüglich ihrer Datenschutzpflichten auf einer Skala von 1-5



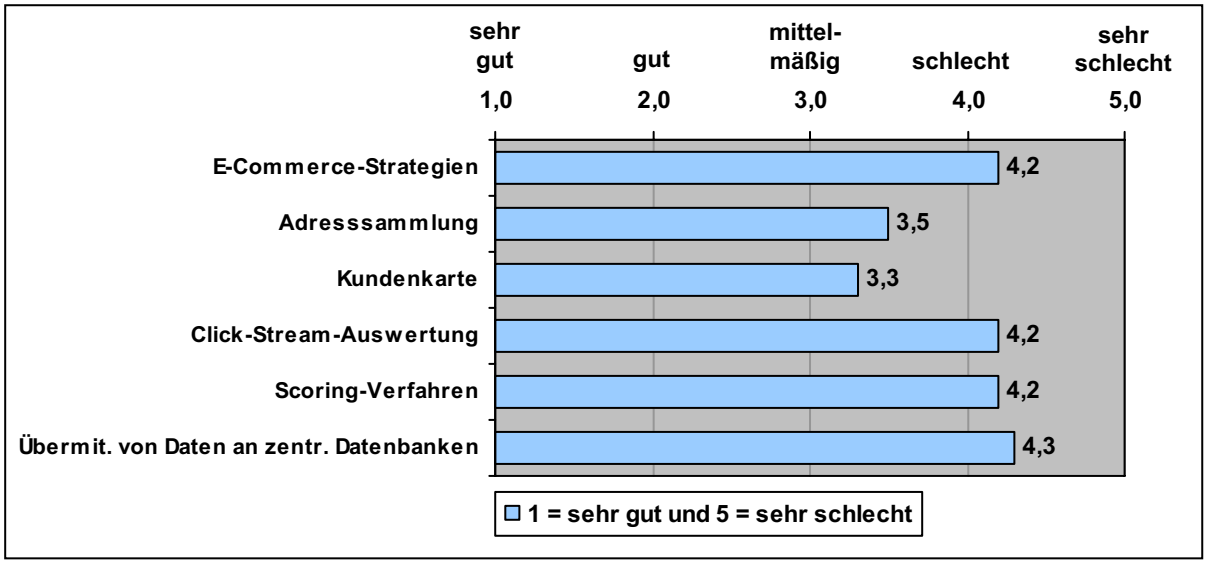

Am besten wissen die Verbraucher nach der Einschätzung der Befragten über die operativen Verarbeitungsprozesse im Bereich der Kreditwirtschaft Bescheid. Hier gingen die Aufsichtsbehörden im Durchschnitt von einem glatt mittelmäßigen Kenntnisstand aus. Ansonsten bewerteten die Befragten das Wissen der Verbraucher in Bezug auf die operativen Verarbeitungsprozesse zwischen mittelmäßig und schlecht. Wobei die Kenntnis in den meisten Branchen als eher mittelmäßig eingeschätzt wird, mit Ausnahme der Information im Bereich der Wohnungswirtschaft. Hier gehen die Befragten im Durchschnitt von einem eher schlechten Informationsstand aus.

Abbildung 24: Durchschnittliche Einschätzung des Kenntnisstandes der Verbraucher in Bezug auf die operativen Verarbeitungsprozesse ihrer Daten in den einzelnen Branchen auf einer Skala von 1-5




Im Bereich der in der Praxis tatsächlich anzutreffenden operativen Verwendungen ihrer Daten schätzen die Befragten den Kenntnisstand der Verbraucher als eher schlecht ein. Zwar halten die Befragten die Verbraucher bei Adresssammlungen durch Preisausschreiben mit nachfolgendem Adresshandel und in Bezug auf die Verwendungen im Rahmen einer Kundenkarte für noch eher mittelmäßig informiert. Bei den operativen Verarbeitungsprozessen im Rahmen von E-Commerce-Strategien, Click-Stream Auswertungen, Durchführung und Ausgestaltung von Scoring-Verfahren und bei der Übermittlung von Daten an zentrale Datenbanken der Versicherungswirtschaft gehen die Befragten durchschnittlich davon aus, dass die Verbraucher schlecht bis sehr schlecht informiert sind.

Abbildung 25: Durchschnittliche Einschätzung des Kenntnisstandes der Verbraucher bzgl. der operativen Verwendungen in der Praxis auf einer Skala von 1-5



Inwieweit die anfragenden Verbraucher vor der Eingabe eigene Schritte zur Lösung ihres Problems unternommen haben, ihre Datenschutzrechte gegenüber dem Unternehmen, also versucht haben, geltend zu machen, wird relativ unterschiedlich eingeschätzt. Im Durchschnitt gehen die Befragten davon aus, dass etwa die Hälfte zuvor eigene Schritte ergriffen haben, wobei sich die konkreten Prozentangaben zwischen 15% bis 80% bewegen.

Die Aufsichtsbehörden wurden zudem befragt, wie sie zu der These stehen, dass die Verbraucher im Großen und Ganzen über die Auskunftspflichten der Unternehmen und ihren Auskunftsanspruch informiert sind, sie ihre Rechte aber nur zu einem verschwindend geringen Anteil auch wahrnehmen. Die Befragten konnten hier vorgegebene Antworten von „Dieser These stimme ich voll zu“ bis hin zu „Ich halte diese These für Unsinn“ ankreuzen. Die Frage polarisierte die Befragten insofern, als dass etwa die Hälfte der Befragten der These überwiegend zustimmten und die andere Hälfte überwiegend nicht zustimmten.

Zum Ende der Befragung wurden die Aufsichtsbehörden nach Maßnahmen gefragt, die aus ihrer Erfahrung heraus geeignet wären, um den Verbraucherdatenschutz zu verbessern. Hier warteten die Befragten mit vielfältigen Antworten auf. Besonders interessant waren in diesem Zusammenhang die Forderungen, dass die Verletzungen der Auskunftspflicht oder der Unterrichtungspflichten bei Erhebung der Daten beim Betroffenen (§ 4 Abs. 3 BDSG) im Rahmen des Ordnungswidrigkeitenrecht sanktioniert wird. Weniger einschneidend und als Form der privatautonomen Konfliktregelung wurde vorgeschlagen, Rücktrittsrechte für die Betroffenen vorzusehen, wenn Datenschutzpflichten – insbesondere Informationspflichten – durch die Daten verarbeitende Stelle verletzt werden.

Vorgeschlagen wurde zudem, den Datenschutz über ein gesetzlich geregeltes Audit als Wettbewerbsfaktor einzuführen oder den Datenschutzgedanken professionell zu vermarkten.

Auch wurden konkrete gesetzliche Regelungen oder Rahmenbedingungen zu den Tätigkeiten der Auskunfteien und der Verwendung von Scoring-Systemen gefordert. Die Einführung von Verbandsklagerechten zum Ausgleich von Marktungleichheiten korrespondierte mit der Forderung nach einer stärkeren gerichtlichen Befassung mit Datenschutzthemen. Insgesamt wurde häufig auf die Verbesserung der Information durch verschiedenste Maßnahmen hingewiesen.

In einem Fall wurde auch vorgeschlagen, den Datenschutz als Marktmodell zu propagieren, d.h. die Daten des Betroffenen als Handelsgut zu betrachten.

## 7.6 Zusammenfassung der Ergebnisse der Befragung der Aufsichtsbehörden

Zusammenfassend lässt sich feststellen, dass die aufsichtsbehördlichen Experten die Erkenntnisse aus der Verbraucherbefragung von einem tendenziell guten Informationsstand über Auskunftsrecht, Widerspruchsrecht und Unterrichtungspflichten nicht durchgängig bestätigen. Die befragten Aufsichtsbehörden bewerteten die Kenntnisse des Widerspruchsrechts und von anderen Datenschutzrechten wie dem Berichtigungs- und insbesondere Sperrungsanspruch als eher schlecht. Ebenso fiel das durchschnittliche Urteil zum Kenntnis-

stand über die Übermittlung von Daten an Dritte und die Unterrichtungspflichten der Unternehmen aus. Auch hier sind die Petenten nach Auffassung der Aufsichtsbehörden eher schlecht als mittelmäßig informiert. Allein beim Auskunftsanspruch schätzen die Befragten den Informationsstand als gut bis mittelmäßig ein. Zumindest insofern ähnelt das Ergebnis der Verbraucherbefragung den Einschätzungen der Aufsichtsbehörden.

Zu beachten ist in diesem Zusammenhang, dass die Aufsichtsbehörden im Hinblick auf die Datenschutzrechte nach der Einschätzung des Kenntnisstandes ihrer Petenten, d.h. also der anfragenden Verbraucher und nicht der Verbraucher allgemein, befragt wurden. Es ist allerdings zu vermuten, dass auch bei der Frage nach dem Kenntnisstand der Verbraucher im Allgemeinen die Antworten nicht anders ausgefallen wären.

Zumindest bezogen sich die Fragen zu den in einzelnen Branchen genutzten operativen Verarbeitungsprozessen und operativen Verwendungen von Daten in der Praxis auf den Kenntnisstand des Verbrauchers im Allgemeinen. Auch in diesem Zusammenhang gehen die befragten aufsichtsbehördlichen Experten überwiegend von einem mittelmäßig bis schlechten Informationsstand aus.

Es bleibt nach der Einschätzung der Aufsichtsbehörden festzuhalten: Auskunfteien, zentrale Warndateien, Inkassounternehmen und die Wohnungswirtschaft stellen für die Verbraucher besonders undurchsichtige Bereiche dar. Hier schätzten die Befragten den Kenntnisstand der Verbraucher über die operativen Verarbeitungsprozesse am schlechtesten ein.

Die Kenntnisse zu den operativen Verwendungen von Daten bewerteten die Aufsichtsbehörden durchschnittlich noch schlechter. Zwar halten die Befragten die Verbraucher für noch eher mittelmäßig informiert, wenn es um die möglichen Datenverwendungen in Rahmen von Kundenkarten und um die Adresssammlung bei Preisausschreiben zu Adresshandelszwecken geht. Bei allen anderen vorgegebenen Bereichen (E-Commerce, Click-Stream, Scoring-Verfahren, zentrale Warndateien) schätzen die Befragten den Informationsstand dagegen mit eher schlecht bis sehr schlecht ein. Hier herrscht nach der Einschätzung der Aufsichtsbehörden ein Informationsdefizit. Sind die Verbraucher über die möglichen Verarbeitungsarten schlecht informiert, dann sind die Möglichkeiten dementsprechend begrenzt, die Verwendung ihrer Daten zu kontrollieren.

Im Unterschied zu den Ergebnissen aus der Befragung der Verbraucherberaterinnen und –berater gehen die aufsichtsbehördlichen Experten von einer viel höheren Anzahl von anfragenden Verbrauchern aus, die zuvor eigene Schritte zur Lösung ihres Problems unternommen haben. Hiernach sollen 50% der Anfragenden zuvor versucht haben, ihre Datenschutzrechte gegenüber dem Unternehmen geltend zu machen. Bei den Verbraucherberaterinnen und -beratern waren dies gerade mal durchschnittlich 10% der Verbraucher, die sich mit datenschutzrechtlichen Anfragen an die Beratungsstellen wenden. Eine Erklärung für diese Diskrepanz ist, dass diejenigen, die sich mit ihren Problemen schon direkt an die Aufsichtsbehörden wenden, vermutlich insgesamt besser über den Datenschutz informiert sind. Zumindest ist ihnen die für datenschutzrechtliche Probleme speziellere Anlaufstelle bekannt. Nach der Verbraucherbefragung sehen nur 11% der Verbraucherinnen und Verbraucher den/die Datenschutzbeauftragte/n als Anlaufstelle an. Diese Verbraucher sind dann mögli-

cherweise eher in der Lage, sich zunächst an die Unternehmen zu wenden, um ihre Rechte geltend zu machen.

Für die aufgestellte These, dass die Verbraucher im Großen und Ganzen über die Auskunftspflichten der Unternehmen und über ihren Auskunftsanspruch informiert sind, sie ihre Rechte aber nur zu einem verschwindend geringen Anteil auch wahrnehmen, lässt sich aus den Antworten der Befragten kein eindeutiges Ergebnis erzielen.

## 7.7 Zusammenfassende Bewertung aller Ergebnisse

### 7.7.1 Wahrnehmung von Datenschutzrechten

Der Befund der Befragung der betrieblichen Datenschutzbeauftragten ist eindeutig: Die Verbraucher bzw. Kunden nehmen ihre Datenschutzrechte so gut wie gar nicht wahr. Zwar gehen die Aufsichtsbehörden davon aus, dass 50% der bei ihnen anfragenden Petenten zuvor eigene Schritte zur Lösung ihres Problems gegenüber dem Unternehmen geltend gemacht haben. Diese Angabe beschränkt sich aber nur auf den kleinen Teil der Bevölkerung, die erstens von der Existenz der Aufsichtsbehörden weiß und zweitens sich auch an diese wendet.

Woran liegt es also, dass die Verbraucher von den ihnen zur Verfügung stehenden Datenschutzrechten so gut wie keinen Gebrauch machen? Darauf könnte die Gegenfrage gestellt werden: Warum sollten sie auch? Warum sollten sie ihre Rechte geltend machen, wenn für sie kein Anlass besteht, ihre Datenschutzrechte wahrzunehmen. Die Gründe hierfür könnten vielfältig sein: Die Verbraucher sehen ihre Daten bei den Unternehmen gut aufgehoben, sie machen sich keine Gedanken über die Verwendung ihrer Daten, weil die Konsequenzen für sie nicht unmittelbar zu spüren sind, sie haben gegenüber der Definitionsmacht der Unternehmen bereits resigniert oder sie vertrauen auf die Funktionsfähigkeit der staatlichen Aufsichtsbehörden. Wie auch immer - weder das konkrete noch das abstrakte Wissen über die eigenen Rechte ist ein Indikator, ob die verantwortlichen Unternehmen die Daten ihrer Kunden auch rechtmäßig erheben, verarbeiten oder nutzen.

### 7.7.2 Informationsgrad der Verbraucher über ihre Rechte

Ein Erklärungsansatz für die geringe Wahrnehmung der Datenschutzrechte ist, dass die Verbraucher nicht hinreichend über ihre Datenschutzrechte informiert sind, um sie ausüben zu können. Nach den Erfahrungen der Verbraucherberaterinnen und –berater ist die unzureichende Information der Hauptgrund für die Zurückhaltung der Verbraucher, ihre Datenschutzrechte in Anspruch zu nehmen. Auch die Aufsichtsbehörden gehen von einem mittelmäßigen bis schlechten Kenntnisstand ihrer Petenten aus. Eine repräsentative Untersuchung des BAT Freizeit- und Forschungsinstituts aus dem Jahre 2001 kommt zu einem ähn-

lichen Ergebnis für die Nutzer des Internets. Danach fühlt sich nur jeder vierte PC-Benutzer (25%) richtig darüber informiert, wie er seine Daten wirksam schützen kann.[283]

Die Verbraucherbefragung bestätigt diese Einschätzung nur bedingt, denn ein Großteil der befragten Verbraucher zeigt sich über seine wesentlichen Rechte zumindest in allgemeiner Form informiert. Allerdings lassen die Antworten auf die Fragen im Rahmen der Verbraucherbefragung keinen Rückschluss darauf zu, ob und dass die Verbraucher ihre Rechte auch in einer konkreten Situation kennen. Zudem können auf der Grundlage der Verbraucherbefragung die Informationen der Verbraucher zu den spezifischen Datenschutzrechten der Löschung, Sperrung, Berichtigung, Benachrichtigung nicht beurteilt werden. Insbesondere in diesem Bereich haben die Verbraucher nach Einschätzung der Experten aus den Aufsichtsbehörden aber große Informationsdefizite.

Gleichwohl ist nach den Ergebnissen davon auszugehen, dass die Verbraucher über ihre Auskunftsansprüche und gewisse Unterrichtungsverpflichtungen im Grundsatz gut informiert sind. Auch die Experten aus den Aufsichtsbehörden bewerten den Informationsstand zum Auskunftsanspruch im Unterschied zu anderen Datenschutzrechten positiv. Das Ergebnis zeigt also, dass die Verbraucher ihrem „Grundgefühl“ nach ganz gut über ihre Rechte Bescheid wissen.

### 7.7.3 Keine Erwartungen an die Rechtswahrnehmung

Es bleibt die Frage, warum die Verbraucher trotzdem in so geringem Maße z.B. Auskunft über die zu ihrer Person gespeicherten Daten verlangen. Denkbar ist, dass sie mit der Wahrnehmung ihrer Rechte keine positive Erwartung verbinden. Angesichts der Machtasymmetrie zwischen Verbraucher und Wirtschaft – so die Hypothese – versprechen sie sich nichts davon, ihre Rechte geltend zu machen. Diese Deutung wird aber von den Verbraucherberaterinnen und –beratern nicht geteilt. Sie sehen in der Desillusionierung der Verbraucher eher selten die Ursache für die geringe Wahrnehmung von Datenschutzrechten. Dabei ist zu berücksichtigen, dass die Beratungsstellen Anlaufstelle für gerade den Typ Verbraucher sind, der sich nicht „geschlagen geben“ will, sondern sich zu informieren versucht, um seine Rechte geltend zu machen. Um die These der Desillusionierung in Sachen Datenschutz zu rechtfertigen, hätte sie im Übrigen bei der Frage nach den Assoziationen zum Thema Datenschutz eine Bestätigung finden müssen, was nicht der Fall ist.

### 7.7.4 Datenschutz ohne Stellenwert?

Denkbar ist außerdem, dass die Verbraucher dem Datenschutz keinen hohen Stellenwert einräumen oder es ihnen schlicht egal ist, was mit ihren personenbezogenen Daten passiert. Gegen eine solche Verbrauchereinstellung zum Thema Datenschutz sprechen allerdings die Erkenntnisse aus den durchgeführten Befragungen:

---

[283] Opaschowski, DuD 2001, 678 (679), der in den Jahren 1998 und 2001 je eine repräsentative Umfrage mit 3.000 Teilnehmerinnen und Teilnehmern durchgeführt hat. Vgl. auch Opaschowski, DuD 1998, 654 ff.; Opaschowski in: Roßnagel, HdBDatSchR, Kap. 2.1.

Nicht ohne Grund assoziieren die zum Thema Datenschutz befragten Verbraucher zahlreich die Stichworte „Bankgeheimnis“ und „Privatsphäre“. Zudem beschäftigt die Verbraucher bei den Assoziationen zum Thema Datenschutz die Praxis der Weitergabe und Übermittlung ihrer Daten. Immerhin äußern fast die Hälfte der befragten Verbraucher Bedenken gegen die Nutzung einer Kundenkarte. Über die Hälfte der Verbraucherberaterinnen und –berater stellen einen Anstieg von datenschutzrelevanten Anfragen in ihrer Beratungspraxis fest. Dabei nannten sie besonders häufig als Grund für diesen Anstieg die Belästigung der Verbraucher durch die Zunahme an unerwünschter Werbung sowie die Bedeutung des Adresshandels. Schließlich ergibt sich auch aus den an die betrieblichen Datenschutzbeauftragten gerichteten Anfragen, dass den Betroffenen die Übermittlung ihrer personenbezogenen Daten an Dritte Sorgen bereitet. Auch die Experten aus den Aufsichtsbehörden berichten von einer zunehmenden Anzahl an Anfragen. Danach ist den Verbrauchern eine unkontrollierte Verarbeitung ihrer persönlichen Daten keineswegs egal.

Diese These wird durch eine repräsentative Umfrage des BAT-Freizeitinstitut aus dem Jahr 2001 bestätigt. Die Befragung ergab u.a., dass 42% der Bevölkerung der Meinung sind, dass sie selbst und andere „zu wenig darauf achten, welche Informationen und Auskünfte sie wem geben“, wobei dieser Anteil mit der beruflichen Stellung wächst.[284] Die Ergebnisse der Studie zeigen zudem, dass der Datenschutz als Akzeptanzfaktor für die Entwicklung der in der Informationsgesellschaft angebotenen Dienste große Bedeutung hat.[285]

### 7.7.5 Datenschutzsensibilität und Systemvertrauen

Eine näher liegende Deutung ist, dass die Verbraucher für das Thema Datenschutz zwar eine Sensibilität und Wertschätzung besitzen, ihr aus der Verarbeitung ihrer Daten möglicherweise entstehendes persönliches Risiko allerdings für gering einschätzen. Diese Risikobewertung kann damit zusammenhängen, dass sich die Verbraucher von den Gefahren einer unbestimmten Datenverarbeitung persönlich nicht betroffen fühlen oder ihr Vertrauen in die staatlichen oder selbstregulativen Sicherungsmechanismen ausreichend ist, mit der Folge ihre Rechte nicht wahrnehmen zu müssen. Ein maßgeblicher Faktor für dieses Systemvertrauen ist das Wissen, mit Rechten gegenüber den Daten verarbeitenden Stellen ausgestattet zu sein. Das Wissen um die eigenen Rechte und ihre fehlende Inanspruchnahme sind also kein Widerspruch, sondern sie stehen in einem engen Zusammenhang. Rechte hat man nicht, um von ihnen jederzeit Gebrauch zu machen, sondern um von ihnen bei Bedarf, wenn es nicht anders geht, Gebrauch machen zu können. Jedes andere Verhalten wäre auch wenig ökonomisch, denn die Wahrnehmung eigener Rechte macht den Einsatz und die Verfügbarkeit von Ressourcen wie Information, Kompetenz, Zeit und Kraft erforderlich. Solange das Zutrauen in die Rechtmäßigkeit der Datenverarbeitung also im Grundsatz besteht, gibt es für

[284] Opaschowski in: Roßnagel, HdBDatSchR, Kap. 2.1, Rn. 53. 54% bei den Selbständigen und Freiberuflern sowie 60% bei den Leitenden Angestellten.

[285] Bizer, Datenschutzrecht, in Schulte (Hrsg.): Handbuch des Technikrechts, 2003, S. 561 (576 f. m.w.N.); Scholz in: Roßnagel, HdBDatSchR, Kap. 9.2, Rn. 143 mwN.

die betroffenen Verbraucher auch keinen Anlass, Ressourcen in die Wahrnehmung seiner Rechte zu investieren.

Unterstellt, die Verbraucher sind ausreichend und gut informiert, so wäre diese Bewertung immerhin Ausdruck der informationellen Selbstbestimmung, die durch gute Erfahrungen bestätigt oder durch schlechte Erfahrungen widerlegt werden könnte. Ihnen wird zugrunde liegen, zu welchen Zwecken Unternehmen die Daten der Verbraucher tatsächlich verwenden. Bedeutung für die Risikobewertung hat also weniger das Wissen über die eigenen Rechte als vielmehr das Wissen über die *tatsächlichen* Verarbeitungsbedingungen der eigenen Daten.

#### 7.7.5.1 Transparenz der tatsächlichen Verwendungsbedingungen

Die Befragung zeigt, dass die Verbraucher eine weitgehend zutreffende Vorstellung darüber haben, welche Informationen ihnen von den verantwortlichen Stellen mitzuteilen sind und ob sie Auskunft verlangen oder Widerspruch einlegen dürfen. In der alltäglichen Praxis wenden die Verbraucher dieses Wissen allerdings nicht an. Zur Absicherung ihrer persönlichen Daten werden sie wenig bis gar nicht initiativ.

Die Ursache für die Zurückhaltung der Verbraucher beruht nicht auf einer Unkenntnis über die ihnen zustehenden Rechte. Der Verbraucher weiß mehr als nur dem Grundgefühl nach über seine Rechte Bescheid. Aber mangels Kenntnis und Vorstellung über die tatsächlichen Datenflüsse und der konkreten operativen Verwendungen seiner Daten fehlt der konkrete Anlass, diese Rechte geltend zu machen. Die Kenntnis der allgemeinen Rechtslage ist für den Verbraucher zu abstrakt, um die Bedeutung der einzelnen Verarbeitungen seiner Daten auf seine persönliche Situation beziehen zu können.

Dort, wo sich eine Datenverarbeitung in einer konkreten Beeinträchtigung wie bspw. in Form unerwünschter Werbung unmittelbar auswirkt oder durch die Medien eine verstärkte Aufklärung über Zusammenhänge zwischen Gewinnspielen und Adressweitergaben stattgefunden hat, ist das Misstrauen der Verbraucher deutlich höher. So ist nach Angaben der Verbraucherberaterinnen und –berater der Anstieg an datenschutzrechtlichen Anfragen in den letzten Jahren deutlich auf die wachsende Beeinträchtigung durch unerwünschte Werbung, insbesondere auf eine vermehrte Werbung für Gewinnspiele, zurückzuführen. Sobald die Verbraucher den Zusammenhang zwischen einer Verwendung ihrer Daten und einer konkreten Beeinträchtigung erkennen können, schlägt sich dies in einer negativen Bewertung nieder, die auch zu einem aktiven Handeln führen kann.

Auch die Aufsichtsbehörden bewerten den Informationsstand der Verbraucher über konkrete operative Verwendungen ihrer Daten als eher schlecht. Zwar gehen die Experten aus den Aufsichtsbehörden davon aus, dass sich die Verbraucher über die Bedeutung von Preisausschreiben zur Generierung von Adressen und anschließendem Adresshandel im Verhältnis zu anderen Verwendungen noch relativ gut bewusst sind. Sie schätzen den Kenntnisstand allerdings auch nur als mittelmäßig ein. Bei anderen operativen Verwendungen halten die Aufsichtsbehörden die Kenntnisse der Verbraucher in der Regel im Durchschnitt für schlecht.

Eine nicht unbeträchtliche Zahl der Verbraucherberaterinnen und –berater geht zudem davon aus, dass den Verbrauchern häufig nicht bewusst ist, dass ihr Problem einen datenschutzrechtlichen Bezug hat. Nach Ansicht dieser Verbraucherberaterinnen und -berater stellen die Verbraucher häufig keinen Zusammenhang zwischen der Verarbeitung ihrer Daten und dem Entstehen ihres Problems her. Ohne diese Kenntnis können die Verbraucher aber auch nicht erkennen, dass ihnen die Anwendung ihrer Datenschutzrechte möglicherweise weiterhelfen könnte.

Den Verbrauchern fehlt mit anderen Worten die Transparenz über die konkrete Art und Weise der Verarbeitung ihrer Daten. Bei der Herausgabe ihrer Daten ist den Verbrauchern nicht hinreichend bewusst, was genau mit ihren Daten geschieht. Es wird den Verbrauchern weder deutlich, über welche Möglichkeiten der Datenverwendung das Unternehmen verfügt, noch welche nachteiligen Folgen ihnen entstehen können. Ohne eine Vorstellung über das „Geschehen hinter den Kulissen“ besteht auch wenig Anlass, eine solche Verwendung und ihre Legitimation zu hinterfragen. Bestätigung findet diese Interpretation in der bereits zitierten, repräsentativen Umfrage des BAT Freizeitinstituts. Als problematisch wird nach dieser Untersuchung das geringe Wissen der Bürger eingeschätzt, „was mit ihren Daten geschieht“. 40% nannten die Unwissenheit der Bevölkerung als Hauptursache für Datenmissbrauch – wobei der Anteil unter den Menschen mit Universitätsabschluss mit 50% der Befragten deutlich höher ist.[286]

Mehr als die Hälfte der befragten Verbraucher steht einer Kundenkarte vorbehaltlos gegenüber. Die aufsichtsbehördlichen Experten bewerten die Kenntnis der Verbraucher über die Möglichkeiten der Datenverarbeitungen durch eine Kundenkarte als eher mittelmäßig. Demnach fehlen den Verbrauchern offensichtlich die Informationen, dass eine Kundenkarte neben der positiven Rabattgewährung über die Zusammenführung ihrer persönlichen Daten auch nachteilige Folgen für sie haben kann.

Anfragen aus der Beratungspraxis der Verbraucherberaterinnen und -berater sind häufig auf Formen der Datenübermittlung zurückzuführen, mit deren Folgen und Auswirkungen die um Rat suchenden Verbraucher plötzlich konfrontiert werden. Auch die aufsichtsbehördlichen Experten bewerteten den Informationsstand der Verbraucher über die Voraussetzungen und Folgen der Übermittlung von Daten an Dritte ebenfalls als eher schlecht. Über Datenübermittlungen an die zentralen Warndateien in der Versicherungswirtschaft sind die Verbraucher nach Ansicht der Aufsichtsbehörden schlecht bis sehr schlecht informiert. Unter den wenigen datenschutzrelevanten Anfragen, die die Unternehmen erhalten, spielen Anfragen zur Datenübermittlung an Dritte eine relativ große Rolle. Auch die betrieblichen Datenschutzbeauftragten stufen die Information der betroffenen Verbraucher über die Weitergabe von Daten im Unterschied zu anderen Informationen als besonders wichtig ein.

[286] Opaschowski in: Roßnagel, HdBDatSchR, Kap. 2.1, Rn. 54.

#### 7.7.5.2 Auswirkungen auf das Systemvertrauen

Die Befragungsergebnisse deuten darauf hin, dass Art und Umfang der konkreten Datenflüsse und ihrer operativen Verwendungen den Verbrauchern unbekannt bzw. undurchsichtig sind. Sie müssen also darauf vertrauen, dass die Verarbeitung ihrer Daten in ihrem Interesse erfolgt. Solange dieses Grundvertrauen besteht, fehlt ein hinreichender Grund, eigene Datenschutzrechte wahrzunehmen.

Umgekehrt kann aber eine individuelle bzw. auch eine über die Medien verstärkte kollektive negative Erfahrung das Systemvertrauen in die „Ordnungsgemäßheit" einer Datenverarbeitung nachhaltig erschüttern. So zeigt eine andere Studie aus dem Jahr 2005, dass das Vertrauen in eine verbraucherfreundliche Regulierung des Datenschutzes in dem Maße signifikant abnimmt, in dem den Betroffenen bewusst wird, dass Gesetzesverstöße für die Verantwortlichen tatsächlich ohne eine Sanktion bleiben.[287] Die Bedeutung dieser Einschätzung wird deutlich, wenn man sich vor Augen hält, dass nach der BAT-Umfrage, knapp ein Drittel der Befragten (29%) der Meinung war, schon einmal das Opfer eines Datenmissbrauchs geworden zu sein. Ein Fünftel (20%) waren der Meinung, dies sei schon mehrfach passiert.[288] Als Ursache vermuteten 39% eine bewusste Missachtung der Datenschutzgesetze und –vorschriften, 37% zu geringe Strafen, 32% die Ausnutzung mangelnder Kontrollen der Aufsichtsbehörden.[289] Das Vertrauen in die Systemstabilität ist mit anderen Worten alles andere als eine zuverlässige Akzeptanzgröße, auf die sich die für eine Datenverarbeitung Verantwortlichen verlassen könnten. Der zum Schutz der betroffenen Verbraucher gesetzte Rechtsrahmen muss sich bewähren, indem Verstöße auch befolgt und sanktioniert werden.

Aus der Akzeptanzfrage der BAT-Umfrage ergibt sich, dass nach der Einschätzung der Befragten die Datenverarbeitung ganzer Branchen buchstäblich ins Bodenlose fällt.[290] Gegenüber bestimmten Branchen besteht sogar ein offenes Misstrauen: So halten nur 31% der Befragten die Versicherungen beim Umgang mit personenbezogenen Daten für zuverlässig. Noch weniger Vertrauen bringen die Bürger für die Bereiche Versand- und Adresshandel auf. Nur 10% trauen dem Versandhandel und nur 8% dem Adresshandel eine ordnungsgemäße Verwendung ihrer persönlichen Daten zu. Die meisten der Befragten befürchten persönliche Nachteile bzw. eine Beeinträchtigung ihrer Privatsphäre.[291]

In der Intransparenz der Datenverwendungen liegt also auch ein hohes Risiko für die Daten verarbeitende Wirtschaft. Das Zutrauen in die Rechtmäßigkeit der Datenverwendung muss keineswegs konstant bleiben. Die Beispiele der Versicherungen oder des Versandhandels zeigen, dass ganze Branchen das Vertrauen „aufs Spiel setzen" können, sie würden die Da-

---

[287] Siehe Spiekermann in: ULD/Humboldt-Universität, TAUCIS, Kap. 5, Anschnitt 3.3. Die Studie ist im Auftrag des BMBF erstellt, zum 31. März 2006 abgeschlossen und noch nicht veröffentlicht.

[288] Opaschowski, DuD 2001, 681.

[289] Opaschowski in: Roßnagel, HdBDatSchR, Kap. 2.1, Rn. 55.

[290] Opaschowski, DuD 2001, S. 678 – 681.

[291] Opaschowski, DuD 2001, 678 (679).

ten ihrer Kunden bzw. der Verbraucher fair und rechtmäßig verwenden. Je abhängiger das Geschäft dieser Branche von der Akzeptanz der Verbraucher ist, desto gravierender können die geschäftlichen Auswirkungen eines solchen Misstrauens der Verbraucher sein. Je unabhängiger eine Branche von den Interessen der Verbraucher handeln kann, wie dies bspw. beim Adresshandel der Fall ist, desto größer ist der ordnungspolitische Handlungsbedarf.

Ein vergleichbares Schicksal wie den Versicherungen und dem Versandhandel könnte auch den Instituten der Kreditwirtschaft blühen. In einer Länder vergleichenden Untersuchung aus dem Jahre 1999 wurde die Vertrauenswürdigkeit der Banken in Sachen Datenschutz getestet. In Deutschland bewerteten die Befragten die Vertrauenswürdigkeit überwiegend positiv (70%).[292] Nach der Untersuchung des ULD zum Einsatz von Scoringsystemen zeigte sich, dass die Kreditinstitute entweder nicht auf die Fragen zur Funktionsweise ihrer Scoringsysteme antworten wollten oder aber, soweit sie antworteten, sie ihre Kunden entweder nicht oder nur auf spezielle Nachfrage über den Einsatz eines internen Scoringsystems unterrichten.[293] Im weiteren Verlauf der Untersuchung stellte sich zudem heraus, dass den Verbrauchern weder die Nutzung von internen noch von externen[294] Scorewerten zur Kreditentscheidung transparent gemacht wird. Bei der hohen öffentlichen Aufmerksamkeit des Themas Kreditscoring spricht einiges für die Annahme, dass die Vertrauenswürdigkeit der Banken in Sachen Datenschutz durch dieses Verhalten nicht gerade gestiegen ist.

Es zeigt sich, dass der Datenschutzsensibilität der Bevölkerung durch einen wirksamen Datenschutz Rechnung zu tragen ist. Zentraler Ansatzpunkt ist, dass den Verbrauchern vertrauenswürdige Informationen über die tatsächliche Verwendung ihrer Daten zur Verfügung stehen, ohne die ihr Systemvertrauen in den Rechtsrahmen des Datenschutzes nicht erhalten werden kann.

### 7.7.6 Transparenz und Entscheidung

Aus der Befragung der betrieblichen Datenschutzbeauftragten lässt sich der Schluss ziehen, dass die Einbeziehung der betroffenen Verbraucher in die Entscheidung über die Verwendung ihrer Daten in Form einer Einwilligungslösung zu einem deutlich höheren Informationsgrad führt. Auch wenn wegen der geringen Fallzahlen nur von einer Tendenz gesprochen werden kann, so ergibt sich aus der Nutzung einer Einwilligung eine erhöhte Bereitschaft, seine Datenschutzrechte wahrzunehmen. Ursache hierfür wird sein, dass die Einwilligung im Zusammenhang mit anderen Erklärungen besonders hervorgehoben werden muss (§ 4 a Abs. 1 Satz 4 BDSG). Der einfache Datenschutzhinweis (§ 4 Abs. 3 BDSG) unterliegt dieser Anforderung nicht, so dass er von den Verbrauchern leicht übersehen werden kann. Zudem

---

[292] IBM Global Service, IBM Multi-National Consumer Privacy Survey, Oktober 1999.

[293] „Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher“, Forschungsprojekt des ULD im Auftrag des BMVEL, S. 28,29.

[294] Externer Scorewert, z.B. erstellt von einer Auskunftei auf der Grundlage des dort vorhandenen Datenmaterials.

macht es einen gravierenden Unterschied, ob von dem Verbraucher eine aktive Handlung oder eine passive Kenntnisnahme erwartet wird.

Bemerkenswert ist in diesem Zusammenhang, dass sich die Gestaltung der Mitwirkung des betroffenen Verbrauchers in Form einer Opt-In bzw. Opt-Out-Erklärung nach der Wahrnehmung der Befragung der betrieblichen Datenschutzbeauftragten nicht auf die Verweigerungsrate der Verbraucher auswirkt. Auf der Grundlage dieser Einschätzung gibt es keinen Grund, den Verbrauchern die Möglichkeit einer aktiven Entscheidung in Form eines Opt-In vorzuenthalten. Sie birgt im Übrigen für die verantwortlichen Stellen bzw. Unternehmen die Chance zu einer offenen Kommunikation mit dem Verbraucher, ob und inwieweit die von dem Unternehmen beabsichtigte Verarbeitung auch in seinem Interesse liegt.

# 8 Defizitanalyse des Datenschutzrechts

## 8.1 Modernisierung des Datenschutzes

Die umfassendste Analyse des geltenden Datenschutzrechts stammt von Roßnagel, Pfitzmann und Garstka in Form eines Gutachtens für das Bundesministerium des Innern.[295] Das Gutachten ist in einem umfassenden Konsultationsprozess entstanden, an dem zahlreiche Fachleute aus den Aufsichtsbehörden, der Verwaltung, der Wirtschaft, der Wissenschaft, der Verbraucherschutzverbände sowie aus Bürgerrechtsorganisationen beteiligt waren. Einzelne Beiträge zu dem Reformprozess sind veröffentlicht worden.[296] Die Analyse ist insofern umfassend, als sie die Angemessenheit des gesamten Datenschutzrechts einschließlich der für die öffentlichen Stellen geltenden bereichsspezifischen Regelungen vor dem Hintergrund der technischen Entwicklung in den Blick nimmt. Die Gutachter kommen zu dem Ergebnis, dass das bisherige Datenschutzkonzept angesichts der technischen Entwicklung von der zentralen Datenverarbeitung zur dezentralen, miniaturisierten und vernetzten Datenverarbeitung und den sich hieraus ergebenden Gefahren einer umfassenden Profilbildung der Betroffenen überholt und nicht risiko- und zieladäquat ist.[297] Mit Belegen wird nachgewiesen, dass das Datenschutzrecht über die Summe der bereichsspezifischen Regelungen in sich intransparente und widersprüchliche Regelungen enthält. Vor diesem Hintergrund bedürfe es eines einheitlichen medienübergreifenden Datenschutzrechts. An anderer Stelle ist gefordert worden, dass auf die Konvergenz der Technik die Konvergenz des Datenschutzrechts folgen müsse.[298] Die Analyse und Kritik des Gutachtens hat auch für den Verbraucherdatenschutz Bedeutung.

Die Aufgaben der Modernisierung hatten die Gutachter in vier Kernaussagen zusammengefasst: Datenschutz müsse effektiv werden, d.h. sich auf die wesentlichen Bedrohungen für die informationelle Selbstbestimmung konzentrieren, vollzugsgeeignet und wirksam kontrolliert werden. Datenschutz müsse risikoadäquat stattfinden, d.h. die Regelungen müssen den Schutz der informationellen Selbstbestimmung „in einer vernetzten und in alle Lebensbereiche hineinragenden Verarbeitung gewährleisten“. Datenschutz müsse verständlich werden, d.h. die Anforderungen müssen „einfach, übersichtlich und klar strukturiert sein“. Und schließlich müsse der Datenschutz attraktiv werden, d.h. es müsse für die Betroffenen und für die Datenverarbeiter einleuchtend und sinnvoll sein, Datenschutzmaßnahmen zu ergreifen.[299]

---

[295] Roßnagel/Pfitzmann/Gartska, Modernisierung des Datenschutzrechts 2002.

[296] Vgl. Bizer, DuD 2001, 274 ff; Weichert, DuD 2002, 264 ff.

[297] Roßnagel/Pfitzmann/Garstka, Modernisierung, S. 22 ff.

[298] Bizer, DuD 2001, 274, 276; DuD 2004, 6, 8, 12.

[299] Roßnagel/Pfitzmann/Garstka, Modernisierung, S. 34.

Eine Umsetzung der Modernisierungsvorschläge der Gutacher ist in der 14. und 15. Legislaturperiode entgegen einiger Ankündigungen[300] nicht erfolgt. Spätere Überlegungen, die Komplexität des gesamten Reformvorhabens durch ein gestuftes Vorgehen zu reduzieren[301], sind nicht aufgegriffen worden.

## 8.2 Rechtsgrundlagen des Datenschutzes

Eine Defizitanalyse des geltenden Datenschutzrechts setzt zunächst eine Analyse der für den Verbraucher relevanten Anwendungsfelder und der sich für seine informationelle Selbstbestimmung sowie seine wirtschaftliche Betätigungsfreiheit ergebenden Risiken voraus. Grob lassen sich zunächst zwei Fallgruppen der Datenverarbeitung unterscheiden: Die erste Fallgruppe ist die gegenüber dem Betroffenen offene Datenverarbeitung, die ihren Ausgangspunkt in dem Vertrag zwischen Unternehmer und Verbraucher und damit in einer unmittelbaren Kommunikation der vertragsschließenden Parteien findet. In der zweiten Fallgruppe sind die Verarbeitungen zusammengefasst, in denen personenbezogene Daten ohne Mitwirkung des Betroffenen erhoben, verarbeitet oder genutzt werden.

### 8.2.1 Datenverarbeitung unter Mitwirkung des Betroffenen

Die Grundkonstellation im Verbraucherdatenschutz beginnt mit dem Vertragsschluss zwischen dem Unternehmer und dem Verbraucher. In einem Prozessmodell lässt sich die Kommunikation über die zwischen dem Unternehmer und dem Verbraucher konsentierte Datenverarbeitung wie folgt abbilden:

- Die Zwecke der Datenverarbeitung werden von dem Unternehmer vor der Erhebung „konkret“ festgelegt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG).
- Der betroffene Verbraucher wird von dem Unternehmer bei der Erhebung seiner Daten über seine Identität, den Zweck der Datenverarbeitung sowie Kategorien der Empfänger unterrichtet (§ 4 Abs. 3 BDSG).
  Diese Informationen korrespondieren mit den Angaben im Verfahrensverzeichnis über die Zweckbestimmung (§ 4 e Satz 1 Nr. 4 BDSG) sowie die betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien (§ 4 e Satz 1 Nr. 5 BDSG) sowie der Empfänger oder Kategorien von Empfängern, denen Daten mitgeteilt werden können (§ 4 e Satz 1 Nr. 6 BDSG).
- Der Unternehmer erhebt nur die zur Vertragserfüllung erforderlichen Daten (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Für weitergehende Daten bedarf es einer informierten und freiwilligen Einwilligung des Verbrauchers (§ 4 a Abs. 1 BDSG).

---

[300] Entschließung der Koalitionsfraktionen SPD und Bündnis90/Die GRÜNEN, BT-Drs. 14/9709. Koalitionsvertrag 2002 bis 2006, S. 67: „Wir werden das Datenschutzrecht auf der Grundlage der Vorarbeiten der 14. Legislatur umfassend reformieren. Der Schutz der Daten der Arbeitnehmerinnen und Arbeitnehmer wird erstmals in einem eigenen Gesetz verankert.“

[301] Bizer, DuD 2005, 6 ff.; Tauss/Kollbeck/Fazlic in: FG Bäumler, S. 41 ff.

- Eine Bonitätsabfrage zur Absicherung einer kreditwährenden Leistung ist durch den Verbrauchervertrag gedeckt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Der betroffene Verbraucher ist hierüber aber zu informieren, damit er die Möglichkeit hat, gegebenenfalls auf die kreditorische Leistung zu verzichten (§ 4 Abs. 3 BDSG).[302]
- Der Unternehmer verarbeitet die zur Vertragserfüllung erforderlichen Daten (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG).
- Sollen die Daten des Verbrauchers für eigene Zwecke der Werbung, Markt- oder Meinungsforschung verwendet werden, so unterrichtet er ihn bei der Erhebung über diesen Zweck (§ 4 Abs. 3 Satz 1 Nr. 2 BDSG) sowie über sein Widerspruchsrecht nach § 28 Abs. 4 BDSG. Widerspricht der Betroffene hat diese Verwendung zu unterbleiben.
- Will der Unternehmer die Daten des Verbrauchers über den konkreten Vertrag hinaus zu einem Kundenprofil zusammenfassen, so bedarf er hierzu der Einwilligung des Verbrauchers (§ 4 a Abs. 1 BDSG).
- Sollen die Daten des Verbrauchers an Dritte für Zwecke der Werbung, Markt- oder Meinungsforschung übermittelt werden, so ist dies nur in den engen Grenzen des Listenprivilegs zulässig (§ 28 Abs. 1 Satz 1 Nr. 3 BDSG) – ansonsten bedarf es seiner Einwilligung (§ 4 a Abs. 1 BDSG). Über den Verwendungszweck der Datenliste und die Kategorien der Empfänger (§ 4 Abs. 3 Satz 1 BDSG) sowie über das Widerspruchsrecht nach § 28 Abs. 4 BDSG ist der betroffene Verbraucher zu unterrichten.
- Eine Übermittlung der Vertragsdaten des Verbrauchers an eine Auskunftei ist nur zulässig, wenn es sich um so genannte „harte“ Negativdaten handelt, die unter staatlicher Mitwirkung entstanden sein müssen (§ 28 Abs. 1 Satz 1 Nr. 2 bzw. § 28 Abs. 3 Satz 1 Nr. 1 BDSG). In Einzelfällen kann auch die Übermittlung von weichen Negativdaten an eine Auskunftei zulässig sein, wenn das schutzwürdige Interesse der Betroffenen das berechtigte Interesse des Kredit gewährenden Unternehmens nicht übersteigt.
- Die Daten des Verbrauchers werden nach der im Verfahrensverzeichnis festgelegten Regelfrist gelöscht (§ 4 e Satz 1 Nr. 7 BDSG), soweit sie nicht mehr für das Vertragsverhältnis benötigt werden. Rechnungen und Buchungsbelege werden mit Rücksicht auf die steuer- bzw. handelsrechtlichen Aufbewahrungspflichten nicht gelöscht, sondern gesperrt (§ 35 Abs. 3 Nr. 1 BDSG).

In diesem Gutachten soll die Datenverarbeitung im Rahmen eines Verbrauchervertrages nur typisiert betrachtet werden, denn eine detaillierte Risiko- und Defizitanalyse würde erfordern, dass unterschiedliche Vertragsarten auf ihre konkreten Verarbeitungsbedingungen nach den Beteiligten, der Art der Daten sowie der Verwendungszwecke betrachtet werden. So macht es einen Unterschied, ob Daten des Verbrauchers für eine Finanzdienstleistung erhoben und verwendet werden, wobei innerhalb dieser Dienstleistung zwischen den Zwecken des Geldverkehrs, des Sparens, des Kredits sowie der Versicherung zu unterscheiden ist. Anders stellen sich über Reisedienstleistung geschlossene Verbraucherverträge dar, die in der Re-

[302] Siehe auch Duhr in Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 26.

gel von unterschiedlichen Beteiligten vom Reisebüro, der Fluglinie sowie der Hoteldienstleistung erbracht werden. Ein ganz anderer Typ ist wiederum der Behandlungsvertrag, den der Arzt oder das Krankenhaus mit dem Patienten schließt, für dessen Datenverarbeitung insbesondere die ärztliche Schweigepflicht zu beachten ist.

Legt man jedoch die oben durchgeführte Typisierung zu Grunde, dann lassen sich folgende wiederkehrende Mängel identifizieren:

- Die betroffenen Verbraucher werden nicht, nicht vollständig und teilweise unzutreffend über die Verwendungszwecke sowie die Empfänger bzw. Kategorien der Empfänger unterrichtet.
- Die verantwortliche Stelle erhebt bei dem Verbraucher Daten, die für den konkreten und ihm gegenüber kommunizierten Zweck nicht erforderlich sind.
- Die verantwortliche Stelle überschreitet entgegen ihrer Unterrichtung des betroffenen Verbrauchers die Zweckbindung seiner Daten, indem sie bspw. über ein Customer Relation Management bzw. Data Mining-System ein Kundenprofil über einen längeren Zeitraum bildet und/oder die Daten für Zwecke der Werbung oder Marktforschung verwendet.
- Die verantwortliche Stelle stützt ihre Einwilligung auf eine nur formularmäßige Einwilligung in den Allgemeinen Geschäftsbedingungen, die nicht den gesetzlichen Anforderungen genügt.
- Der betroffene Verbraucher wird nicht über sein Widerspruchsrecht gegen eine Verwendung seiner Daten zu Zwecken der Werbung, Markt- und Meinungsforschung informiert.
- Die verantwortliche Stelle übermittelt für Zwecke der Kreditprüfung unzulässige Informationen an eine Auskunftei.
- Die verantwortliche Stelle unterlässt es, ihre innerbetriebliche Organisation so zu gestalten, dass die Verwendung von Verbraucherdaten überprüft werden kann.[303]
- Die verantwortliche Stelle löscht bzw. sperrt die Daten des Betroffenen nicht, obwohl der mit dem betroffenen Verbraucher erreichte Zweck der Verarbeitung bereits erreicht ist.

Die beschriebenen Defizite beruhen nicht auf Schutzlücken des geltenden Datenschutzrechts, sondern auf der fehlenden Einhaltung des geltenden Datenschutzrechts sowie Mängeln im internen Datenschutzmanagement der Unternehmen (s.u. S. 150).

### 8.2.2 Datenverarbeitung ohne Mitwirkung des Betroffenen

Unter Gesichtspunkten des Verbraucherdatenschutzes kritisch sind die Verarbeitungen, in die der Betroffene nicht unmittelbar einbezogen ist, d.h. in denen die Verbraucherdaten entgegen dem datenschutzrechtlichen Grundsatz der Direkterhebung nach § 4 Abs. 1 BDSG nicht beim Betroffenen erhoben werden, so dass er über die Verwendungszwecke auch nicht informiert werden kann. Hierzu gehören insbesondere:

[303] Vgl. Anlage zu § 9 Satz 1 BDSG.

- Datensammlungen in Auskunfteien, die sich einerseits aus Einmeldungen von Unternehmen, andererseits aus unterschiedlichen allgemein zugänglichen Quellen wie Telefon- und Adressbüchern, öffentlichen Registern sowie aus dem Internet speisen. Hierbei werden häufig personenbezogene Daten mit statistischen Auswertungen von bspw. soziodemographischen Informationen über den Wohnort oder Informationen über den Wohngebäudetyp verschnitten.
- Datensammlungen des Adresshandels, die ebenso wie bei Auskunfteien mit allgemein zugänglichen Informationen und statistischem Material zusammengeführt und an Dritte für Werbezwecke verkauft werden.
- Scoringsysteme, die personenbezogene Daten eines Kunden bzw. Interessenten mit weiteren Informationen aus allgemein-zugänglichen Quellen und mit soziodemographischem Material zusammenführen, um die Kreditwürdigkeit des betroffenen Verbrauchers anhand von statistisch erlangten Bewertungen solcher Informationen zu prognostizieren.[304]

Das Datenschutzrisiko dieser Verfahren besteht für den Betroffenen darin, dass eine solche Datenverarbeitung für ihn nicht transparent ist, obwohl die über ihn zusammengestellten Informationen für ihn individuell von großer Bedeutung sind und gegebenenfalls höchstsensible Bereiche der privaten Lebensführung betreffen. So werden die Datensammlungen der Auskunfteien bspw. im Rahmen einer Bonitätsprüfung, d.h. zur Beurteilung seiner wirtschaftlichen Leistungskraft verwendet. Zudem können durch die Zusammenführung von verschiedenen Einzeldaten – auch aus allgemein zugänglichen Quellen – neue Informationen entstehen bzw. Erkenntnisse gewonnen werden, die über den Informationsgehalt der Einzeldaten weit hinaus gehen und für den Betroffenen intransparent sind.

Nach § 33 Abs. 1 Satz 2 BDSG ist der betroffene Verbraucher bei der geschäftsmäßigen Speicherung zum Zwecke der Übermittlung nicht bereits von der Speicherung seiner Daten, sondern erst „von der erstmaligen Übermittlung“ zu benachrichtigen und bei dieser Gelegenheit auch von „der Art der übermittelten Daten“ sowie nach Satz 3 der Vorschrift auch über die Kategorien der Empfänger in Kenntnis zu setzen, soweit er nach den Umständen des Einzelfalles nicht mit einer Übermittlung an diese rechnen muss. Dass der Betroffene nicht schon zum Zeitpunkt der Speicherung unterrichtet wird, ist ein klarer Wertungswiderspruch zu den für eine Verarbeitung für eigene Geschäftszwecke geltenden Informationspflichten nach § 4 Abs. 3 Satz 1 BDSG. Angesichts des erhöhten Gefährdungspotenzials bei der Verarbeitung für fremde Geschäftszwecke, bei der die verantwortliche Stelle noch nicht einmal ein Vertragsverhältnis mit dem Betroffenen unterhält, ist dieser nicht gerechtfertigt.[305]

Rechtsgrundlage für das Erheben, Speichern und Verändern für fremde Geschäftszwecke ist § 29 Abs. 1 BDSG. Die Vorschrift regelt die Voraussetzungen einer Datenverarbeitung für Zwecke der Übermittlung, insbesondere „wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient“. Dies ist zulässig,

[304] Hierzu näher ULD, Scoringsysteme 2005.

[305] Mallmann in: Simitis, BDSG, § 33, Rn. 22, Gola/Schomerus, BDSG, § 33, Rn. 15.

wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können (§ 29 Abs. 1 Satz 1 Nr. 2 BDSG) oder kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat (§ 29 Abs. 1 Satz 1 Nr. 2 BDSG). Nicht ohne Risiko für den Betroffenen ist, dass die nach dem Gesetz erforderliche Abwägung im Einzelfall in den Händen der verantwortlichen Stelle liegt, die ihrerseits ein wirtschaftliches Interesse an der Übermittlung von Verbraucherdaten hat. Faktoren für diese Abwägung sind insbesondere folgende:

- Die Daten der betroffenen Verbraucher müssen aktuell und vollständig sein. Nach § 35 Abs. 2 Satz 2 Nr. 4 BDSG ist in jedem Fall eine Löschungsfrist von vier Jahren zu beachten, wenn eine Prüfung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist. Ergibt sich bereits früher, dass die Daten unrichtig sind, so verletzt ihre weitere Speicherung schutzwürdige Belange des Betroffenen und ist rechtswidrig.[306]
- Wertungen, Schätzungen und Prognosen begründen Zweifel an der Zulässigkeit der Speicherung, wenn sie mangels Tatsachenbasis überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigen.[307]
- Gespeichert werden dürfen im Regelfall harte Negativdaten, wenn nicht im Einzelfall schutzwürdige Belange der Betroffenen überwiegen. Weiche Negativmerkmale, insbesondere soweit sie auf einseitigen Maßnahmen des Gläubigers (wie etwa außergerichtliche Mahnungen) beruhen, dürfen im Einzelfall nur unter engen Voraussetzungen gespeichert werden.[308]
- Das Zusammenführen von Informationen über den Verbraucher aus unterschiedlichen Quellen kann als Verändern i.S.d. § 3 Abs. 4 S. 2 Nr. 2 BDSG gegen schutzwürdige Belange verstoßen, wenn durch die Verknüpfung der Daten völlig neue Informationen entstehen.[309]
- Werden aufgrund der eingespeicherten Daten „Werte“ über den Verbraucher ermittelt, die Auskunft über seine Bonität oder Kreditwürdigkeit geben, so ist der Betroffene über diese zu unterrichten, andernfalls überwiegt das schutzwürdige Interesse der betroffenen Verbraucher.[310]

In diesem wirtschaftlichen Interesse liegt ein entscheidender Unterschied zwischen einer Verarbeitung für eigene geschäftliche Zwecke einerseits (§ 28 BDSG) und der für Zwecke der Übermittlung andererseits (§ 29 BDSG). Im Fall einer Verarbeitung für eigene Zwecke hat die verantwortliche Stelle in der Regel nur ein geringes Interesse, die Daten ihrer Kunden Dritten zur Verfügung zu stellen, weil sie damit nur die Bindung ihrer Kunden an das Unternehmen gefährden und die Konkurrenz stärken würde. Im Unterschied dazu besteht das

---

[306] Vgl. Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 43.

[307] Vgl. Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 44.

[308] Näher Mallmann-Simitis, BDSG, § 29, Rn. 57; Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 33 f.

[309] Vgl. Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 51.

[310] Vgl. Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 46, 49; ULD, Scoringverfahren, S. 93.

Interesse im Fall einer Verarbeitung für Zwecke der Übermittlung gerade in der Generierung von Daten, die an Dritte mit wirtschaftlichem Gewinn verkauft werden sollen. Aus diesem Grund bedarf die Datenübermittlung nach § 29 Abs. 2 BDSG besonderer Sicherungen:

- Die Empfänger der Daten müssen ein berechtigtes Interesse an der Kenntnis der Daten des Betroffenen „glaubhaft machen" (§ 29 Abs. 2 Satz 1 Nr. 1 BDSG). Ein berechtigtes Interesse besteht jedoch nur, wenn die Kenntnis der Daten für den vom Empfänger beabsichtigten Zweck auch erforderlich ist.[311] Die Anfrage muss sich also nach der Person, nach der sich der Empfänger erkundigt, sowie nach dem Umfang der Daten auf eine konkrete Kreditanfrage des Betroffenen beziehen.[312]
- Um falsche Auskünfte aufgrund einer Verwechslung von Namen auszuschließen, dürfen Daten über einen betroffenen Verbraucher nicht übermittelt werden, wenn er nicht zuverlässig authentifiziert worden ist.[313]
- Bei einer Übermittlung sind nach § 29 Abs. 1 Satz 2 BDSG die Gründe „für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung" von der übermittelnden Stelle zu protokollieren. Im Fall eines automatisierten Abrufes ist hierzu nach Satz 3 der Vorschrift der Empfänger der Daten verpflichtet. Darüber hinaus gelten die Regelungen über die Ziehung von Stichproben für das automatisierte Abrufverfahren nach § 10 Abs. 4 Satz 3 BDSG.[314]

Defizitär ist, dass die für die Übermittlung verantwortliche Stelle den betroffenen Verbraucher nicht bereits bei der ersten Speicherung über diesen Umstand im Umfang der nach § 4 Abs. 3 BDSG geltenden Informationspflichten unterrichten muss.

Defizitär ist auch die Einschränkung des Auskunftsanspruches des Betroffenen über Herkunft und Empfänger der an die verantwortliche Stelle gemeldeten Daten. Nach § 34 Abs. 1 Satz 3 BDSG ist keine Auskunft in den Fällen zu erteilen, in denen das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt (s.o. S. 55 f.).[315] Die Reduktion des Anspruches auf die Fälle, in denen der Betroffene die Unrichtigkeit seiner Daten begründet darlegt, verlagert die Beweislast für die Verpflichtung zur Auskunft unangemessen auf den Betroffenen. Der Auskunftsanspruch soll den Eingriff in das informationelle Selbstbestimmungsrecht kompensieren. Er wird durch eine Berufung auf Geschäftsgeheimnisse entwertet, zumal der Betroffene hier wiederum der einseitigen Entscheidungsmacht der verantwortlichen Stelle ausgeliefert ist, ohne geeignete Mechanismen zu erhalten, die Rechtmäßigkeit der Verweigerung mit Hinweis auf ein Geschäftsgeheimnis zu kontrollieren bzw. nachzuvollziehen.

---

311 BGHZ 91, 233, 240; Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 52.

312 Mallmann in: Simitis, BDSG, § 29, Rn. 110; Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 53.

313 Vgl. Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 63.

314 Näher Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 70 f.

315 Näher Duhr in: Roßnagel, HdBDatSchR, Kap. 7.5, Rn. 82.

### 8.2.3 Heimliche Datenerhebungen

Bereits die „Modernisierungs-Gutachter“ haben die fehlende Technikadäquanz des Datenschutzrechts kritisiert. Für einen zukunftsgerichteten Verbraucherdatenschutz werden insbesondere die von dem Betroffenen unbemerkten Datenerhebungen, die ihn in seinem Verhalten kontrollieren und steuern sollen, an erheblicher Bedeutung gewinnen. In diesem Zusammenhang werden Anwendungen – angefangen beim massenhaften Einsatz von RFID in Produkten bis hin zu Sensoren und Lesegeräten zur Steuerung von ganzen Räumen und Umgebungen – zentrale Bedeutung erlangen. In Verbindung mit Kunden- und Zahlungskarten werden nicht nur Kundenprofile kontaktlos und funkgesteuert erfasst, sondern raum- und flächenbezogene Bewegungs- und Verhaltensprofile erstellt.

Ob Sensoren RFID-Tags auslesen, Lesegeräte biometrische Merkmale, Videokameras optische Bilder erfassen, Filter im Internet elektronische Identitätszertifikate abfangen und auswerten oder über das Handynetz Standortdaten erfasst werden – die Informationsdichte über die Menschen in dieser Welt des ubiquitären Computing wird miteinander vernetzt. Steuerungs- und Manipulationspotenzial wird ungeahnte Ausmaße annehmen und damit eine neue Qualität erreichen.[316] Die Objekte werden über ihre Träger „sprechen“ und ihre Informationen miteinander in mächtigen Hintergrundsystemen verknüpfen. In den Szenarien des ubiquitären Computing werden die Objektinformationen ihren jeweiligen Trägern zugeordnet, in vernetzten Hintergrundsystemen verwaltet, ausgewertet und optimiert. Die Ergebnisse dienen dazu, die technischen Umgebungen an die vermeintlichen oder tatsächlichen „Bedürfnisse“ der Individuen anzupassen.

Das geltende Datenschutzrecht und die Datenschutzpolitik sind auf diese Herausforderungen einer allgegenwärtigen vernetzten Totalerfassung nicht eingestellt. Das Modernisierungsgutachten aus dem Jahr 2001 hat zu dieser Entwicklung Perspektiven und Handlungsmöglichkeiten aufgezeigt, ohne dass Politik und Gesetzgebung auch nur ansatzweise reagiert hätten. Sie erfordern nicht nur einen korrigierten Rechtsrahmen, sondern vor allem auch eine gezielte Entwicklung von datenschutzfreundlichen Techniken.

## 8.3 Vollzug und Kontrolle

### 8.3.1 Vollzugsdefizit

Komplizierte Regelungen erschweren die Normanwendung durch die zur Befolgung verpflichteten Stellen. Abgesehen von den genannten Herausforderungen der zukünftigen technischen Entwicklung sind die vorhandenen Datenschutznormen auf die gegenwärtigen Herausforderungen des Verbraucherdatenschutzes bis auf wenige Ausnahmen weitgehend ein-

[316] Siehe demnächst ausführlich ULD/Humboldt-Universität Berlin, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS), Studie im Auftrag des BMBF, April 2006.

gestellt. Mit den Kenntnissen der datenschutzrechtlichen Regelungen und Kasuistik können die Experten der Aufsichtsbehörden sowie der Unternehmen die gegenwärtigen Datenschutzfragen angemessen subsumieren und einer Klärung zuführen. Die Normanwendung stößt jedoch an ihre Grenzen, wenn das Datenschutzrecht in der Fläche von der Vielzahl kleinerer und mittlerer Unternehmen angewendet werden soll.[317]

Die §§ 28 und 29 BDSG stellen in ihrer Komplexität ein Dickicht an Abwägungsklauseln, Ausnahmen und Rückausnahmen dar. Nicht weniger komplex sind die zahlreichen Ausnahmen zur Benachrichtigung in § 33 Abs. 2 BDSG, die nach § 34 Abs. 4 BDSG auch für den Auskunftsanspruch gelten. Was für den Unternehmer als verantwortliche Stelle gilt, muss erst recht für den Verbraucher Geltung beanspruchen: Komplizierte Rechtsregeln behindern nicht nur den Normvollzug, sie blockieren letztlich auch die Betroffenen, die Voraussetzungen einer zulässigen Datenverarbeitung zu erkennen und ihre Rechte effektiv wahrzunehmen.

### 8.3.2 Sanktionen

Ein Grundproblem des geltenden Datenschutzrechts sind die unzureichenden Sanktionsmöglichkeiten von Normverstößen. Auf die Befugnisse der Aufsichtsbehörden nach § 38 BDSG wird in einem späteren Abschnitt noch näher eingegangen (s.u. S. 153). Eine kursorische Prüfung, ob die oben skizzierten Mängel bei der Befolgung des Verbraucherdatenschutzes (s.o. S. 144 ff.) als Ordnungswidrigkeit gilt und mit einem Bußgeld sanktioniert wird, ergibt ein ernüchterndes Ergebnis. Konkrete Bußgeldbewehrungen, die allein einen präventiven Charakter entfalten könnten, sind rar. Bußgeldbewehrt ist lediglich, wenn der Betroffene nicht über sein Widerspruchsrecht nach § 28 Abs. 4 BDSG unterrichtet wurde (§ 43 Abs. 1 Nr. 3 BDSG).

Nicht als gesonderte Tatbestände der Ordnungswidrigkeiten sind in § 43 BDSG erfasst:

- Eine unterlassene, nicht vollständige oder unzutreffende Unterrichtung der Betroffenen.
- Ein Verstoß gegen die dem Betroffenen mitgeteilte Zweckbindung der Daten, bspw. indem die Daten für Zwecke der Werbung und Marktforschung verwendet werden.
- Die Bildung von umfassenden Kundenprofilen.
- Die Übermittlung von Verbraucherdaten an eine Auskunftei.
- Die unterlassene Löschung oder Sperrung von Verbraucherdaten, obwohl ihr Zweck erreicht worden ist.
- Die Missachtung der Auskunftspflicht gegenüber dem Betroffenen.

[317] Dies gilt nicht nur für den Verbraucherdatenschutz, sondern insbesondere auch für den Bereich des Arbeitnehmerdatenschutzes, der in dieser Studie keine Berücksichtigung findet.

Als Auffangtatbestand kann in vielen Fällen[318] § 43 Abs. 2 Nr. 1 BDSG zur Anwendung kommen, wonach eine unbefugte Datenverarbeitung als Ordnungswidrigkeit sanktioniert wird. Allerdings wird dieser Tatbestand von den Aufsichtsbehörden mit Rücksicht auf den Bestimmtheitsgrundsatzes nach Art. 103 Abs. 2 GG und die zahlreichen Abwägungsklauseln im materiellen Datenschutzrecht nur sehr zurückhaltend angewendet.[319]

Die Sanktionierung einer verweigerten oder unrichtigen Auskunftserteilung als Sicherung des zentralen Instruments der informationellen Selbstbestimmung fehlt im Bußgeldkatalog des § 43 BDSG gänzlich.

[318] Siehe zu Einzelfällen wie bspw. einer unterlassenen Löschung, Ehmann in: Simitis, BDSG, § 43 Rn. 52 ff.

[319] Ehmann in: Simitis, BDSG, § 43, Rn. 22; Petri in: FG Bäumler, S. 231 f.

# 9 Beseitigung der Defizite im Verbraucherdatenschutz

Die beschriebenen Defizite lassen sich durch Maßnahmen auf drei Ebenen beseitigen: Zum einen durch eine Schärfung der materiellen Anforderungen an den Datenschutz, zum zweiten durch eine Verbesserung der Maßnahmen der Aufsicht und Kontrolle und schließlich durch Maßnahmen des proaktiven Datenschutzes.

## 9.1 Materielle Anforderungen

Ein grundlegendes Problem des geltenden Verbraucherdatenschutzrechts ist die Komplexität der gesetzlichen Regelungen. Sie sind durch eine Vielzahl an Abwägungstatbeständen sowie zahlreichen Ausnahmen und Rückausnahmen gekennzeichnet. Eine Neuordnung der materiellen Regelungen sollte sich ungeachtet der Frage der Umsetzungsstrategie[320] auf ein einfaches Regelungsmodell konzentrieren, in dem die zulässigen Zwecke und ihre Voraussetzungen normenklar und verständlich geregelt werden. Dabei ist es sinnvoll, die Darstellung der Regelungen an dem Prozess der Entstehung und der Abwicklung eines Verbrauchervertrages zu orientieren, um ihre Umsetzung zu vereinfachen.

### 9.1.1 Datenverarbeitung mit Mitwirkung des Betroffenen

Den Ausgangspunkt des Verbraucherdatenschutzes sollte die Datenverarbeitung zur unmittelbaren Erfüllung des Verbrauchervertrages sein (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Jede weitere über diesen Verwendungszweck hinausgehende Datenverarbeitung beim Betroffenen sollte grundsätzlich der Mitwirkung des betroffenen Verbrauchers bedürfen. Beispiele für derartige weitere Verwendungszwecke sind die Zwecke der Werbung und Marktforschung und eine umfassende Auswertung der Kundendaten in Form von Verbraucherprofilen. Zum einen wird durch die Einbeziehung des betroffenen Verbrauchers seine informationelle Selbstbestimmung gestärkt, zum anderen bekommt das Unternehmen auf diese Weise Gelegenheit, seine legitimen Interessen gegenüber seinem Vertragspartner zu begründen und zu rechtfertigen. Die Verwendung der Daten des Verbrauchers zu anderen als den über den Vertrag konsentierten Zwecken ist als eine Chance zur Kommunikation mit ihm zu verstehen und zu gestalten.[321]

Legitime Auswertungsinteressen der Unternehmer sollten in Anlehnung an die Regelung im Teledienstdatenschutz unter Pseudonym ausdrücklich zugelassen werden. Jedoch ist durch eine allgemeine Rechtsregel sicherzustellen, dass die Zuordnungstabelle aus Pseudonym und Klarnamen einer besonderen und strikten Zweckbindung unterliegt, um eine Auswertung der Verbraucherdaten unter Identifizierung des Verbrauchers zu verhindern. Die Zuord-

[320] Hierzu Bizer, DuD 2004, 6 ff.

[321] Vgl. Roßnagel/Pfitzmann/Garstka, Modernisierung, S. 72.

nungstabelle ist technisch-organisatorisch abzusichern. Besondere Bedeutung hat ein revisionssicherer, d.h. nachprüfbarer Schutz dieser Zuordnungstabelle.

Die Erforderlichkeit der Datenverarbeitung ist durch klare Regeln der Löschung bzw. der Sperrung personenbezogener Daten zu stärken. Für Vertragsdaten ist eine Regelsperrung bzw. -löschung festzulegen; dabei ist mit Rücksicht auf die gesetzlichen Aufbewahrungsfristen zwischen den Prozessdaten, beginnend mit dem Bestellvorgang über die Lieferung bis zur Bezahlung einerseits und den steuerlich relevanten Rechnungs- und Buchungsdaten andererseits zu unterscheiden.

Die Übermittlung von Verbraucherdaten an Dritte bspw. für Bonitätsanfragen sollte ausschließlich nur mit Einwilligung des Betroffenen zulässig sein. Denn mit der Übermittlung an Dritte entfernen sich die Daten des Verbrauchers aus seinem Horizont, ohne dass er seine Rechte geltend machen kann. In diesem Fall müssen die Daten des Betroffenen einer strikten Zweckbindung unterliegen, ohne eine Aufweichung der Zweckbindung, wie sie derzeit in § 28 Abs. 5 Satz 2 BDSG bei der Datenverarbeitung auf gesetzlicher Grundlage vorgesehen ist.

Materiell sind vor allem die Rechte der Betroffenen zu vereinfachen und zu stärken. Die Informationen des Verbrauchers sollten vollständig, verständlich und transparent sein (s.u. S. 179). Grundsätzlich sollten dem Verbraucher alle seine Daten, die auch dem Unternehmer zur Verfügung stehen, zumindest lesend zugänglich sein. Die Entwicklung im E-Commerce zeigt, dass es längst möglich und teilweise auch Praxis ist, dass jeder Verbraucher sein Datenkonto bei seinem Vertragspartner zumindest lesend einsehen kann. Viele Unternehmen nutzen diese Möglichkeit zur Kundenbindung und um die Daten des Verbrauchers durch ihn selbst aktualisieren zu lassen. Angesichts der geringen Zahl von Auskunftsersuchen sind die zahlreichen Ausnahmetatbestände verzichtbar.

### 9.1.2 Datenverarbeitung ohne Mitwirkung des Betroffenen

Besonderer Aufmerksamkeit bedürfen die Datenschutzregelungen, die eine Verarbeitung für Zwecke der Übermittlung ermöglichen. Sie sind für den Fachmann in der Praxis operationalisierbar, aber für den Verbraucher intransparent und nicht nachvollziehbar. Aus diesem Grund sind die Erlaubnistatbestände für die Tätigkeit des Adresshandelns, der Auskunfteien und des Scorings zu benennen und die gesetzlichen Voraussetzungen aufzuführen, unter denen personenbezogene Daten gespeichert und übermittelt werden dürfen.

Zu streichen sind die zahlreichen Ausnahmetatbestände, mit denen der Gesetzgeber die Transparenzpflichten zu Lasten der Verbraucher abgeschwächt und reduziert hat. Da die Daten in der Regel nicht, zumindest nicht vollständig beim Betroffenen erhoben werden, sind die Transparenzpflichten der gewerblich tätigen Übermittlungsdienstleister gegenüber den betroffenen Verbrauchern zu schärfen, aber nicht wie im gegenwärtigen Rechtszustand zu schwächen. So sollten die Betroffenen bereits mit der Einmeldung ihrer Daten informiert und über ihre rechtlichen Möglichkeiten unterrichtet werden. Gleichzeitig würde eine solche Informationspflicht die Qualität der Daten zum Schutz der Verbraucher, aber auch der Unter-

nehmer verbessern, weil die Betroffenen die Möglichkeit haben unmittelbar auf unzutreffende Daten zu reagieren.

Besonderer Konzepte bedarf die Risikominimierung bei RFID- oder Ubiquitous Computing-Anwendungen. Werden RFID-Tags bspw. während des Einkaufs personenbezogen erfasst, so erfordert dies im Fall einer Authentifizierung des Verbrauchers eine datenschutzrechtliche Einwilligung. Nach der Bezahlung der Waren sind die RFID-Tags automatisch zu löschen, damit sie nicht von den Lesegeräten Dritter erfasst und der Person zugeordnet werden können.[322]

## 9.2 Aufsicht und Kontrolle

Neben einer Vereinfachung und Schärfung des materiellen Datenschutzrechts liegen Defizite des Verbraucherdatenschutzes vor allem im Vollzugsdefizit der Aufsichtsbehörden sowie im innerbetrieblichen Bereich.

### 9.2.1 Aufsichtsbehörden

Auf die Befugnisse und Möglichkeiten der Aufsichtsbehörden wird in Kapitel 10 näher eingegangen (s.u. S. 166 ff.).

### 9.2.2 Betriebliche Datenschutzorganisation

Ein wichtiges Element zur Durchsetzung des Verbraucherdatenschutzes ist die Stärkung der betrieblichen Datenschutzorganisation. Ihre Aufgabe ist es, für die Umsetzung und Einhaltung der Datenschutz- und Datensicherheitsanforderungen im Unternehmen zu sorgen. Die Datenschutzorganisation leistet damit einen Beitrag, die Normbefolgung im Unternehmen – im Managementjargon als Compliance bezeichnet – durchzusetzen. Die Beseitigung des Vollzugsdefizits im Datenschutzrecht ist damit eine Gestaltungsaufgabe des Datenschutzmanagements.[323] Es gilt „den Datenschutz in die Prozesse des Unternehmens zu bringen“.

#### 9.2.2.1 Aufgabe Compliance und Riskmanagement

Die Datenschutzorganisation hat auch die Aufgabe, Vorsorge vor Schäden zu treffen, die dem Unternehmen durch Verstöße gegen die Regeln des Datenschutzes und der Datensicherheit entstehen können. Solche Schäden können aus der Verletzung der informationellen Selbstbestimmung der Betroffenen entstehen; sie können aber auch in Imageschäden und Vertrauensverlusten liegen, die sich aus einem rechtswidrigen Umgang mit den Daten der Verbraucher ergeben. Solche Schäden können im Übrigen auch bereits daraus entstehen,

[322] Zu weiteren Überlegungen wird auf die Studie der ULD/Humboldt-Universität Berlin, TAUCIS, 2006 verwiesen.

[323] Zum Datenschutzmanagement: Kongehl (Hrsg.), Datenschutzmanagement, Freiburg 2005.

dass die Verbraucher den Umgang mit ihren Daten nicht als „fair“ ansehen. So trauen nach einer repräsentativen Umfrage in Deutschland lediglich 30% der Befragten den Versicherungen einen zuverlässigen Umgang mit ihren Daten zu.[324] Ein geradezu vernichtendes Zeugnis wird nach dieser Untersuchung dem Adresshandel ausgestellt, dem nur 8% einen richtigen Umgang mit ihren Daten zutrauen.[325] Derartige Indikatoren können sich jedoch nicht nur branchenspezifisch, sondern auch für einzelne Unternehmen zu einem ernsthaften Problem auswachsen. Beispiele aus der Vergangenheit sind die Bonusmeilenaffäre aus dem Jahr 2002, die auf einen Datendiebstahl durch einen Mitarbeiter der Fluglinie zurückzuführen war.[326] Nicht überzeugend ist es schließlich, wenn das Unternehmen sich von einem Gericht bescheinigen lassen muss, dass seine Verwendungsregeln – meistens in den Allgemeinen Geschäftsbedingungen – nicht den gesetzlichen Bestimmungen entspricht, sondern gegen wesentliche Grundgedanken des Datenschutzes verstößt.[327] Erfahrungsgemäß ist es einfacher und kostengünstiger, ein einmal bei den Verbrauchern erworbenes Vertrauenskapital zu sichern, als den Verlust an Vertrauen wieder zu kompensieren und den „guten Ruf“ des Unternehmens zu stabilisieren. Die Datenschutzorganisation ist damit auch Teil des Risikomanagements, mit dem die Verantwortlichen im Rahmen ihrer Sorgfaltspflichten als Geschäftsführer oder Vorstände Schäden vorzubeugen haben.

#### 9.2.2.2 Verfahrensverzeichnis

Bausteine der Datenschutzorganisation ist die Klärung von Aufgaben und Verantwortlichkeiten, die Strukturierung der eigenen Datenverarbeitung, die Festlegung der Datenschutzanforderungen, die Sensibilisierung der Mitarbeiter und eine Überprüfung der konkreten Anweisungen.

Verantwortlich für die Einhaltung der Datenschutzanforderungen sind die verantwortliche Stelle bzw. die für sie handelnden Organe wie der Firmeninhaber, die Geschäftsführer oder der Vorstand einer juristischen Person. Verantwortung wird durch die Festlegung und Verteilung von Aufgaben und Zuständigkeiten wahrgenommen, so dass sich die Verantwortung der Organe im Wesentlichen auf die Organisation des Unternehmens sowie die zentralen Entscheidungen konzentriert. In diesem Sinne werden in Unternehmen Verantwortlichkeiten typischerweise für die Verwaltung und Sicherheit der Informationstechnik sowie für den Umgang mit Kunden- bzw. Verbraucherdaten festgelegt, die damit jeweils auch die geltenden Regeln des Datenschutzrechts zu beachten haben. Aufgabe des betrieblichen Datenschutzbeauftragten ist es insbesondere, auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hinzuwirken (§ 4 g Abs. 1 Satz 1 BDSG). Hierzu gehört, die „ord-

---

[324] Opaschowksi in: HdBDatSchR, Kap. 2.1, Rn. 50 f.

[325] Opaschowksi in: HdBDatSchR, Kap. 2.1, Rn. 52.

[326] http://www.wdr.de/themen/wahl2002/aktuell/bonusmeilen/lufthansa.jhtml.

[327] Beispiel aus der Vergangenheit LG München vom 01.02.2001, DuD 2001, 292, 294 (Payback) oder LG München I, Urteil vom 09.03.2006, Az.: 12 O 12679/05 (nicht rechtskräftig) – noch nicht veröffentlicht.

nungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden“ (§ 4 g Abs. 1 Satz 3 Nr. 1 BDSG).

In welchen automatisierten Verfahren personenbezogene Daten verarbeitet werden, ergibt sich aus dem Verfahrensverzeichnis mit den Angaben des § 4 e BDSG. Sind bei der verantwortlichen Stelle mehr als fünf Arbeitnehmer mit der Erhebung, Verarbeitung oder Übermittlung personenbezogener Daten beschäftigt, so muss ein solches Verzeichnis entweder in einem Register durch die zuständige Aufsichtsbehörde im Wege des Meldeverfahrens nach § 4 f Abs. 1, Abs. 3 BDSG oder durch den betrieblichen Datenschutzbeauftragten der verantwortlichen Stelle selbst geführt werden (§§ 4 e Abs. 2, 4 g Abs. 2 BDSG). Unabhängig von der Zahl der Beschäftigten obliegt den Stellen, die personenbezogene Daten zum Zweck der Übermittlung speichern (Adresshandel, Auskunfteien etc.) eine Meldepflicht nach § 4 d Abs. 4 BDSG.

Aus dem Verfahrensverzeichnis ergeben sich nach § 4 e Satz 1 BDSG neben den Identifikationsdaten über die verantwortlichen Stelle,

- die Zweckbestimmungen der Datenerhebung, -verarbeitung oder nutzung,
- die Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
- die Empfänger oder Kategorien von Empfängern, denen Daten mitgeteilt werden können,
- Regelfristen für die Löschung der Daten,
- eine geplante Datenübermittlung in Drittstaaten (außerhalb der EU) sowie
- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Verarbeitung angemessen sind.

Das Verfahrensverzeichnis ist dem betrieblichen Datenschutzbeauftragten von der verantwortlichen Stelle zur Verfügung zu stellen (§ 4 g Abs. 2 Satz 1 BDSG)[328] und auch fortlaufend zu aktualisieren.[329] Sinn und Zweck ist es, dem betrieblichen Datenschutzbeauftragten einen Überblick über Art und Umfang der Verarbeitung personenbezogener Daten zu liefern, damit er seiner Aufgabe nachkommen kann.[330]

#### 9.2.2.3 Datenschutzkonzept

Von Bedeutung ist, die Verpflichtung des Unternehmens, seine Datenverarbeitung unter den Gesichtspunkten der Datensicherheit konzeptionell zu strukturieren. Die Anlage zu § 9 Satz 1 BDSG spricht ausdrücklich von der Gestaltung der „innerbetrieblichen Organisation“, die den Anforderungen des Datenschutzes gerecht werden müsse. An anderer Stelle erhebt das

[328] Simitis in: Simitis, BDSG, § 4 g, Rn. 63.

[329] Simitis in: Simitis, BDSG, § 4 g, Rn. 61.

[330] Simitis in: Simitis, BDSG, § 4 g, Rn. 60.

BDSG die Grundsätze der Datenvermeidung und Datensparsamkeit zu einem Gestaltungsziel der Datenverarbeitungssysteme (§ 3 a BDSG).

Um diese Anforderungen umzusetzen, bedarf es eines Datenschutzkonzeptes, das zum einen die Einhaltung der Datenschutzrechte gewährleistet, aber auch die Anforderungen der IT-Sicherheit. Hierzu gehören nach den allgemeinen Anforderungen der IT-Sicherheit[331] eine Dokumentation der im Unternehmen betriebenen Informationstechnik (Bestandsaufnahme), eine Analyse der möglichen Gefährdungen für Systeme und Daten (Risikoanalyse), die Festlegung eines Schutzbedarfes, die organisatorischen und technischen Sicherheitsmaßnahmen sowie eine Beschreibung und Bewertung der verbleibenden Restrisiken (Sicherheitskonzept). Bestandteil des Sicherheitskonzeptes ist schließlich auch die Revionsfähigkeit und -festigkeit der vorgesehenen Sicherheitsmaßnahmen, deren Einhaltung und Gewährleistung einer Überprüfung durch Dritte zugänglich sein muss.

Zur Einhaltung und Gewährleistung der Datenschutzrechte könnten z.B. konzeptionell die Bearbeitung von Anfragen mit datenschutzrechtlichem Hintergrund nach Zuständigkeit und Ablauf – auch nach außen transparent – festgelegt werden. Bei der Befragung der betrieblichen Datenschutzbeauftragten wurden bis zu 23 verschiedene Stellen genannt, die in den jeweiligen Unternehmen für die Bearbeitung von datenschutzrechtlichen Anfragen zuständig sind. Schon die Ermittlung der zuständigen Stelle, an die beispielsweise ein Auskunftsanliegen zu richten ist, kann sich danach als ein schwieriges Unterfangen darstellen. Insofern hat eine organisatorisch abgesicherte und transparente Anfragenbearbeitung durchaus Potential, sich als vertrauensbildende Maßnahme nicht nur für den Verbraucher, sondern auch für das Unternehmen im Sinne einer Kundenbindung durch Effektivität auszuzahlen.

Die Grundregeln der IT-Sicherheit, ergänzt um die Elemente des Datenschutzrechtes, sind angesichts ihrer Abhängigkeit und Komplexität heute Stand der Technik.[332] Trotz aller Umsetzungsdefizite vor allem in kleineren und mittleren Unternehmen (KMU) ist die Gestaltung eines Datenschutz- und Datensicherheitskonzeptes aus Gründen von Compliance und Riskmanagement ohne Alternative. Der Verbraucherdatenschutz ist ein „integraler Bestandteil“ dieser Strukturierungsaufgabe.

#### 9.2.2.4 Betrieblicher Datenschutzbeauftragter

Zur Verbesserung des Verbraucherdatenschutzes und zur Beseitigung des Vollzugsdefizits auf Seiten der verantwortlichen Stelle kommt dem betrieblichen Datenschutzbeauftragten eine wichtige Rolle zu. Bereits die Aufgabe der Überwachung und Kontrolle der Datenverarbeitung im Unternehmen (§ 4 g Abs. 1 Satz 3 Nr. 1 BDSG) erfordert es, die Revisionsprozesse des Unternehmens um die Überwachung der Datenverarbeitung zu erweitern, indem die Einhaltung der rechtlichen und sicherheitstechnischen Anforderungen geprüft und kontrolliert werden. Mit der Revision dieser Prozesse wird in der Praxis immer auch die Frage

[331] Ernestus in Roßnagel, HdBDatSchR, Kap. 3.2, Rn. 22 ff.

[332] Ernestus in Roßnagel, HdBDatSchR, Kap. 3.2, Rn. 22 ff.

aufgeworfen, auf welche Weise die bemängelten Zustände behoben, Abläufe verbessert und damit die Anforderungen des Verbraucherdatenschutzes erfüllt werden.

Die Aufgabe des betrieblichen Datenschutzbeauftragten beschränkt sich damit nicht nur auf diese reaktive Kontrolle, sondern sie enthält damit gleichzeitig auch proaktive Elemente der Beratung.[333] So wird die Aufgabe des betrieblichen Datenschutzbeauftragten in § 4 g Abs. 1 Satz 1 BDSG mit der Formulierung beschrieben, er „wirke auf die Einhaltung" der Datenschutzvorschriften „hin". Diese Rolle beschränkt sich nicht darauf, bei den Mitarbeitern im Sinne von § 4 g Abs. 1 Satz 3 Nr. 2 BDSG für die notwendigen Kenntnisse im Datenschutz zu sorgen, sondern „Hinwirken" impliziert auch eine aktive Begleitung der Gestaltung der für den Datenschutz relevanten Datenverarbeitung von ihrer Entwicklung über ihre Implementierung bis zum Produktivbetrieb.

Dass ein solches proaktives Rollenverständnis im gesetzlichen Leitbild des betrieblichen Datenschutzbeauftragten angelegt ist, ergibt sich nicht nur der Aufgabenbeschreibung der Mitwirkung, sondern auch daraus, dass der Gesetzgeber in § 4 d Abs. 5 f. BDSG die Aufgabe der Vorabkontrolle übertragen hat. Hierzu hat der betriebliche Datenschutzbeauftragte automatisierte Verarbeitungen, soweit sie „besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen", vor Beginn der Verarbeitung zu kontrollieren. Als Regelbeispiel nennt der Gesetzgeber zum einen die Verarbeitung besonderer Datenarten (§ 3 Abs. 9 BDSG), zum anderen, dass die Verarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeit, seiner Leistung oder seines Verhaltens (§ 4 d Abs. 5 Nr. 2 BDSG). Eine Vorabkontrolle ist allerdings nicht verpflichtend, wenn die Verarbeitung der Zweckbestimmung eines Vertragsverhältnisses und damit auch eines Verbrauchervertrages dient. Bei den im Gesetz genannten Fällen handelt es sich jedoch nur um Regelbeispiele. Eine Vorabkontrolle ist darüber hinaus auch in den Fällen angebracht, in denen die Daten der Verbraucher jenseits der unmittelbaren Vertragserfüllung bspw. zur Bildung und Auswertung von Kundenprofilen verwendet werden sollen.[334]

Auch jenseits dieser Vorabkontrolle kann und sollte die Rolle des betrieblichen Datenschutzbeauftragten in den Unternehmen zu Gunsten des Verbraucherdatenschutzes deutlich gestärkt werden, damit er zu Gunsten der Verbraucher die Gestaltung der technischen Systeme und die Prozesse der Verarbeitung mitgestalten kann. Hierbei wird es weniger auf ein „stop or go" ankommen, sondern vielmehr auf die Kompetenz, die erforderlichen Anstöße zu liefern, damit Systeme und Prozesse datenschutzgerecht gestaltet werden können. Das Gestaltungsprinzip der Datenvermeidung und Datensparsamkeit in § 3 a BDSG liefert hierzu eindeutige Vorgaben: So ist nach dieser Regelung insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem Schutzzweck steht. Tatsache ist bereits heute, dass unter den Bedingungen der zunehmenden Verlagerung und Verteilung automatisierter Verarbeitungsprozessen an Dritte Verfahren der Anonymisierung und Pseudonymisierung von Verbraucherdaten nicht nur aus Datenschutzgründen, sondern auch zum

---

[333] Königshofen, Erwartungen in; Bäumler, Der neue Datenschutz, S: 235.

[334] Zu den möglichen Kriterien vgl. Walz in: Simitis, BDSG, § 4 d, Rn. 27.

Schutz der Unternehmenswerte an Bedeutung gewinnen. Der betriebliche Datenschutzbeauftragte kann in diesem Prozess eine wichtige Aufgabe sowohl im Interesse der Verbraucher als auch des Unternehmens übernehmen.

In keiner Weise zieladäquat ist der nun dem Bundestag aus dem Bundesrat vorgelegte Vorschlag, das Quorum der mit der Datenverarbeitung befassten Mitarbeiter für die Bestellungspflicht eines betrieblichen Datenschutzbeauftragten heraufzusetzen.[335] Mit diesem Vorschlag wird die Selbstregulierung im Unternehmen geschwächt mit der Folge, dass die Bedeutung der staatlichen Aufsicht steigen müsste. Da dies aber nicht beabsichtigt wird, führt der Vorschlag lediglich zu einer flächendeckenden Verstetigung des Vollzugsdefizits.

Darüber hinaus ist das Kriterium für die Bestellung betrieblicher Datenschutzbeauftragter in keiner Weise risikoadäquat. Ausgangspunkt für die Bestellung eines betrieblichen Datenschutzbeauftragten können nur Art und Umfang der im Unternehmen verarbeiteten personenbezogenen Daten sein, aber nicht die mit der Datenverarbeitung beschäftigten Mitarbeiter. Die Verarbeitung von Verbraucherdaten erfolgt in den Datenverarbeitungsanlagen der Unternehmen praktisch immer „ohne Anwalt“, wenn nicht wenigstens ein betrieblicher Datenschutzbeauftragter für die Rechtskonformität der Datenverarbeitung Sorge trägt.

### 9.2.3 Fachkunde

Eine proaktive Rolle des betrieblichen Datenschutzbeauftragten muss von den Verantwortlichen des Unternehmens gewollt sein. Zwangsläufig setzt eine solche Ausgestaltung im Sinne einer proaktiven Beratung eine entsprechende Qualifizierung des betrieblichen Datenschutzbeauftragten voraus. Nach § 4 f Abs. 2 Satz 1 BDSG ist Voraussetzung seiner Bestellung, dass er die „erforderliche Fachkunde und Zuverlässigkeit“ für die Erfüllung seiner Aufgabe besitzt. In der Praxis zeigt sich, dass Erfolg und Akzeptanz des betrieblichen Datenschutzbeauftragten maßgebend von seiner Fachkunde und seiner betrieblichen Erfahrung im Unternehmen abhängen. Hier liegt es an den Verantwortlichen, das Anforderungsprofil des betrieblichen Datenschutzbeauftragten nicht nur auf das Minimum des gesetzlich erforderlichen Wissens- und Kenntnisstandes zu setzen,[336] sondern als eine konzeptionelle Chance zur Prozessoptimierung nach innen und zur Vertrauensbildung gegenüber den Verbrauchern und Kunden des Unternehmens zu begreifen.

Zumindest nach seiner rechtlichen Stellung ist der betriebliche Datenschutzbeauftragte abgesichert. Er ist unmittelbar dem Leiter der verantwortlichen Stelle zu unterstellen, d.h. des Unternehmens, das die Verbraucherdaten verarbeitet (§ 4 f Abs. 3 Satz 1 BDSG), und er ist in der „Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei“ (§ 4 f Abs. 3 Satz 2 BDSG).

---

[335] BT-Drs. 16/31 vom 03.11.2005. Das Quorum soll von 5 auf 20 Mitarbeiter heraufgesetzt werden.

[336] Fehlt es an der erforderlichen Fachkunde kann die Aufsichtsbehörde einschreiten und die Abberufung des betrieblichen Datenschutzbeauftragten verlangen (§ 38 Abs. 5 Satz 3 BDSG).

Ob er allerdings auch seiner beruflichen Stellung nach abgesichert ist, bleibt fraglich. Zwar normiert § 4 f Abs. 3 Satz 2 BDSG ein so genanntes Benachteiligungsverbot für den betrieblichen Datenschutzbeauftragten. Dieses greift jedoch oft zu kurz:[337] Der betriebliche Datenschutzbeauftragte, der diese Tätigkeit neben seiner eigentlichen Position im Unternehmen ausübt, genießt lediglich einen funktionsbezogenen Kündigungsschutz. Der betriebliche Datenschutzbeauftragte in Vollzeit, der sich bei der Unternehmensführung durch seine Tätigkeit unbeliebt gemacht hat, muss gegebenenfalls nach Ablauf seiner Bestellung um eine Weiterbeschäftigung bangen. Diese Unsicherheiten können sich auf die Art der Aufgabenwahrnehmung durch den betrieblichen Datenschutzbeauftragten auswirken.

Mit welcher Effizienz der betriebliche Datenschutzbeauftragte seine Aufgaben wahrnehmen kann, hängt nicht nur von seiner persönlichen Fachkunde ab, sondern auch von seiner personellen und sachlichen Ausstattung. Das Gesetz fordert, dass die verantwortliche Stelle ihn „bei der Erfüllung seiner Aufgaben zu unterstützen hat“. Hierzu gehören bspw. auch Weisungen, die die Mitarbeiter verpflichten, den betrieblichen Datenschutzbeauftragten zu unterrichten, ihn vor datenschutzrelevanten Entscheidungen rechtzeitig zu beteiligen sowie gegebenenfalls seine Anordnungen zu befolgen, soweit ihm Entscheidungsbefugnisse eingeräumt sind.[338] Sie hat ihm insbesondere Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen, allerdings unter der in der Praxis bedeutsamen Einschränkung nur, „soweit dies für die Erfüllung seiner Aufgaben erforderlich ist“ (§ 4 f Abs. 5 Satz 1 BDSG). Nähere Kriterien liefert das Gesetz nicht. Das bedeutet, dass die für die Aufgabenerfüllung erforderlichen Ressourcen sich an Art und Umfang der Verarbeitung personenbezogener Daten auszurichten hat.[339] Welche Maßstäbe und Kriterien im Einzelnen anzulegen sind, könnte der Gesetzgeber präzisieren. Sie näher zu bestimmen könnte aber auch Aufgabe der verbandlichen Selbstregulierung sein (§ 38 a BDSG).

### 9.2.4 Sanktionen

Eine wichtige Maßnahme zur Effizienzsteigerung des Datenschutzes ist, dass die bei Datenschutzverstößen zu erwartenden Sanktionen eindeutig bestimmt sind. Der Gesetzgeber hat mit der Auswahl der in § 43 Abs. 1 BDSG genannten Tatbestände eine Reihe von in der Praxis bedeutsamen Verstöße ohne eine ausdrückliche Sanktion gelassen, so dass sie lediglich über den Auffangtatbestand der „unbefugten Datenverarbeitung“ nach § 43 Abs. 1 Nr. 1 BDSG sanktioniert werden können. Damit wird jedoch die präventive Funktion der Bestimmung eines Tatbestandes als Ordnungswidrigkeit verkannt. Sinn und Zweck der Bußgeldbewehrung ist weniger, das Bußgeld auch tatsächlich zu verhängen, sondern über die Androhung des Bußgeldes die verantwortlichen Stellen zur Befolgung der datenschutzrechtlichen Bestimmungen anzuhalten. Diese präventive Funktion soll der Bußgeldkatalog aber nicht erst gegenüber einem juristisch qualifizierten Mitarbeiter, sondern vor allem gegenüber

---

[337] Simitis in: Simitis, BDSG, § 4 f. Rn. 131; Berufsverband der Datenschutzbeauftragten Deutschlands (BvD), DuD 2005, 272 ff. m.w.N. aus der arbeitsgerichtlichen Rechtsprechung.

[338] Simitis in: Simitis, BDSG, § 4 f., Rn. 147.

[339] Simitis in: Simitis, BDSG, § 4 f., Rn. 149; Bergmann/Möhrle/Herb, BDSG, § 4 f., Rn. 165.

dem für die Informationstechnik, die Kundenbetreuung und das Marketing verantwortlichen Mitarbeiter haben.

Ein Beispiel für die Unterregulierung des Bußgeldkataloges ist die Verletzung der Transparenzpflichten von der Unterrichtung bei der Datenerhebung nach § 4 Abs. 3 BDSG, der nachträglichen Benachrichtigung nach § 33 BDSG sowie der Auskunft nach § 34 BDSG. Ihre Verletzung ist trotz ihrer überragenden Bedeutung für den Verbraucherdatenschutz an keiner Stelle des § 43 Abs. 1 BDSG ausdrücklich genannt. Ein anderes Beispiel ist, dass in § 43 Abs. 1 Nr. 1 BDSG lediglich die Verletzung der Meldepflicht sanktioniert wird, nicht jedoch das Führen eines aktuellen Verfahrensverzeichnisses, wenn die Meldepflicht aufgrund der Bestellung eines betrieblichen Datenschutzbeauftragten nach § 4 d Abs. 2 BDSG entfällt.[340] Ein weiteres Beispiel ist schließlich, dass die für die Zweckbindung bedeutsame „konkrete Festlegung" der Verwendungszwecke, die nach § 28 Abs. 1 Satz 2 BDSG bei der Erhebung der Daten vorzunehmen ist, nicht bußgeldbewehrt ist und zwar auch bei solchen Unternehmen, die diese Festlegung nicht schon im Rahmen der Meldepflicht (§ 4 e Nr. 4 BDSG) vornehmen müssen.

Die Unterregulierung der Bußgeldtatbestände hat nicht nur eine falsche Signalwirkung gegenüber den verantwortlichen Stellen. Sie entmutigt auch die betroffenen Verbraucher. Es liegt nahe, dass das Vertrauen in eine verbraucherfreundliche Regulierung des Datenschutzes signifikant abnimmt, wenn den Betroffenen bewusst wird, dass Gesetzesverstöße für die Verantwortlichen tatsächlich ohne Sanktionen bleiben. Für diese These gibt es mittlerweile auch empirische Belege.[341]

## 9.3 Proaktiver Datenschutz

Von grundlegender Bedeutung für die Verbesserung des Verbraucherdatenschutzes ist ungeachtet der Rolle eines wirksamen und damit glaubwürdigen reaktiven Datenschutzes ein proaktiver Datenschutz. Er beruht im Wesentlichen auf drei Säulen, nämlich der Beratung der Unternehmen, dem Konzept Datenschutz durch Technik sowie der Etablierung des Datenschutzes als Wettbewerbskriterium.

### 9.3.1 Datenschutz durch Beratung

Durch eine Beratung der Unternehmen soll verhindert werden, dass die Programme zur Datenverarbeitung so gestaltet werden, dass sie gegen die Regeln des Datenschutzes verstoßen.[342] Es gilt, Investitionen in die Datenverarbeitung bereits im Ansatz in die richtige, nämlich datenschutzkonforme Gestaltung zu lenken. Die Aufgabe der Beratung gilt der Lösung

---

[340] Siehe Gola/Schomerus, BDSG, § 43, Rn. 5.

[341] Siehe Spiekermann in: ULD/Humboldt-Universität Berlin, TAUCIS, Kap. 5, Anschnitt 3.3. Die Studie ist im Auftrag des BMBF erstellt, zum 31.03.2006 abgeschlossen und noch nicht veröffentlicht.

[342] Ausführlich Weichert, Datenschutzberatung – Hilfe zur Selbsthilfe, in: Bäumler, Der neue Datenschutz, S. 213 ff.

von Einzelfällen, aber auch der Gestaltung von Konzepten und Geschäftsmodellen, soweit sie mit der Verarbeitung personenbezogener Daten verbunden sind. Diese Aufgabe kann im Unternehmen von dem betrieblichen Datenschutzbeauftragten wahrgenommen werden (s.o. S. 158). Sie gehört auch zum Selbstverständnis der gesetzlichen Aufgabenwahrnehmung einiger Aufsichtsbehörden (s.u. S. 171).[343] Die Aufsichtsbehörde in Baden-Württemberg veröffentlicht bspw. jährliche Datenschutzhinweise für die verantwortlichen Stellen, die über das Internet verfügbar sind.[344] Bei anderen Aufsichtsbehörden scheitern derartige Veröffentlichungen an fehlenden Ressourcen und beschränken sich auf die Aufbereitung aktueller Fälle.[345] Eine Plattform für diese Angebote bietet das Virtuelle Datenschutzbüro.[346]

Schließlich kann sich der betriebliche Datenschutzbeauftragte „in Zweifelsfällen“ an die Aufsichtsbehörde wenden (§ 4 f Abs. 1 Satz 2 BDSG) und muss dies im Falle des § 4 Abs. 6 Satz 3 BDSG sogar.

Durch die Aufsichtsbehörden erfolgt auch eine Beratung der Verbraucherinnen und Verbraucher, die sich mit ihrem Anliegen an diese wenden (s.o. S. 65). Eine Berichterstattung hierüber erfolgt im Regelfall in den von der Aufsichtsbehörde nach § 38 Abs. 1 Satz 6 BDSG regelmäßig, mindestens alle zwei Jahre zu veröffentlichenden Tätigkeitsbericht. Die Erfahrungen und Schlussfolgerungen stehen damit anderen Stellen sowie den Verbraucherinnen und Verbrauchern allgemein zugänglich zur Verfügung.[347] Allerdings zeigt sich in der Praxis, dass eine wirksame Verbraucherinformation einer medialen Aufbereitung in anderer Form als die amtlichen Tätigkeitsberichte bedarf. So hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein im Auftrag des Bundesverbandes der Verbraucherzentralen eine Broschüre mit 99 Tipps zum Datenschutz für Verbraucher herausgegeben, die von beiden Einrichtungen als Druckexemplar vertrieben wird und im Internet verfügbar ist.[348]

### 9.3.2 Datenschutz durch Technik

Unter der Überschrift „Datenschutz durch Technik“ wird das juristische Konzept des Datenschutzes um einen wichtigen Stützpfeiler der Technikgestaltung ergänzt und erweitert.[349] Datenschutz versteht sich nicht als Technikfeind, sondern als Innovationsmotor[350] für datenschutz- und verbraucherfreundliche Verarbeitungstechniken. Bereits 1995 hatte der Forschungsrat gefordert, der traditionell normative ausgestaltete Datenschutz müsse angesichts

---

[343] Hillenbrandt-Beck in: Roßnagel, HdBDatSchR, Kap. 5.4, Rn. 96.

[344] http://www.innenministerium.baden-wuerttemberg.de/de/Infomaterial/83471.html.

[345] http://www.datenschutzzentrum.de/wirtschaft/index.htm.

[346] www.datenschutz.de.

[347] Hillenbrandt-Beck in: Roßnagel, HdBDatSchR, Kap. 5.4, Rn. 97.

[348] http://www.datenschutzzentrum.de/download/BDSG_Handbuch.pdf.

[349] Vgl. Bizer, Datenschutz durch Technikgestaltung in: Bäumler/von Mutius, S. 28 ff.

[350] So der Titel eines Beitrages von Rannenberg in: Bäumler (Hrsg), S. 190.

der neuen Bedingungen der Datenverarbeitung durch „*Datenschutztechnologie*“ ergänzt werden.[351]

Normativer Ausgangspunkt ist § 3 a BDSG. Danach haben sich die Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, „keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Umgesetzt wird diese Vorgabe unter der Überschrift der Privacy Enhancing Technologies (PET).[352] Einen wichtigen Beitrag zur Entwicklung und Implementierung datenvermeidender Techniken liefern Konzepte eines datenschutzfreundlichen Identitätsmanagements bspw. unter Verwendung von Pseudonymen.[353] Das prominenteste Vorhaben ist das Projekt PRIME, in dem unter Beteiligung und Mitwirkung der Wirtschaft mit Mitteln der EU marktgerechte Konzepte eines Identitätsmanagements entwickelt werden.[354] Für den Verbraucherdatenschutz ist diese Entwicklung von großer Bedeutung, weil ein effizienter Datenschutz nicht nur auf der Ebene der rechtlichen Regulierung, sondern der datenschutzfreundlichen Begrenzung der Verarbeitungstechnologien in den Unternehmen ansetzen muss. Intelligente Pseudonymitätskonzepte können einerseits das Auswertungsinteresse der Unternehmen an einem validen Datenmaterial über ihre Kunden befriedigen und gleichzeitig den Schutz der informationellen Selbstbestimmung gewährleisten.

### 9.3.3 Datenschutz als Wettbewerbskriterium

Das moderne Datenschutzrecht versucht der zunehmenden Bedeutung des Datenschutzes als Akzeptanzkriterium seitens der Nutzer durch eine stärkere Implementierung marktwirtschaftlicher Instrumente gerecht zu werden.[355] Der Datenschutz wird auf diese Weise zu einem *Wettbewerbsfaktor* der Unternehmen.[356] Ihrer Intention nach zielen die beiden zentralen Instrumente einer ergänzenden marktwirtschaftlichen Ausrichtung des Datenschutzrechts – das freiwillige Datenschutzaudit und das Gütesiegel – auf eine Prämierung der Datenschutzanstrengungen und -investitionen in Form eines Zertifikates, mit dem im Wettbewerb

---

[351] Deutscher Forschungsrat 1995, S. 32. Später auch 54. Konferenz der Datenschutzbeauftragten vom 23./24.10.1997, DuD 1997, 735.

[352] Überblick bei Marit Hansen in: Roßnagel, HdBDatSchR, Kap. 3.3.

[353] Siehe Hansen, Mit dem Werkzeugkasten in die Informationsgesellschaft, in FG Bäumler, S. 283 ff. Bauer/Meints/Hansen (Eds.): Structured Overview on Prototypes and Concepts of Identity Management Systems; Pfitzmann/Hansen: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management; Federrath/Berthold, Identitätsmanagement in: Bäumler, Der neue Datenschutz, S. 189 ff.

[354] http://www.datenschutzzentrum.de/projekte/idmanage/links.htm.

[355] Bäumler, DuD 2002, 325 ff.; Bäumler/v. Mutius, Datenschutz als Wettbewerbsvorteil 2002; Roßnagel in: HdBDatSchR, Kap. 3.7.

[356] Grundlegend Büllesbach RDV 1997, 239 f.

geworben werden kann. Zudem sind die Regelungen über die datensparsame Technikgestaltung als finales Recht auf flankierende Marktmechanismen angewiesen, die ihre Entwicklung und Implementierung in konkrete Anwendungen befördern.[357]

Wenn die Systeme komplexer und die zeitlichen Aufwendungen zur Nachsteuerung zugunsten des Datenschutzes wachsen, dann ist die richtige Konsequenz aus diesem Befund, dass der Datenschutz bereits standardmäßig in die Produkte implementiert werden muss. Das Datenschutz-Gütesiegel hat hierbei die Funktion, die Datenschutzkonformität des Produktes gegenüber den Verbraucherinnen und Verbrauchern zu signalisieren. Gleichzeitig ermöglicht das Datenschutz-Gütesiegel dem Unternehmen, das den Aufwand getätigt hat, sein Produkt mit der Auszeichnung des Datenschutz-Gütesiegels zu bewerben. Eine vergleichbare Wirkung kommt dem Datenschutz-Audit zu, mit dem die Verfahren der Datenverarbeitung aufgrund ihrer geprüften Datenschutzkonformität ausgezeichnet werden. Gütesiegel und Audit sind Instrumente des präventiven Datenschutzes, mit denen Hersteller und Anbieter sich gegenüber den Verbraucherinnen und Verbrauchern von einem unabhängigen Dritten die Datenschutzkonformität ihrer Datenverarbeitung bestätigen lassen. Ist auf der einen Seite im Rahmen der aufsichtsbehördlichen Praxis festzustellen, dass die missbräuchliche Datenverarbeitung den Verbraucher emotional enttäuscht und der Vertrauensverlust zur Abwendung vom Unternehmen führt, so lässt sich umgekehrt die nach außen als datenschutzkonform zertifizierte Datenverarbeitung als vertrauensbildende Maßnahme wettbewerbsrechtlich und kundenbindend nutzen.

Ein anderer wichtiger Mechanismus, die Durchsetzung von Datenschutzanforderungen über die Regularien von Markt und Wettbewerb zugunsten der Verbraucherinnen und Verbrauchern zu stärken und das Normbefolgungsdefizit abzubauen, ist die wettbewerbsrechtliche Unterlassungsklage durch einen Wettbewerber oder durch einen klagebefugten Verband wie bspw. die Verbraucherverbände. Allerdings schwankt die Rechtsprechung, ob und in welchen Fällen ein Verstoß gegen Datenschutzbestimmungen auch einen Wettbewerbsverstoß darstellt[358] bzw. Datenschutzbestimmungen eine verbraucherschützende Wirkung zukommt.[359] Je nach Einschätzung der Rechtslage kann der Verstoß gegen Datenschutzbestimmungen durch einen Verbraucherverband im Wege einer Unterlassungsklage bzw. einem Wettbewerber gerügt werden.

---

[357] Bizer in: Simitis, BDSG, § 3 a, Rn. 36 ff.; Bizer in. Schulte, S. 595 f.

[358] Zustimmend BGH, NJW 1992, 2419; OLG Köln, WRP 1982, 540; OLG Koblenz, DuD 1999, 358; LG Mannheim, NJW 1996, 1835; LG Hamburg, CR 1997, 21; LG München I, CR 1998, 83; LG Stuttgart, DuD 1999, 295; OLG Köln, RDV 2001, 103 ff.; Ablehnend bspw. OLG Frankfurt, DuD 1997, 47.

[359] A.A. OLG Düsseldorf, DuD 2004, 631 f.

# 10 Verbesserung der Effizienz der staatlichen Datenschutzaufsicht

Bevor Maßnahmen zur Verbesserung der Effizienz der Datenschutzaufsicht dargestellt werden, sind kurz die Organisation und die Befugnisse der Datenschutzaufsichtsbehörden darzustellen.

## 10.1 Organisation der Datenschutzaufsicht

Die datenschutzrechtliche Aufsicht nach § 38 BDSG fällt in die Verwaltungskompetenz der Bundesländer. Nach § 38 Abs. 6 BDSG bestimmen die Landesregierungen oder eine von diesen ermächtigte Stelle, welche Behörde für die Kontrolle der Durchführung des Datenschutzes bei nicht-öffentlichen Stellen sowie öffentlich-rechtlichen Wettbewerbsunternehmen zuständig ist. Die Aufsichtsbehörden sind folglich Landesbehörden, deren örtliche Zuständigkeit sich nach den jeweiligen Verwaltungsverfahrensgesetzen richtet. Maßgebend für die örtliche Zuständigkeit ist der Sitz bzw. die Betriebsstätte des zu kontrollierenden Unternehmens. [360]

Die Aufsichtsbehörden sind in den einzelnen Ländern in unterschiedlicher Weise organisiert. So sind die Aufsichtsbehörden in Baden-Württemberg, Brandenburg, Niedersachsen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt und Thüringen in das Innenministerium des jeweiligen Landes und in die allgemeine Verwaltung eingebunden oder sind als Mittelbehörde dem jeweiligen Innenministerium nachgeordnet (etwa als Mittelbehörden in Bayern, Hessen).

In Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen und Schleswig-Holstein sind die Behörden bei der jeweiligen Landesbeauftragten bzw. dem jeweiligen Landesbeauftragten für den Datenschutz angegliedert, wobei die Rechts- und zum Teil auch die Fachaufsicht von den einzelnen Innenministerien bzw. -senaten ausgeübt wird.

In der datenschutzrechtlichen Literatur ist seit Jahren umstritten, ob die Eingliederung der Aufsichtsbehörden in den Weisungsstrang eines Ministeriums den Anforderungen nach Art. 28 der EG-Datenschutzrichtlinie erfüllen kann, wonach die Datenschutzkontrolle in völliger Unabhängigkeit auszuüben ist.[361] Die EU-Kommission ist der Ansicht, dass die in Deutschland praktizierten Modelle die Anforderungen der EG-Datenschutzrichtlinie nicht erfüllen und hat deswegen im Jahr 2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet.[362]

Die Aufsichtsbehörden üben nach § 38 BDSG die Kontrolle über alle nicht-öffentlichen Stellen im Sinne des § 2 Abs. 4 Satz 1 bzw. § 27 Abs. 1 Satz 1 Nr. 1 BDSG aus. Davon ausge-

---

[360] Walz in: Simitis, BDSG, § 38, Rn. 8.

[361] Aus der Literatur: Die EU-Konformität wird angenommen von Lepper/Wilde, CR 1997, 703 ff.; Hillenbrandt-Beck in: Roßnagel, HdBDatR, Kap. 5.4, Rn. 26; verneint von Hellermann/Wieland, DuD 2000, 284 ff.; Groß, DuD 2002, 684 ff.

[362] EU-Kommission, DuD 2005, 607.

nommen sind die Unternehmen, die geschäftsmäßig Telekommunikationsdienste oder Postdienste erbringen. Hier wird die Datenschutzkontrolle anstelle der Aufsichtsbehörde nach § 38 BDSG durch den Bundesbeauftragten für den Datenschutz nach seinen Befugnissen gegenüber öffentlichen Stellen wahrgenommen (§ 115 Abs. 4 TKG bzw. § 42 Abs. 3 PostG). Die Anordnungsbefugnis liegt jedoch nach § 115 Abs. 1 bzw. § 42 Abs. 1 PostG bei der Bundesnetzagentur (früher Regulierungsbehörde für Post und Telekommunikation). Beanstandungen sind direkt gegenüber dem Bundesministerium für Wirtschaft auszusprechen (§ 115 Abs. 4 TKG bzw. § 42 Abs. 3 PostG). Obwohl die Post- und Telekommunikationsdienste nicht mehr als Sondervermögen des Bundes erbracht werden, blieb die Bundeszuständigkeit erhalten.

## 10.2 Rechtliche Befugnisse der Aufsichtsbehörden

Der Aufsichtsbehörde sind nach § 38 BDSG verschiedene Instrumente zur Kontrolle eingeräumt. Diese reichen von Unterrichtungs- und Anzeigebefugnissen (§ 38 Abs. 1 Satz 5 BDSG) über Veröffentlichungsbefugnisse (§ 38 Abs. 2 Satz 1 BDSG), Auskunftsrechte (§ 38 Abs. 3 Satz 1 BDSG) und Betretungs-, Prüfungs-, Besichtigungs- und Einsichtsbefugnisse (§ 38 Abs. 4 Satz 1, 2 BDSG) bis hin zu Anordnungs-, Untersagungs- und Abberufungsbefugnissen (§ 38 Abs. 5 Satz 1, 2, 3 BDSG).

### 10.2.1 Kontrollrecht

Die Aufsichtsbehörde hat das Recht zur anlasslosen Kontrolle der Datenverarbeitung einer nicht-öffentlichen Stelle. Die Aufsichtsbehörde kann also auch von sich aus Kontrollen vornehmen und damit Schwerpunkte setzen, ohne dass sie eines konkreten Anlasses z.B. durch eine Petition bedarf. Allerdings beschränkt sich diese Kontrolle auf eine automatisierte Datenverarbeitung.[363]

### 10.2.2 Auskunftsrecht

Die der Kontrolle unterliegenden Stellen haben der Aufsichtsbehörde nach § 38 Abs. 3 Satz 1 BDSG Auskunft zu erteilen und zwar in dem Umfang, in dem es zur Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich ist. Dem Auskunftspflichtigen steht nach Satz 2 der Vorschrift ein Auskunftsverweigerungsrecht zu, soweit er sich selbst oder einen in § 383 Abs. 1 Nr. 1 bis 3 Zivilprozessordnung aufgeführten Angehörigen durch die Auskunft der strafrechtlichen Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Die verantwortliche Stelle ist zur wahrheitsgemäßen, vollständigen und rechtzeitigen Beantwortung der durch die Aufsichtsbehörde ggfs. mit Fristsetzung gestellten Fragen verpflichtet,

[363] Siehe zur beschränkten Kontrolle der Tätigkeit eines Privatdetektivs OVG Hamburg, DuD 2005, 737.

soweit ein Auskunftsverweigerungsrecht nicht besteht. Die vorsätzliche oder fahrlässige Zuwiderhandlung gegen diese Verpflichtung stellt eine Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 10 BDSG dar.

### 10.2.3 Betretungs-, Prüfungs-, Besichtigungs- und Einsichtsbefugnisse

Darüber hinaus muss die verantwortliche Stelle den Mitarbeitern der Aufsichtsbehörde den Zugang zum Grundstück und den Geschäftsräume, die Prüfungsmöglichkeit, die Besichtigung und die Einsicht in Geschäftsunterlagen gewähren (§ 38 Abs. 4 BDSG). Das Einsichtsrecht gilt für alle prüfungsrelevanten Geschäftsunterlagen und umfasst insbesondere auch das Verfahrensverzeichnis nach § 4 g Abs. 2 Satz 1 BDSG. Ein Zuwiderhandeln ist nach § 43 Abs. 1 Nr. 10 BDSG bußgeldbewehrt. Die genannten Maßnahmen haben zu den Betriebs- und Geschäftszeiten zu erfolgen und müssen zur Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sein. Die Duldung des Auskunftspflichtigen kann mit den Mitteln des Verwaltungsvollstreckungsrechtes des jeweiligen Landes erzwungen werden.

In der Regel ist ein Erscheinen der Aufsichtsbehörde vor Ort nur dann erforderlich, wenn ein Auskunftsersuchen auf schriftlichem, telefonischem, elektronischem Weg etc. als weniger einschneidende Maßnahmen entweder fehlgeschlagen ist oder nicht dazu geführt hat, der Aufsichtsbehörde eine abschließende und umfassende rechtliche Beurteilung des konkreten Falles zu ermöglichen. Eine Voranmeldung ist ratsam, um die verantwortlichen Personen vor Ort anzutreffen. Eine Verpflichtung besteht hierzu besteht allerdings nicht.[364]

### 10.2.4 Anordnungs-, Untersagungs- und Abberufungsbefugnis

Neben Ordnungswidrigkeitsverfahren und Strafantrag ist die Anordnungsbefugnis und Untersagungsbefugnis nach § 38 Abs. 5 Satz 1 BDSG das stärkste Kontrollinstrument der Aufsichtsbehörde. Die Anordnung stellt einen Verwaltungsakt dar, welcher als belastende Maßnahme grundsätzlich eine Anhörung der verantwortlichen Stelle erforderlich macht.

Nach § 38 Abs. 5 Satz 1 BDSG kann die Aufsichtsbehörde allerdings nur Maßnahmen im Rahmen der Anforderungen nach § 9 BDSG zur Beseitigung festgestellter technischer oder organisatorischer Mängel anordnen. Teilweise wird in der Regelung des § 38 Abs. 5 Satz 1 BDSG eine Begrenzung der Anordnungsbefugnis auf Maßnahmen zur Beseitigung von Verstößen gegen die Datensicherheit gesehen, so dass die Aufsichtsbehörde eine Beseitigung materieller Rechtsverstöße nicht verlangen könne.[365] Dem steht allerdings entgegen, dass § 9 BDSG all jene technischen und organisatorischen Maßnahmen vorschreibt, die für die Ausführung der Vorschriften des BDSG und damit des materiellen Datenschutzrechts erforderlich sind. Insofern kann auch bei materiellen Rechtsverstößen über den Weg der Anordnung von Datensicherungs- bzw. organisatorischen Maßnahmen eine Beseitigung materiell

[364] Walz in: Simitis, BDSG, § 38 Rn. 30.

[365] Von Lewinski, RDV 2001 275 (276); Walz in: Simitis, BDSG § 38 Rn. 39.

rechtswidriger Zustände erreicht werden.[366] Hierbei ist zu berücksichtigen, dass die Anordnungsbefugnis im Lichte der EG-Datenschutzrichtlinie auszulegen ist. Sie sieht in Art. 28 Abs. 3, 2. Spiegelstrich vor, dass die zuständige Behörde mit wirksamen Einwirkungsbefugnissen auszustatten ist. Hierzu gehört zwangsläufig die Befugnis, die Sperrung, Löschung oder Vernichtung von personenbezogenen Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anordnen zu können.[367] Auch die Anordnung der Löschung von Daten, die auf der Grundlage einer unwirksamen Einwilligung des Betroffenen erhoben und gespeichert wurden, ist eine zulässige Anordnung der Aufsichtsbehörde. Ob die Aufsichtsbehörde die Bestellung eines betrieblichen Datenschutzbeauftragten anordnen darf, wenn unter Verstoß gegen die materielle Verpflichtung nach § 4 f Abs. 1 BDSG ein solcher von der verantwortlichen Stelle nicht berufen wird, dürfte umstritten sein.[368]

Unter den Voraussetzungen des § 38 Abs. 5 Satz 2 BDSG kann die Aufsichtsbehörde bei Nichtvollzug der Anordnung auch den Einsatz einzelner Verfahren untersagen. Das vorsätzliche oder fahrlässige Handeln gegen eine vollziehbare Anordnung nach § 38 Abs. 5 Satz 1 BDSG ist eine Ordnungswidrigkeit (§ 43 Abs. 1 Nr. 11 BDSG).

Die Aufsichtsbehörde hat ferner die Möglichkeit per Verwaltungsakt die Abberufung eines betrieblichen Datenschutzbeauftragten zu verlangen, der die zur Erfüllung der Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht oder nicht mehr besitzt (§ 38 Abs. 5 Satz 3 BDSG).

### 10.2.5 Unterrichtungs- und Anzeigebefugnisse

Die Behörde ist nach § 38 Abs. 1 Satz 5 BDSG berechtigt, den Betroffenen über Verstöße gegen das Datenschutzrecht zu unterrichten. Auf diese Weise erhält der Betroffene Kenntnis von dem Datenschutzverstoß, kann seine Geschäftsbeziehung zu dem Unternehmen abbrechen, die Öffentlichkeit unterrichten, nach § 44 BDSG Strafantrag stellen und seine Ansprüche im Wege der Zivilklage (u.a. Schadensersatz nach § 7 BDSG) geltend machen.

Zudem ist die Aufsichtsbehörde berechtigt, Verstöße der für die Ahndung und Verfolgung zuständigen Stelle also bspw. der Staatsanwaltschaft anzuzeigen. Bei schwerwiegenden Verstößen kann sie die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen einschalten (§ 38 Abs. 5 Satz 2 BDSG). Da die Anwendung der Gewerbeordnung nach § 38 Abs. 7 BDSG unberührt bleibt, kann die Gewerbeaufsichtsbehörde ihre gewerberechtlichen Eingriffsbefugnisse, insbesondere die der Gewerbeuntersagung nach § 35 GewO, auch bei Verstößen gegen das Datenschutzrecht ausüben. Es ist Aufgabe der Gewerbeaufsichtsbehörde zu beurteilen, ob der Datenschutzverstoß auf die Unzuverlässigkeit

[366] Von Schmeling, DuD 2002 351, 355.

[367] Von Schmeling, DuD 2002 351, 355.

[368] Von Schmeling, DuD 2002 351, 354.

des Gewerbetreibenden schließen lässt.[369] Aus der Praxis sind derartige Fälle nicht bekannt, so dass davon auszugehen ist, dass sie praktisch bedeutungslos sind.

### 10.2.6 Veröffentlichungsbefugnis

Nach § 38 Abs. 2 Satz 1 BDSG führt die Aufsichtsbehörde ein Register über automatisierte Verarbeitungen, die nach § 4d BDSG meldepflichtig sind. Das Register dient der Aufsichtsbehörde als Informationsgrundlage für die Überwachungs- und Prüftätigkeit und schafft zudem Transparenz für die Öffentlichkeit, da es von jedem eingesehen werden kann (§ 38 Abs. 2 Satz 2 BDSG).[370]

Darüber hinaus kann sich die Aufsichtsbehörde wegen Gesetzesverstößen an die Öffentlichkeit wenden. So hat der BGH im Zusammenhang mit der öffentlichen Äußerung eines Landesbeauftragten für den Datenschutz über einen Gesetzesverstoß einer öffentlichen Stelle entschieden, dass ein zur Kontrolle eines anderen Amtsträgers Berufener, keine wichtigen öffentlichen Interessen durch die Offenbarung eines Gesetzesverstoßes gefährdet, „wenn er die Öffentlichkeit auch als Verbündeten gewinnen will, um auf ein gesetzmäßiges Verhalten hinzuwirken“.[371] In einem anderen Fall, der eine öffentliche Äußerung des Bundesbeauftragten für den Datenschutz zur Rechtmäßigkeit einer Gebäudebilddatenbank betraf, bestätigte das Verwaltungsgericht Köln das Recht des Beauftragten, Sachverhalte, die den nichtöffentlichen Bereich betreffen, in der Öffentlichkeit darzustellen und auch zu bewerten.[372] Dabei bezog sich das Gericht ausdrücklich auf die höchstrichterliche Rechtsprechung, dass ein Staatsorgan durch seine Aufgabenstellung legitimiert ist, zum Schutz anderer Grundrechte vor Produkten zu warnen, „wenn ein hinreichend gewichtiger, dem Inhalt und der Bedeutung des berührten Grundrechtes entsprechender Anlass besteht, und wenn die negativen Werturteile nicht unsachlich sind, sondern auf einem im wesentlichen zutreffenden oder zumindest sachgerecht und vertretbar gewürdigten Tatsachenkern beruhen“.[373]

### 10.2.7 Ordnungswidrigkeitsverfahren und Strafantrag

Zudem kann die Aufsichtsbehörde bei Vorliegen eines Tatbestandes nach § 43 BDSG ein Verfahren zur Verhängung von Ordnungswidrigkeiten in den im Gesetz genannten Fällen durchführen. Wenn eine Ordnungswidrigkeit nach § 43 Abs. 2 BDSG vorsätzlich gegen Entgelt oder mit Bereicherungsabsicht begangen worden ist, kann die Aufsichtsbehörde Strafantrag stellen.

---

[369] Walz in: Simitis, BDSG, § 38 Rn. 47.

[370] Walz in: Simitis, BDSG, § 38 Rn. 21, 22.

[371] BGH, DuD 2003, 311, 313.

[372] VG Köln, DuD 1999, 354 ff.

[373] Vgl. BVerfG, NJW 1989, 3269; BVerwG, NVwZ 1994, 162; BVerwGE 87, 37; 82, 77.

### 10.2.8 Beratung

Neben den Kontrollbefugnissen haben die Aufsichtsbehörden gegenüber den Daten verarbeitenden Stellen ebenso wie gegenüber Verbraucherinnen und Verbrauchern auch ein umfassendes Beratungsrecht, das sie in Abhängigkeit ihrer Personalausstattung auch wahrzunehmen versuchen.[374]

## 10.3 Effizienzsteigerung der Aufsichtsbehörden

### 10.3.1 Organisation

Von außen betrachtet ist für die Verbraucher die Datenschutzkontrolle durch staatliche Aufsichtsbehörden wirksam, wenn sie über einen Ansprechpartner in allen Fragen des Datenschutzes verfügen. Verwirrend ist es für die Verbraucher, wenn die Zuständigkeit ein und dieselbe Branche (bspw. Verkehrsbetrieb, Sport- und Freizeitanlagen und -veranstaltungen, Energieversorgung, Abwasser- und Müllentsorgung) je nach Rechtskonstruktion mal dem öffentlichen und mal dem nicht-öffentlichen Sektor zuzuordnen sind, so dass in dem einen Fall die für den öffentlichen Bereich und in dem anderen Fall die für den nicht-öffentlichen Sektor zuständige Aufsichtsbehörde Adressat der Eingabe sein muss. Nicht weniger verwirrend ist es für den Verbraucher, wenn der Bundesbeauftragte für den Telekommunikationsdatenschutz, aber die Aufsichtsbehörden der Länder für den Datenschutz bei den Internetangeboten zuständig sind, weil es sich aus seiner Sicht um ein einheitliches Angebot handelt. Schließlich können viele Verbraucher nicht nachvollziehen, warum die Datenschutzaufsicht über die Gebühreneinzugszentrale des öffentlich-rechtlichen Rundfunks (GEZ) überwiegend bei den Datenschutzbeauftragten der Landesrundfunkanstalten, und nur in wenigen Fällen (Brandenburg, Bremen und Hessen) bei den unabhängigen Datenschutzbeauftragten der Länder liegt.[375]

Dem Verbraucher sollte der Datenschutz „aus einer Hand“ angeboten werden. Es ist wenig verbraucher- und kundenfreundlich, wenn dem Verbraucher, der sich mit einem materiellen Anliegen an einen Datenschutzbeauftragten wendet, zunächst einmal Zuständigkeitsfragen vermittelt werden müssen. Aus diesem Grund ist die Übertragung der Aufgabe der Aufsichtsbehörden nach § 38 BDSG an die jeweiligen Landesbeauftragten für den Datenschutz ungeachtet der unterschiedlichen Konstruktionen[376] eine sinnvolle Lösung. Sie ist im Übrigen auch aus Gründen der Synergieeffekte, der Verwaltungsvereinfachung sowie zur Sicherung

---

[374] Hillenbrand-Beck in: Roßnagel, HdBDatSchR, Kap. 5.4, Rn. 96.

[375] Dies wird von Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten anders gesehen: bspw. Herb in: Roßnagel, HdBDatSchR, Kap. 5.3, Rn. 29 ff.

[376] Siehe bspw. die Berliner Lösung, Garstka, DuD 2000, 289. Das Modell Schleswig-Holstein Bäumler, DuD 2000, 20 ff.

der europarechtlich gebotenen Unabhängigkeit der Datenschutzaufsicht im nicht-öffentlichen Bereich geboten.[377]

Im Interesse der Vereinfachung des Zugangs zu Datenschutzfragen betreiben alle Datenschutzbeauftragten des Bundes und der Länder unter dem Namen „Virtuelles Datenschutzbüro“ seit dem Jahr 2000 ein Internetportal (www.datenschutz.de). Die Geschäftsführung liegt beim Unabhängigen Landeszentrum für den Datenschutz in Schleswig-Holstein (ULD). Unter diesem Portal werden Informationen zu zentralen Datenschutzthemen sowie die zuständigen Ansprechpartner vermittelt.[378] Mitglied im Virtuellen Datenschutzbüro sind auch zwei Datenschutzbeauftragte der öffentlich-rechtlichen Rundfunkanstalten. Den Aufsichtsbehörden steht das Virtuelle Datenschutzbüro offen.

Die Entwicklung dezentraler und vernetzter Datenverarbeitung stellt die Aufsichtsbehörden vor zusätzliche Herausforderungen der Abstimmung und Kooperation. Die Aufsichtsbehörden bemühen sich zu allen zentralen Themen von bundesweiter Bedeutung um eine Koordination ihrer Rechtsauffassung gegenüber den Daten verarbeitenden Stellen. Wie in anderen Themenfeldern verläuft die Abstimmung der Aufsichtsbehörden der Länder unter Mitwirkung des Bundes in föderalen Abstimmungsrunden. Im so genannten „Düsseldorfer Kreis“ stimmen die Aufsichtsbehörden zwei Mal im Jahr in einer zweitägigen Tagung grundlegende Positionen ab. Aus Gründen der Effektivität sind ferner Arbeitsgruppen zu den Themen Auskunfteien, Kreditwirtschaft, Versicherungswirtschaft und Telemedien gebildet worden. Aufgrund seiner föderalen Struktur ist der Düsseldorfer Kreis jedoch nur ein informelles Gremium, das keine bindenden Beschlüsse fasst.[379] Eine horizontale Abstimmung bei der Auslegung und Anwendung der Datenschutzbestimmungen zu zentralen Themen des Verbraucherdatenschutzes ist notwendig. Unter den gegenwärtigen Bedingungen der föderalen Organisation ist dies nur auf der Basis einer von allen 16 Aufsichtsbehörden gemeinsam getragenen Auffassung möglich.

In dieser Situation besteht die Gefahr, dass die Findungsprozesse einer gemeinsamen Linie zu zentralen Fragen so zeitaufwändig sind, dass die Chance für einen proaktiven Datenschutz vertan wird. Dabei ist zu berücksichtigen, dass auch die Daten verarbeitenden Stellen zunächst ein überwiegendes Interesse an Rechtssicherheit haben. Aus ihrer Sicht sollen zentrale Datenschutzbestimmung von den Aufsichtsbehörden gegenüber allen Wettbewerbern gleich ausgelegt und angewendet werden. Die Interessen der Daten verarbeitenden Stellen sowie des Verbraucherdatenschutzes sind insofern kongruent. Zugunsten eines einheitlich wirkenden Verbraucherdatenschutzes müssen die föderalen Abstimmungsprozesse vereinfacht werden. Richtungsweisend könnte eine Praxis werden, Mehrheitsvoten über zentrale Auslegungs- und Anwendungsfragen ungeachtet der jeweiligen Länderzuständigkeit im Einzelfall zur informellen Grundlage der eigenen Verwaltungspraxis heranzuziehen und zu berücksichtigen.

---

[377] Schaar in: Bäumler, E-Privacy, S. 73; ders, DuD 2005, 579; Arlt in: Bäumler, Der neue Datenschutz, S. 281 f.; Garstka in: Bäumler, Der neue Datenschutz, S. 159 ff.

[378] Köhntopp, Virtuelles Datenschutzbüro in: Bäumler, E-Privacy, S. 291 ff.

[379] Siehe Hillenbrandt-Beck in: Roßnagel, HdBDatSchR, Kap. 5.4, Rn. 98.

Aus Sicht des Verbraucherdatenschutzes wie auch der verantwortlichen Stellen ist ein weiteres Problem die Zuständigkeitsaufteilung im Bereich von Telekommunikation und Neuen Medien. Sowohl die Anbieter als auch die Verbraucher erwarten auch hier einen Datenschutz aus „einer Hand“,[380] d.h. eine einheitliche Rechtsauslegung zum TK- und Online-Datenschutz. Diese ist wegen der Zuständigkeit des Bundesbeauftragten für den gesamten Bereich des TK-Datenschutzes gewährleistet. In der Praxis wenden sich aber gerade kleine und mittlere Unternehmen aus Gründen der Entfernung und aus der Sicht der Sachnähe an ihre regionalen Aufsichtsbehörden, weil diese für die anderen Fragen, wie die des Verbraucher- und des Arbeitnehmerdatenschutzes zuständig sind. Umgekehrt ist es im Bereich der Onlinedienste: Hier sind zwar die Aufsichtsbehörden der Länder zuständig. Insofern bedarf es einer horizontalen Abstimmung mit den anderen Aufsichtsbehörden sowie mit dem Bundesbeauftragten, um eine Divergenz von TK- und Telemedien-Datenschutz zu vermeiden. Vor dem Hintergrund der im Grundgesetz geregelten Verwaltungskompetenz der Länder (Art. 83 GG) kann die Lösung nur in zügigeren Abstimmungsprozeduren liegen, mit denen ein gewisses Maß an Verbindlichkeit erzeugt wird. Gleichzeitig wird zu überlegen sein, auf welche Weise dem regionalen Beratungsbedürfnis „aus einer Hand“ vor Ort Rechnung getragen wird, ohne die Zuständigkeit des Bundesbeauftragten für den Datenschutz zu Fragen des TK-Datenschutzes im Grundsatz in Zweifel zu ziehen. Derartige Kooperationsmodelle sind noch nicht entwickelt, geschweige denn Praxis der Aufsichtsbehörden.

Als weitere mittelfristige Tendenz bietet sich für die Länder die Handlungsoption, über Verwaltungskooperationen oder über Fusionen von Bundesländern[381] die Tätigkeit von Aufsichtsbehörden entweder enger miteinander zu verzahnen oder sie für einen länderübergreifenden Zuständigkeitsbereich zusammenzulegen.[382]

Um den Datenschutz auch gegenüber international tätigen Unternehmen für den Verbraucher zu gewährleisten, müssen die Aufsichtsbehörden auf diesem Gebiet intensiver kooperieren und sich abstimmen und dies nicht nur auf nationaler, sondern vor allem auch auf europäischer Ebene. Prüfsteine sind „Vertragsklauseln“ und „verbindliche Unternehmensregeln“, aus denen sich nach § 4 c Abs. 2 Satz 1 BDSG die erforderlichen Garantien zum Schutz des Persönlichkeitsrechts und der damit verbundenen Rechte der Betroffenen ergeben, um eine Datenübermittlung in Drittstaaten ohne angemessenes Schutzniveau genehmigungsfähig zu machen.[383] Durch so genannte „Standardvertragsklauseln“ bemüht sich die Europäische Kommission mit Unterstützung des Art. 31-Auschusses, in dem ein Vertreter der Aufsichtsbehörden sitzt,[384] um eine gewisse Vereinheitlichung der Genehmigungspra-

---

[380] Schaar in: Bäumler, E-Privacy, S. 73; Bizer, DuD 2001. 276.

[381] Z.B. Brandenburg und Berlin, Rheinland-Pfalz und Saarland, Niedersachen und Bremen, Schleswig-Holstein und Hamburg.

[382] Erste Beispiele liegen für die Verwaltungskooperation zwischen Hamburg und Schleswig-Holstein für die Landesämter für Statistik sowie die Eichämter vor. Ein Staatsvertrag zur gemeinsamen Medienaufsicht ist bereits in Vorbereitung.

[383] Siehe bspw. Büllesbach, Selbstregulierung in: FG Bäumler, S. 243 f.; Brühann, Selbstregulierungsinstrumente in: FG Büllesbach, S. 289 ff.; Schröder, DuD 2004, 462 ff.

[384] Heil, DuD 1999, 655.

xis.[385] Dieses Unterfangen ist schon deswegen erforderlich, weil sich die Unternehmen nach den Erfahrungen in der Praxis für die Genehmigung der Datenübermittlung diejenigen Aufsichtsbehörden aussuchen, bei denen sie mit der größten Nachgiebigkeit gegenüber ihrem Anliegen und mit der höchsten Aufgeschlossenheit bei der Begutachtung der „Garantien" rechnen. Dieses „Forum-Shopping" erfolgt im Regelfall gerade nicht im Interesse des Verbraucherdatenschutzes, sondern ausschließlich im Interesse der Unternehmen und einer an kurzfristigen Interessen orientierten Standortpolitik. Einer solchen Entwicklung lässt sich nur Einhalt gebieten, wenn bei einer verbesserten europäischen Abstimmung das Schutzniveau der Verbraucher angeglichen und nicht das niedrigste Niveau zum Maßstab der Genehmigung gemacht wird.

### 10.3.2 Befugnisse

Strukturell wird die Tätigkeit der Aufsichtsbehörden durch die zahlreichen Abwägungsklauseln im Datenschutzrecht erschwert. Sobald eine Interessenabwägung für die Entscheidung über die Rechtmäßigkeit der Datenverarbeitung erforderlich ist, neigen die Aufsichtsbehörden dazu, die Sanktionierungsinstrumente der Anordnung bzw. der Verhängung von Bußgeldern restriktiv einzusetzen. Die Lösung dieses Problems liegt nicht in einer Nachregulierung der Befugnisse, sondern in einer Reduzierung der Abwägungsentscheidungen zugunsten eindeutig gefasster Verwendungszwecke und Tatbestände. Ein deutlicher Anstoß in diese Richtung ging von den Beratungen zur Modernisierung des Datenschutzrechts im Jahr 2001 aus. Die Anregungen sind allerdings von der letzten Bundesregierung nicht aufgegriffen worden.[386]

Vor dem Hintergrund der restriktiven Sanktionierungspraxis der Aufsichtsbehörden bei Abwägungsentscheidungen ist es dringend erforderlich, dass der Verstoß gegen eindeutig formulierte Datenschutzpflichten sowie der Verstoß gegen die für den Verbraucherdatenschutz zentralen Informationspflichten ausdrücklich als Ordnungswidrigkeiten sanktioniert werden und nicht mehr unter den unbestimmten Rechtsbegriff der „unbefugten Verarbeitung" subsummiert werden müssen (s.u. S. 179). Entsprechendes sollte umgesetzt werden, um Verstöße der verantwortlichen Stellen gegen andere Betroffenenrechte zu sanktionieren.

Die Befugnisse der Aufsichtsbehörden sind – mit wenigen Ausnahmen – ausreichend. Die Befugnis zu Anordnungen nach § 38 Abs. 5 Satz 1 BDSG ist im Einklang mit den europarechtlichen Vorgaben („wirksamen Befugnisse") auch bei materiellen Datenschutzverstößen anzuwenden (s.u. S. 168 f.). Die Aufsichtsbehörden sind „keine zahnlose Tiger", vorausgesetzt sie wollen keine sein oder – soweit sie weisungsabhängig agieren – sollen keine sein. Einer Stärkung bedürfen allerdings die Anordnungsbefugnisse nach § 38 Abs. 5 Satz 2 BDSG. Dies ist schon deswegen erforderlich, um das (noch) vorhandene Systemvertrauen der betroffenen Verbraucher in die Wirksamkeit des Datenschutzes nicht durch fehlende Sanktionen bei Datenschutzverstößen zu enttäuschen und „aufs Spiel" zu setzen.

---

[385] Rittweger/Schmidl, DuD 2004, 617 ff.; Ausführlich Simitis in: ders., BDSG, § 4 c, Rn. 45 ff.

[386] Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzes 2001; Weichert, DuD 2001, 264 ff.; Bizer DuD 2001, 274 ff.; zuletzt zu einem Strukturplan der Umsetzung Bizer, DuD 2004, 6 ff.

So sollte die Aufsichtsbehörde bspw. ermächtigt werden, die Sperrung, Löschung oder Vernichtung von personenbezogenen Daten, die widerrechtlich verarbeitet wurden, durch einen bindenden Verwaltungsakt anzuordnen.[387] Die Verfasser des Modernisierungsgutachtens hatten im Einklang mit dem Verhältnismäßigkeitsgrundsatz zudem ein zweistufiges Instrumentarium vorgeschlagen: Ein vorläufiges Verbot mit Fristsetzung zur Beseitigung des rechtswidrigen Zustandes, auf das bei erfolglosem Verstreichen der Frist ein endgültiges Verbot folgt. Auf diese Weise kann ein präventiv wirkender Anreiz geschaffen werden, das Datenschutzrecht zu befolgen. Umgesetzt werden sollte schließlich auch die in Art. 28 Abs. 3 3. Spiegelstrich der EG-Datenschutzrichtlinie 95/46/EG vorgesehene Möglichkeit, den für die rechtswidrige Verarbeitung Verantwortlichen zu verwarnen. Die Verwarnung könnte z.B. eine Schulungsverpflichtung nach sich ziehen. [388]

Die Aufsichtsbehörden sind ferner – wie im Übrigen jede öffentliche Verwaltung – dazu verpflichtet, die verantwortlichen Stellen zu beraten.[389] In welchem Umfang und mit welchen Schwerpunkten diese Pflicht wahrgenommen wird, liegt im Ermessen der Aufsichtsbehörde. Die Erfahrung zeigt, dass diese Beratung von den verantwortlichen Stellen, den betrieblichen Datenschutzbeauftragten sowie den betroffenen Verbrauchern in Anspruch genommen wird.

Zu einer veränderten Wahrnehmung der aufsichtsbehördlichen Tätigkeit kann – wie die Erfahrungen des Unabhängigen Landeszentrums in Schleswig-Holstein zeigen – auch die Zertifizierung datenschutzkonformer Produkte durch ein Gütesiegel führen. Das Gütesiegel wird in Schleswig-Holstein von einer anderen Abteilung nach Prüfung durch einen unabhängige Gutachter (s.u. S.187) erteilt.

### 10.3.3 Kompetenzen

Die Datenschutzaufsicht wird von den Aufsichtsbehörden bisher als ordnungsbehördliche Aufgabe begriffen. Die Konsequenz ist, dass die Arbeit der Aufsichtsbehörden mit wenigen Ausnahmen überwiegend einen juristischen Schwerpunkt haben. Deutliche Mängel der Datenschutzaufsicht bestehen im Bereich des technischen Datenschutzes, der sowohl für die Analyse der technisch-organisatorischen Gegebenheiten vor Ort als auch besonders für eine proaktive Beratung von großer Bedeutung ist.[390] Das Defizit im technischen Datenschutz ist weitgehend erkannt, lässt sich jedoch aufgrund der vorhandenen Personalstruktur und Technikausstattung nicht von heute auf morgen abbauen.[391]

Eine gute Datenschutzberatung erfordert allerdings nicht nur ein qualifiziertes Verständnis des Datenschutzrechts, der wesentlichen Datenschutzrisiken und der wirksamen technisch-organisatorischen Sicherheitsmaßnahmen auf den Ebenen des System- und Selbstdaten-

---

[387] Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, S. 198.

[388] Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, S. 199.

[389] Siehe bspw. Hillenbrand-Beck in Roßnagel, HdBDatSchR, Kap. 5.4, Rn. 96.

[390] Weichert in: Bäumler, Der neue Datenschutz, S. 227 f.; Lutterbeck in: ebenda, S. 254 f.; Schaar in: Bäumler. E-Privacy, S. 75 f.

[391] Lutterbeck in: Bäumler, Der neue Datenschutz, S. 274.

schutzes gleichermaßen, sondern auch die Fähigkeit, sich in Vorgänge und Managementprozesse hineinzudenken, um gemeinsam mit verantwortlichen Stellen eine wirksame Datenschutzstrategie im Interesse ihrer Kunden und Verbraucher entwickeln zu können.

Gegenüber den Verbrauchern ist Datenschutz zunächst eine auf Vermittlung ausgerichtete Aufgabe. Die Verbraucher erwarten auf ihre Eingaben eine wirksame Unterstützung und Aufklärung bei der Wahrnehmung ihrer Datenschutzrechte. Der Sachverhalt muss zwar datenschutzrechtlich und sicherheitstechnisch erfasst und bearbeitet, vor allem jedoch allgemein verständlich im Einzelfall kommuniziert werden. Hierfür bedarf es einer gewissen „pädagogischen und kommunikativen Kompetenz".[392] Die Eingabenbearbeitung beschränkt sich längst nicht mehr auf die klassische bürokratische Kommunikation im schriftlichen Verfahren, sondern erstreckt sich auch auf eine verbindliche Beratung per Telefon oder Email oder erfordert ausgeprägte Techniken der Verhandlungsführung.

Fast in jedem Einzelfall finden sich Problemlagen, deren Lösung auch für eine Vielzahl anderer Personen von Bedeutung ist. Die zweijährlichen Tätigkeitsberichte der Aufsichtsbehörden vermitteln zumindest dem Fachmann einen Eindruck von der Allgemeingültigkeit zahlreicher Einzelfälle, die in den Aufsichtsbehörden bearbeitet werden. Diese Berichte sind aber in der Regel als Arbeitsnachweis an einen parlamentarischen, administrativen Leserkreis adressiert und nicht an den praktischen Bedürfnissen der Verbraucher orientiert. Vielmehr erwarten die Verbraucher eine konkrete Handreichung, eine praktische Formulierung oder eine eindeutige Verhaltensanweisung, die sie konkret in ihrer Situation umsetzen können.

Tätigkeitsberichte sind häufig im Stil öffentlicher Verlautbarungen formuliert und gerade nicht an medialen Rezeptionsgewohnheiten der heutigen Internet- und Fernsehkultur orientiert. Für diese anspruchsvolle Übersetzungsleistung bedarf es Mitarbeiter, die über eine gewisse „mediale Kompetenz" verfügen, um komplizierte Sachverhalte in einfache Verhaltensanweisungen zu transformieren.[393] Dass es an diesen Voraussetzungen offensichtlich fehlt, zeigt der geringe Bekanntheitsgrad der Aufsichtsbehörden bei den befragten Verbrauchern (s.o. S. 90). Dieses Ergebnis wird durch die repräsentative BAT-Untersuchung aus dem Jahr 2001 bestätigt, wonach drei Viertel der Befragten noch nie etwas vom Datenschutzbeauftragten gehört hatten.[394] Um dieses gravierende Informationsdefizit bei den Verbrauchern abzubauen, bedarf es einer grundlegenden Reformierung der Öffentlichkeitsarbeit.

Ansätze sind vorhanden: So hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein gemeinsam mit dem Verbraucherzentrale Bundesverband e.V eine Broschüre mit dem Titel „99 +1 Tipps zum Datenschutz" entwickelt, in der für Verbraucher und kleine und mittlere Unternehmen die zentralen Datenschutzrechte vermittelt werden. Die Broschüre kann auch im Internet herunter geladen werden.[395] Neben dem Einsatz von Faltblättern als

---

[392] Weichert in: Bäumler, Der neue Datenschutz, S. 228.

[393] Weichert in: Bäumler, Der neue Datenschutz, S. 228.

[394] Opaschowski, DuD 2001, 680.

[395] http://www.datenschutzzentrum.de/download/BDSG_Handbuch.pdf.

Verbreitungsmedium für einzelne Themen[396] erlangt vor allem das Internet mehr und mehr Bedeutung bei der Vermittlung von datenschutzrechtlichen und technischen Sachverhalten. Es fehlt aber bspw. ein bundesweites Informationsangebot, in dem praktische „Tipps zum Verbraucherdatenschutz" bereitgestellt werden. Dies liegt im Wesentlichen daran, dass den Aufsichtsbehörden, soweit sie nicht mit den Landesbeauftragten für den Datenschutz identisch sind, entweder die Ressourcen fehlen oder sie aufgrund ihres ordnungsbehördlichen Vorverständnisses bzw. das ihrer Vorgesetzten die gemeinsame Plattform des Virtuellen Datenschutzbüros nicht zur Vermittlung von Datenschutzhinweisen für die Verbraucher nutzen wollen oder können. Öffentlichkeitsarbeit im Weisungsstrang ist typischerweise eine politische Aufgabe der Leitungsebene eines Ministeriums, so dass es die herkömmlichen Aufsichtsbehörden in dieser Hinsicht mangels Unabhängigkeit schwer haben. Bernd Lutterbeck hatte bereits 1998 nach einer Analyse der Webseiten der Datenschutzbeauftragten festgestellt, dass sie sich „überwiegend als Bürokratien mit einem eher langweiligen Aufgabenbereich" präsentieren.[397] Es steht zu vermuten, dass er die Präsentation der Aufsichtsbehörden auch heute nicht wesentlich anders beurteilen würde. Jedenfalls trägt die Präsentation im Internet nicht dazu bei, den Bekanntheitsgrad der staatlichen Datenschutzkontrolle in der Bevölkerung nennenswert zu vergrößern.

Von nicht geringer Bedeutung für den Verbraucherdatenschutz ist schließlich die *mediale Präsenz* der Aufsichtsbehörden in der Öffentlichkeit. Hierzu gehört neben der Aufbereitung und Verfügbarkeit der Themen des Verbraucherdatenschutzes die Bereitschaft, für Beiträge auf öffentlichen und fachöffentlichen Veranstaltungen zur Verfügung zu stehen. Derartige Veranstaltungen sind immer eine Chance, die Verbraucher durch eine „Hilfe zum Selbstdatenschutz" zu unterstützen.[398] Trotz einiger positiver Ansätze[399] ist die Zusammenarbeit der Aufsichtsbehörden mit den Verbraucherverbänden stark entwicklungsbedürftig. Eine zentrale Ursache für diesen Mangel ist, dass im ordnungsbehördlichen Verständnis der Aufsichtsbehörden die Verbraucherverbände als Non Government Organisation (NGO) außerhalb der Staatsverwaltung stehen. Eine andere Sichtweise und Praxis wird den Aufsichtsbehörden strukturell möglich, wenn diese Aufgabe den unabhängigen Landesbeauftragten für den Datenschutz zugeordnet ist.

Datenschutz ist Grundrechtsschutz, der nicht umsonst zu haben ist.[400] Viele Möglichkeiten, den Verbraucherdatenschutz zu entwickeln, zu vermitteln und zu fördern bleiben ungenutzt,

---

[396] Siehe bspw. das Angebot an Faltblättern des Brandenburger Landesbeauftragten für Datenschutz und Akteneinsicht: [http://www.lda.brandenburg.de/sixcms/detail.php?template=lda_info_d];
Das Angebot des Bundesbeauftragten für den Datenschutz und Informationsfreiheit:
[http://www.bfdi.bund.de/cln_029/nn_531942/DE/Oeffentlichkeitsarbeit/Infomaterial/Faltblaetter/Faltblaetter__node.html__nnn=true]
sowie das Angebot des ULD [http://www.datenschutzzentrum.de/ldsh/infomaterial.htm].

[397] Was Lutterbeck in: Bäumler, Der neue Datenschutz, S. 258 im Jahr 1998 auf die Datenschutzbeauftragten gemünzt hatte, gilt auch heute zwölf Jahre später immer noch für die meisten Aufsichtsbehörden.

[398] Weichert in: Bäumler, Der neue Datenschutz, S. 225.

[399] Vgl. Brönneke/Brobowski in: E-Privacy, S. 141 ff.

[400] Schaar in: Bäumler, E-Privacy., S. 67; Weichert in: Bäumler, Der neue Datenschutz, S. 229.

weil den Aufsichtsbehörden die personellen und sachlichen Ressourcen fehlen. Wie begrenzt diese auch immer sein mögen, Ressourcen können und müssen eingeteilt und eingesetzt werden. Mit welchen Prioritäten und in welchen Bündnissen ein effektiver Verbraucherdatenschutz von den Aufsichtsbehörden betrieben wird, bestimmen letztlich die Datenschutzbeauftragten bzw. die Leiter der Aufsichtsbehörden.[401] Kein Zweifel, die Situation der Aufsichtsbehörde ist beklagenswert, aber umgekehrt kann gilt auch, dass „mehr als nichts auch mit geringen Ressourcen immer möglich ist“.

[401] Vgl. Lutterbeck in: Bäumler, Der neue Datenschutz, S. 258.

# 11 Maßnahmen zur Verbesserung der Transparenz

## 11.1 Aufsichtsbehörde

Die Verletzung datenschutzrechtlicher Informationspflichten ist im geltenden Datenschutzrecht nur eingeschränkt sanktioniert. Zwar „kontrolliert“ die *Aufsichtsbehörde* die Ausführung der Datenschutzbestimmungen nach § 38 Abs. 1 Satz 1 BDSG, jedoch sind ihre Befugnisse bei Feststellung eines Verstoßes gegen Datenschutzbestimmungen sehr beschränkt. Sie kann den Verstoß der zur Verfolgung oder Ahndung zuständigen Stelle anzeigen sowie – bei schwerwiegenden Verstößen – die Gewerbeaufsicht zur Durchführung gewerberechtlicher Maßnahmen unterrichten (§ 38 Abs. 1 Satz 5 BDSG). Über besondere Eingriffsmöglichkeiten verfügt die Aufsichtsbehörde nach § 38 Abs. 5 BDSG nur, wenn die Anforderungen des technischen Datenschutzes unzureichend umgesetzt sind. Zu diesen Anforderungen zählen die Informationspflichten jedoch nicht.[402]

### 11.1.1 Verfolgung und Ahndung

Mit einem *Bußgeld* sanktioniert das BDSG in § 43 Abs. 1 Nr. 8 BDSG lediglich die nicht richtige oder nicht vollständige Benachrichtigung des Betroffenen nach § 33 Abs. 1 BDSG. Ferner wird in § 43 Abs. 1 Nr. 3 BSDG der unterbliebene oder unrichtige Hinweis auf das Widerspruchsrecht nach § 28 Abs. 4 Satz 2 BDSG mit einem Bußgeld belegt. Datenschutzrechtlich nicht ausdrücklich ist jedoch die Verletzung sonstiger Informationspflichten wie bspw. im Fall einer Erhebung beim Betroffenen nach § 4 Abs. 3 BDSG sanktioniert.[403] Entsprechendes könnte für den Verstoß gegen Hinweispflichten bei einer Videoüberwachung oder im Zusammenhang mit dem Einsatz von Chipkarten gelten. Ansonsten bliebe der Betroffene im nicht-öffentlichen Bereich auf Ansprüche aus Vertrag oder Delikt angewiesen.

Der Auffangtatbestand des § 43 Abs. 2 Nr. 1 BDSG hat für die Verletzung der Informationspflichten praktisch keine Bedeutung, weil dieser nur das unbefugte Erheben oder Verarbeiten personenbezogener Daten erfasst und damit für die Verletzung von Informationspflichten kaum in Betracht kommt. Einschlägig kann dieser Tatbestand jedoch werden, wenn der Betroffene vor seiner Einwilligung nach § 4 a Abs. 1 BDSG über den Zweck der Erhebung, Verarbeitung oder Nutzung unzureichend unterrichtet worden ist. In diesem Fall ist die Einwilligung unwirksam und eine Erhebung oder Verarbeitung erfolgt nach § 43 Abs. 2 Nr. 1 BDSG „unbefugt“. Ein vergleichbarer Fall liegt vor, wenn eine Datenverarbeitung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG deshalb unzulässig ist, weil der Betroffene nicht hinreichend informiert wurde und dadurch seine schutzwürdigen Interessen überwiegen. Eine Strafandrohung setzt nach § 43 Abs. 1 BDSG allerdings eine vorsätzliche Handlung mit Bereicherungs-

[402] Walz in: Simitis, BDSG, § 38, Rn. 38 ff.; Sokol in: Simitis, BDSG, § 4, Rn. 57 ff.

[403] Sokol in: Simitis, BDSG, § 4, Rn. 57 f.

bzw. Schädigungsabsicht voraus. Weitere Straftatbestände, die durch die Verletzung von Informationspflichten verletzt sein könnten, sind nicht ersichtlich.

### 11.1.2 Einschaltung der Gewerbeaufsicht

Beschränkt sind die Möglichkeiten der Aufsichtsbehörde, mit Hilfe der Gewerbeaufsicht den Verstoß gegen Informationspflichten zu sanktionieren. Zunächst verlangt § 38 Abs. 1 Satz 5 BDSG bereits für eine Unterrichtung der Gewerbeaufsicht durch die datenschutzrechtliche Aufsichtsbehörde einen „*schwerwiegenden Verstoß*“, d.h. mindestens die Androhung einer Sanktion in Form einer Ordnungswidrigkeit, wenn nicht sogar die Verwirklichung eines Straftatbestandes.

Selbst wenn diese Voraussetzungen zu bejahen sind, hat die Aufsichtsbehörde jedoch keinen Einfluss auf die Ermessensausübung der Gewerbeaufsicht bei der Prüfung und Anordnung gewerberechtlicher Maßnahmen. Das Fehlen jeder Rechtsprechung in diesem Bereich belegt die geringe praktische Bedeutung der gewerberechtlichen Einwirkungsmöglichkeit.[404]

Gewerberechtliche Anordnungen wie bspw. die Untersagung eines stehenden Gewerbes setzen ferner nach § 35 Abs. 1 Satz 1 GewO Tatsachen voraus, welche die *Unzuverlässigkeit* des Gewerbetreibenden oder einer mit der Leitung des Betriebes beauftragten Person darzulegen geeignet sind. Die Entscheidung über die gewerberechtliche Unzuverlässigkeit ist eine Prognoseentscheidung, die sich auf die Tatsache eines als Ordnungswidrigkeit oder Straftat sanktionierten Verhaltens stützen kann, zumindest aber an ein Verhalten knüpft, dass die Annahme einer fehlenden Eignung zur Durchführung des Gewerbes auch in der Zukunft rechtfertigt.

### 11.1.3 Benachrichtigung des Betroffenen

Als „schärfstes Schwert“ verbleibt der Aufsichtsbehörde damit ein Instrument, das auf den ersten Blick stumpf und unscheinbar wirkt. § 38 Abs. 1 Satz 5 BDSG ermächtigt die Aufsichtsbehörde, „die Betroffenen“ über den Verstoß gegen datenschutzrechtliche Bestimmungen zu unterrichten. Die *Betroffenenunterrichtung* kann in der Praxis die ohnehin bestehende Schieflage im informationellen Gleichgewicht zwischen verantwortlicher Stelle und Betroffenen korrigieren helfen.

Im Fall einer Einwilligung hat der Betroffene der verantwortlichen Stelle einen Vorschuss an Vertrauen in die Rechtmäßigkeit ihrer Datenverarbeitung eingeräumt. Dieses Vertrauen wird durch den Datenschutzverstoß missbraucht und der Betroffene muss seine Konsequenzen ziehen können. Voraussetzung ist allerdings, dass er von dem Datenschutzverstoß durch die Aufsichtsbehörde in Kenntnis gesetzt wird.

Erfolgt die Datenverarbeitung auf einer gesetzlichen Grundlage, dann ist der Betroffene 1ebenfalls nicht ohne Reaktionsmöglichkeiten auf den Normverstoß. Zum einen verbleiben

[404] Walz in: Simitis, BDSG, § 38, Rn. 47.

dem Betroffenen vertragsrechtliche Ansprüche, weil die Verletzung von Informationspflichten einen Verstoß gegen zumindest nebenvertragliche Pflichten darstellt.[405] Zudem wird der Betroffene von zukünftigen Vertragsabschlüssen Abstand nehmen können.

Angesichts der Sorge von Unternehmen vor einem Imageschaden, kann der Möglichkeit des Betroffenen, die *Öffentlichkeit* über den Normverstoß des Unternehmens zu informieren, eine präventive Wirkung zukommen. Eine solche Information durch die Aufsichtsbehörde könnte zulässig sein, wenn wegen der Vielzahl der Betroffenen die Aufsichtsbehörde keine andere Möglichkeit hat, als sie über den Weg in die Öffentlichkeit über den Datenschutzverstoß zu informieren. Ausdrücklich an die Öffentlichkeit wendet sich der Tätigkeitsbericht, den die Aufsichtsbehörde nach § 38 Abs. 1 Satz 6 BDSG alle zwei Jahre zu veröffentlichen hat. In der Praxis üben die Aufsichtsbehörden bei der namentlichen Nennung eines Unternehmens angesichts der Rechtsprechung über Verbraucherwarnungen große Zurückhaltung.

Denkbar ist auch die Unterrichtung relevanter gesellschaftlicher Gruppen der Selbstorganisation der für den Verstoß verantwortlichen Stelle wie dem Berufsverband der verantwortlichen Stelle oder aber Berufskammern, die ihrerseits ein Interesse daran haben, Schaden von ihrer Branche abzuwenden, und Datenschutzverstöße „schwarzer Schafe“ im Rahmen der verbandlichen Selbstregulierung zu vermeiden.

Der Betroffene kann sich schließlich an Organisationen des Verbraucherschutzes und des Datenschutzes wenden, die über wirksamere Möglichkeiten zur Information der Öffentlichkeitsarbeit verfügen als er selbst.

### 11.1.4 AGB-Kontrolle

Ob und inwieweit die Unterlassung einer datenschutzrechtlich gebotenen Unterrichtung oder Benachrichtigung Gegenstand einer Verbraucherschutzklage nach § 1 des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagegesetz – UKlaG)[406] sein kann, ist davon abhängig, ob und in welchem Umfang der Verwender die Erfüllung der datenschutzrechtlichen Informationspflichten „als Vertragsbedingungen“ nach § 305 Abs. 1 Satz 1 BGB vorformuliert. Gegen eine Bewertung als AGB spricht der Charakter der datenschutzrechtlichen Informationspflichten als selbständige vom Vertrag zwischen Verwender und Kunden unabhängige Verpflichtung des Verwenders in seiner Eigenschaft als datenschutzrechtlich Verantwortlicher.

Das Unterlassungsklagegesetz bietet aber in § 2 Abs. 1 auch die Möglichkeit eines allgemeinen Unterlassungsanspruches gegen verbraucherschutzwidrige Praktiken gegen denjenigen, der in anderer Weise als durch Verwendung oder Empfehlung von Allgemeinen Geschäftsbedingungen Vorschriften zuwiderhandelt, die dem Schutz der Verbraucher dienen. Um welche als „Verbraucherschutzgesetze“ legal definierte Vorschriften es sich dabei handelt, ist einem – nicht abschließenden („insbesondere“) – Katalog zu entnehmen, der jedoch

[405] Siehe oben Kap. 2. Sowie Sokol in: Simitis, BDSG, § 4, Rn. 57.

[406] Art. 3 des Gesetzes über die Modernisierung des Schuldrechts.

weder einen Hinweis auf die datenschutzrechtlichen Vorschriften allgemein noch auf die datenschutzrechtlichen Informationspflichten im Besonderen enthält.[407]

Für eine solche Einordnung der datenschutzrechtlichen Informationspflichten spricht, dass sie den Betroffenen wie andere Informationspflichten auch in seiner Eigenschaft als Verbraucher über Kommunikationsbedingungen des Verwenders unterrichten. Aus der Perspektive der Daten verarbeitenden Stelle ist die Erhebung und Verarbeitung personenbezogener Kundendaten nur ein Baustein eines umfassenden Marketingkonzeptes, mit dem der Verbraucher als Kunde gewonnen und gehalten werden soll. Unter dieser Voraussetzung ist eine Trennung zwischen datenschutz- und verbraucherrechtlichen Informationspflichten künstlich. Die Einbeziehung der datenschutzrechtlichen Informationspflichten in den Begriff der Verbraucherschutzgesetze im Sinne von § 2 Abs. 2 UKlaG ist daher grundsätzlich gerechtfertigt.

Aktivlegitimiert sind nach §§ 3 ff. UKlaG qualifizierte Verbraucherschutzvereine, rechtsfähige Vereine zur Förderung gewerblicher Interessen und die Industrie- und Handelskammern. Datenschutzorganisationen führt das Gesetz zwar nicht ausdrücklich auf, ihre Anerkennung nach § 4 UKlaG als Verbraucherschutzverband ist aber auch nicht ausgeschlossen.

## 11.2 Wettbewerbsrecht

Denkbar ist schließlich auch eine Sanktionierung von Verstößen gegen datenschutzrechtliche Informationspflichten als Verletzung der „guten Sitten“ im Wettbewerb nach § 1 UWG. Verstöße gegen das Wettbewerbsrecht können allerdings nicht von den Betroffenen selbst, sondern nur von den Wettbewerbern geahndet werden.

Voraussetzung eines derartigen wettbewerbsrechtlichen Anspruches ist, dass die Unterlassung von datenschutzrechtlich gebotenen Informationspflichten irgendwie geartete Auswirkung auf den Wettbewerb hat.[408] Die datenschutzrechtliche Informationspflicht muss nach § 4 Nr. 11 UWG dazu bestimmt sein, „im Interesse der Marktteilnehmer das Marktverhalten zu regeln“. Im Wettbewerb zwischen den für eine Datenverarbeitung verantwortlichen Stellen wird dies regelmäßig angenommen werden können, weil die dem Betroffenen gebotenen Informationen über die Verarbeitung seiner Daten bspw. über die Kategorien möglicher Empfänger diesen in seiner Entscheidung für oder gegen eine wirtschaftlich relevante Kommunikation mit der Daten verarbeitenden Stelle beeinflusst.[409] Es ist der eigentliche Sinn und Zweck der datenschutzrechtlichen Informationspflichten, den Betroffenen nicht nur einen Ausgleich für die von ihnen nach § 28 f. BDSG hinzunehmende Datenverarbeitung, sondern

---

[407] Aus diesem Grund schlagen Roßnagel/Pfitzmann/Garstka, Modernisierung, S. 203 ff. eine Präzisierung der einschlägigen Bestimmungen vor.

[408] Vgl. zum folgenden Hoeren/Lütkemeier, Unlauterer Wettbewerb durch Datenschutzverstöße, in: Sokol (Hrsg.), Neue Instrumente im Datenschutz, Düsseldorf 1999, S. 115.

[409] Das OLG Düsseldorf hat dies für die Hinweispflicht auf das Widerspruchsrecht nach § 28 Abs. 4 BDSG verneint. Für die Unterrichtungspflicht § 4 Abs. 1 TDDSG ablehnend LG München, DuD 2005, 53: LG Essen, DuD 2005, 312.

ihnen auch Entscheidungsfähigkeit in der Auswahl ihrer Kommunikationspartner zu verschaffen, denen sie ihre Daten zu überlassen bereit sind.[410]

Wissensdefizite über die Verarbeitung ihrer Daten sind angesichts der Bedeutung des Datenschutzes als Akzeptanzfaktor auch wettbewerbsbezogen – jedoch ist die Rechtsprechung hierzu uneinheitlich.[411] Der Wettbewerbsbezug besteht, weil die Kenntnis der konkreten Verarbeitungsbedingungen ihrer Daten das Verhalten der (potentiell) Betroffenen in der Entscheidung zur Kommunikation sowie der Auswahl eines Unternehmens als Anbieter einer Ware oder Dienstleistung negativ beeinflussen kann. Die Verletzung von datenschutzrechtlichen Informationspflichten ist unter diesen Voraussetzungen als ein *Vorsprung durch Rechtsbruch* zu werten. Angesichts der uneinheitlichen Rechtsprechung ist jedoch eine Klarstellung durch den Gesetzgeber notwendig.[412]

## 11.3 Förderung

Neben repressiven Regelungsmechanismen, mit deren Hilfe den datenschutzrechtlichen Informationspflichten zur Wirksamkeit verholfen werden kann, kann den datenschutzrechtlichen Informationspflichten auch durch präventive Mechanismen einer proaktiven Förderung eine größere Wirkung verschafft werden.

### 11.3.1 Selbstregulierung

Eine Durchsetzung datenschutzrechtlicher Informationspflichten kann bspw. durch eine verbandliche Selbstregulierung nach § 38 a Abs. 1 BDSG unterstützt werden. Danach können Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, „Entwürfe für Verhaltensregelungen zur Förderung der Durchführung von datenschutzrechtlichen Regelungen“ der zuständigen Aufsichtsbehörde unterbreiten, die diese Entwürfe auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht überprüft.[413]

Verhaltsregelungen nach § 38 a BDSG können das geltende Datenschutzrecht nicht unterschreiten, ihm aber durch flankierende Hilfestellungen und innerverbandliche Sanktionen zu seiner wirksameren Durchsetzung verhelfen. Allerdings sind Verhaltensregelungen nicht bekannt, die ihre Mitglieder explizit zur Befolgung datenschutzrechtlicher Informationspflichten anhalten.

Spielräume für eine unterstützende Wirkung durch Selbstregulierung bestehen aber auch außerhalb einer förmlichen Anerkennung nach § 38 a BDSG. Ein Beispiel für einen derartigen Selbstregulierungsmechanismus sind die „Qualitätskriterien für Internet-Angebote“ der

---

[410] Dies wird übersehen bspw. von U. Heil, RDV 2004, 205, 210.

[411] Die Rechtsprechung ist nicht einheitlich: einerseits LG Stuttgart, DuD 1999, 295; LG Mannheim, DuD 1996, 363; OLG Karlsruhe DuD 1997, 352, andererseits ablehnend.

[412] Vgl. auch Roßnagel/Pfitzmann/Garstka, Modernisierung, S. 204 f.

[413] Zu § 38 a BDSG siehe: Bizer in: Simitis, BDSG, § 38 a.

Initiative D21 vom 15. April 2005, zu deren Umsetzung sich Unternehmen im Rahmen einer „Anbietererklärung“ selbstbindend bereit erklären können.[414] Für die Gestaltung der Privcy Policy wird auf den privacy protector der OECD[415] verwiesen. Eine systematische Untersuchung über die Wirksamkeit dieser und vergleichbarer Regelungen fehlt bislang.

Betätigungsfelder für selbstregulative Initiativen bietet auch die verbandliche Festlegung von Standards für die Darstellung von Hinweisschildern und Informationen für die Betroffenen. Ein Beispiel ist die Entwicklung eines einheitlichen Piktogramms durch das Deutsche Normungsinstitut e.V. Ende 2004. Es wird den verantwortlichen Stellen angeboten, damit sie ihrer gesetzlichen Verpflichtung gemäß § 6 b Abs. 2 BDSG nachkommen können, die Videoüberwachung öffentlicher Räume zu kennzeichnen.[416] Den an der Entwicklung des Piktogramms beteiligten Unternehmen lag daran, ein einheitliches Symbol zu entwickeln, das für die Betroffenen einen hohen Wiedererkennungswert hat. Bislang hat das Symbol allerdings noch keine große Verbreitung gefunden.

### 11.3.2 Datenschutz-Audit

Informationen über die Verarbeitung seiner Daten können für den Betroffenen unmittelbar von Bedeutung sein, wenn er die Möglichkeit hat, zwischen mehreren Anbietern bzw. Daten verarbeitenden Stellen auszuwählen und auf diese Weise seine Datenschutz-Motivation ein Entscheidungskriterium für die Auswahl seines Anbieters umzusetzen. Transparenz über die Bedingungen der Verarbeitung personenbezogener Daten ist unter diesen Voraussetzungen ein *positiver Wettbewerbsfaktor*, dessen Vernachlässigung für das Unternehmen zu strategischen Nachteilen am Markt führen kann.

Aber auch ohne eine unmittelbare Wettbewerbssituation können Informationspflichten die Wirksamkeit von Datenschutzregelungen steigern. Letztlich erzeugen die von einem Unternehmen an die Verbraucher adressierten Informationen gegenüber diesen eine Art kommunikativer Verbindlichkeit, deren Nichterfüllung Enttäuschung und sensible Reaktionen der Öffentlichkeit nach sich ziehen kann.

Verstöße gegen eigene Zusagen können für das Unternehmen bzw. einer Branche zu einem Verlust an Ansehen führen, der als Imageschaden mittel- oder langfristig den Ruf des Unternehmens, unter Umständen einer Branche, auf jeden Fall aber den Wert einer Marke beeinträchtigen kann. Die Existenz derartiger negativer Trends lassen sich aus einer Reihe von Umfragen der letzten Jahre ablesen.[417]

---

[414] http://www.internet-guetesiegel.de/docs/D21_Qualitaetskriterien_2005.pdf.

[415] Siehe Carblanc, Building bridges between different approaches of privacy in: FG Büllesbach 2002, S. 316 ff. (http://www.alfred-buellesbach.de/PDF/30_Carblanc.pdf).

[416] Bizer in: Simitis, BDSG, § 6 b, Rn. 69; s.a. http://www.heise.de/newsticker/meldung/47148.

[417] Nachweise bei Bizer, Datenschutzrecht in: Schulte, Handbuch des Technikrechts 2003, S. 576 f. Vgl. Opaschowski, DuD 2001, 678; ders., Datenschutz in der Gesellschaft in: Roßnagel, HdBDatSchR, Kap. 2.1, Rn. 49 ff.

Letztlich stellen Art, Umfang und Gestaltung der Unterrichtung einen „*datenschutzrechtlichen Lackmustest*“ dar, welche Wertschätzung der Anbieter der informationellen Selbstbestimmung seinen Kunden in Wirklichkeit einräumt.

Vor diesem Hintergrund verschiebt sich das Problem von der bloßen Normbefolgung zur Frage ihrer Vertrauenswürdigkeit. Die zentrale Frage ist, welche vertrauenswürdige Institution den für die Datenverarbeitung verantwortlichen Stellen die Rechtskonformität ihrer Datenschutz-Policy, insbesondere die Vollständigkeit und Rechtmäßigkeit ihrer Informationen bestätigt.

Einen Lösungsansatz bietet das Datenschutzaudit. Nach § 9 a BDSG können datenverarbeitende Stellen ihr Datenschutzkonzept durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen und das Ergebnis dieser Prüfung veröffentlichen. Bestandteil eines solchen Datenschutzkonzeptes wäre insbesondere die Einhaltung und Umsetzung der für die Stelle einschlägigen Datenschutzvorschriften und damit auch der datenschutzrechtlich gebotenen Informationspflichten. Allerdings fehlt noch immer das für das Datenschutzaudit erforderliche Ausführungsgesetz.

In eine vergleichbare Richtung zielt das Konzept des Datenschutz-Gütesiegels nach § 4 Abs. 2 Satz 1 LDSG Schleswig-Holstein, das in eine Verpflichtung der Landesbehörden, sich vorrangig für förmlich geprüfte „Produkte“ zu entscheiden, eingebettet ist.[418] Maßstab der Prüfung ist die Vereinbarkeit mit den „Vorschriften über den Datenschutz und die Datensicherheit“, so dass die Erfüllung der datenschutzrechtlichen Informationspflichten ein integraler Bestandteil dieser Prüfung ist. Im Unterschied zur Bundesregelung besteht in Schleswig-Holstein nicht nur eine Ausführungsverordnung[419], sondern es liegen auch Erfahrungen aus über 30 Gütesiegelverfahren vor.[420]

## 11.4 Fazit

Den datenschutzrechtlichen Informationspflichten kommt für einen marktwirtschaftlichen Datenschutz eine *zentrale Bedeutung* zu. Transparenz über die Verarbeitungsbedingungen personenbezogener Daten ist die maßgebliche Voraussetzung einer Verbindung zwischen informationeller Selbstbestimmung und Entscheidungsfreiheit des (potentiell) von einer Datenverarbeitung Betroffenen zwischen Anbietern von Waren und Dienstleistungen.

Allerdings weist das Recht der datenschutzrechtlichen Informationspflichten *strukturelle Schwächen* auf. Das Recht der Informationspflichten findet sich in verschiedenen Regelungsorten im BDSG und ist zersplittert. Auf der materiellen Ebene fehlt trotz eindeutiger

---

[418] Bizer/Körffer, VuM 2006, 24 ff.; Bäumler, DuD 2002, 325 ff.; sowie die Beiträge von Diek, Gütesiegel nach dem schleswig-holsteinischen Landesdatenschutzgesetz, und Hansen/Probst, Datenschutzgütesiegel aus technischer Sicht: Bewertungskriterien des schleswig-holsteinischen Datenschutzgütesiegels in: Bäumler/v.Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil 2002, S. 163 ff.

[419] Landesverordnung über ein Datenschutzaudit vom 3. April 2001, GVBl. S. 51.

[420] Siehe www.datenschutzzentrum.de/guetesiegel/

Parallelen eine Verzahnung mit dem Recht des Verbraucherschutzes (AGB-Recht, Fernabsatz, E-Commerce). Nicht ausreichend sind die Anforderungen an die *Gestaltung* datenschutzrechtlicher Informationspflichten, die entweder fehlen oder mit anderen vergleichbaren Regelungen nicht abgestimmt sind.

Defizitär ist vor allem die *Durchsetzung* datenschutzrechtlicher Informationspflichten: Während die Verletzung von Informationspflichten im Zusammenhang mit einer datenschutzrechtlichen Einwilligung ihre Unwirksamkeit nach sich zieht, fehlen adäquate Mechanismen, wenn sich die Datenverarbeitung auf eine gesetzliche Grundlage stützt. Weder ist die Verletzung datenschutzrechtlicher Informationspflichten einheitlich als Ordnungswidrigkeit sanktioniert noch verfügen die Aufsichtsbehörden über ausreichende Befugnisse, um die Einhaltung dieser Informationspflichten im Einzelfall durchsetzen zu können.

Ein wirksamer, aber in der Praxis wenig genutzter Mechanismus besteht in der Möglichkeit der Aufsichtsbehörde, den *Betroffenen* über den Tatbestand der Verletzung von Informationspflichten zu informieren. Praktisch bewähren müssen sich die Möglichkeiten, die Verletzung datenschutzrechtlicher Informationspflichten mit Hilfe von Unterlassungsklagen gegen Allgemeine Geschäftsbedingungen oder im Wege wettbewerbsrechtlicher Unterlassungsklagen zu ahnden. Ob und inwieweit sich die Umsetzung datenschutzrechtlicher Informationspflichten im Wege der *Selbstregulierung* verbessern lassen, wird sich noch erweisen müssen. Als ein insgesamt taugliches Instrument hat sich bereits das Instrument des Datenschutz-Gütesiegels erwiesen.

# 12 Verbesserung durch Selbstregulierung und Datenschutzaudit

## 12.1 Selbstregulierung

In einer miteinander verflochtenen, globalen Wirtschaft gilt die Festlegung der Unternehmen und Verbände auf Mindeststandards im Wege der Selbstregulierung als eine Erfolg versprechende Alternative gegenüber zeitaufwendigen zwischenstaatlichen Prozessen der Koordination, in denen nationale oder kontinentale Standards angepasst werden.[421] Als Vorbild für eine solche Deutung dient die internationale *Standardisierung der Technik* bzw. die Entwicklung des Internets als offenes Netz. Optimistisch fortgeschrieben kann sich am Ende einer solchen Entwicklung ein Welt-Datenschutzrecht etablieren, das nicht über Staaten, wohl aber über die Unternehmen als Anbieter von Dienstleistungen und Waren weltweit Anerkennung findet.[422]

### 12.1.1 Erwartungen an die Selbstregulierung

Aus der Sicht des Staates kann die Nutzung von Selbstregulierungspotentialen eine entlastende Wirkung entfalten; insbesondere kann ein Mechanismus der Selbstverpflichtung die *Durchsetzungskosten* staatlichen Rechts minimieren sowie das Vertrauen der Kunden und Nutzer in die Integrität der Datenverarbeitung und damit in die Informationsgesellschaft stärken.[423] Insbesondere international tätigen Unternehmen bieten verbindlich im Wege der Selbstregulierung festgelegte Standards Vorteile gegenüber den häufig heterogenen normativen Standards der Nationalstaaten.

Andererseits lässt sich nicht verhehlen, dass es selbstregulativen Datenschutzstandards häufig an ausreichenden Mechanismen fehlt, die den Betroffenen auch eine Durchsetzung der kodifizierten Rechte gewährleisten.[424] Auch muss berücksichtigt werden, dass das Koordinationsinteresse von gegeneinander im Wettbewerb befindlichen Unternehmen nur gering ausgeprägt ist. Zudem fehlt es den einschlägigen Verbänden an einer ausreichenden *Durchsetzungsmacht* gegenüber ihren Mitgliedern, insbesondere wenn sie mit anderen Verbänden konkurrieren. Schließlich stellt sich den Unternehmen in einem durchregulierten Umfeld wie dem Datenschutz die Frage, welche Vorteile eine Verständigung mit den Konkurrenten über eine Auslegung unbestimmter Rechtsbegriffe bieten kann. Häufig scheinen die Anwendungskosten des staatlichen Datenschutzrechts geringer zu sein als die einer verbandlichen

---

[421] Bspw. Jacob/Heil in: FG Büllesbach, S. 213 ff.; siehe zum Folgenden Bizer in: Schulte, S. 597 ff.

[422] Vgl. bspw. die Aktivitäten des Global Business Dialogue, Protection of Personal Data, 26. September 2000.

[423] Hoffmann-Riem, AöR 123 (1998), S. 537; Roßnagel/Pfitzmann/Garstka. Modernisierung, S. 153 mwN.; BT-Enquete, BT-DrS. 14/11004, S. 17 f.

[424] Jacob/Heil, in: FG Büllesbach, , S. 213 ff.; Bizer in: Simitis, BDSG, § 38 a, Rn. 13.

Koordination, einschließlich der Etablierung entsprechender Mechanismen ihrer Durchsetzung.[425]

### 12.1.2 Mechanismen der Selbstregulierung

Das deutsche Datenschutzrecht hat Mechanismen der Selbstregulierung in Umsetzung des Art. 27 EG-Datenschutzrichtlinie vor allem in drei Regelungen etabliert. Im Rahmen der Regelungen über den *Datentransfer in Drittstaaten* kann die zuständige Aufsichtsbehörde im Einzelfall eine Übermittlung in einen Drittstaat auch ohne die Feststellung eines angemessenen Schutzniveaus genehmigen, wenn sich ausreichende Garantien zum Schutz des Persönlichkeitsrechts „aus Vertragsklauseln oder verbindlichen Unternehmensregelungen" ergeben.[426] Auf die Probleme des Fehlens von Regelungen zu Lasten des Verbraucherdatenschutzes ist bereits oben hingewiesen worden (s.o. S. 173 f.).

Weiterhin können *Berufsverbände* und andere Vereinigungen gem. § 38 a BDSG Entwürfe für Verhaltensregelungen „zur Förderung der Durchführung von datenschutzrechtlichen Regelungen" der zuständigen Aufsichtsbehörde zur Prüfung unterbreiten, die diese auf die Vereinbarkeit mit dem geltenden Datenschutzrecht hin überprüft.[427] Die Praxis zeigt, dass sich verbandsangehörige Unternehmen aus Gründen des Wettbewerbes regelmäßig nur auf das niedrigste Niveau der staatlichen Regelung verständigen. Unter dieser Voraussetzung besteht keine Notwendigkeit einer gesonderten verbandlichen Regelung, weil diese lediglich den Normbefehl des Gesetzes wiederholen würde. Eine innerverbandliche Sanktionierung von Datenschutzverstößen bspw. bei einer zweckwidrigen Verwendung von Kundendaten ist eine nur theoretische Alternative. Die Mitglieder eines Verbandes haben regelmäßig kein Interesse, sich dem Risiko einer verbandsinternen Abstrafung auszusetzen, die ihnen wirtschaftliche Nachteile und den Wettbewerbern wirtschaftliche Vorteile vermittelt.

Der dritte Anwendungsfall betrifft das so genannte *Medienprivileg* nach § 41 Abs. 1 BDSG, wonach die Länder mit Rücksicht auf Art. 5 Abs. 1 GG in ihrer Gesetzgebung vorsehen müssen, dass die Presse und Medienunternehmen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im journalistisch-redaktionellen Bereich den §§ 5, 9 und 38 a BDSG „entsprechende Regelungen" zur Anwendung kommen.[428] Der Presserat hat mittlerweile einen Datenschutzkodex verfasst, dessen Wirksamkeit aber noch der Bewährung bedarf. Im Übrigen ist das Medienprivileg für den Verbraucherdatenschutz ohne Bedeutung.

Vorschläge und Konzepte zur Stärkung des Datenschutzes durch Mechanismen der Selbstregulierung bestehen.[429] Die rahmenrechtlichen Voraussetzungen sind mit § 38 a BDSG

---

[425] Zurückhaltend Bizer DuD 2001, 126.

[426] Vgl. Büllesbach/Höss-Löw DuD 2001, 135 ff. Brühann in: FG Büllesbach 2002, S. 289, 293 ff.

[427] Beispiele wären die Bereiche des Direktmarketings oder der Versicherung, Walz, Selbstkontrolle versus Fremdkontrolle in: FS Simitis 2000, S. 461.

[428] Näher Walz in: FG Büllesbach 2002 S. 301, 304; Walz in: Simitis, BDSG, § 41.

[429] Systematisch aufgearbeitet bei Roßnagel in: ders, HdBDatSchR, Kap. 3.6, Rn. 106 ff.

gegeben.[430] Die Praxis der verbandlichen Selbstregulierung bleibt aber aus den oben genannten Gründen erheblich hinter den Erwartungen zurück. Die Erwartung, der Verbraucherdatenschutz würde im Wege einer verbandlichen Regelungsstruktur einen höheren Wirksamkeitsgrad erreichen, ist bisher durch die Praxis widerlegt.

### 12.1.3 Betrieblicher Datenschutzbeauftragter

Eine erheblich größere Bedeutung für die Etablierung von Selbstregulierung hat der betriebliche Datenschutzbeauftragte. Er ist zwar gesetzlich vorgesehen und ist insofern keine Einrichtung der Selbstregulierung, sondern der betrieblichen Selbstorganisation (s.o. S. 158). Die betrieblichen Datenschutzbeauftragten haben zentrale Bedeutung für den Verbraucherdatenschutz in solchen Unternehmen, die im Massengeschäft Verbraucherdaten verarbeiten und in einem hohen Maß von dem Vertrauen ihrer Kunden und damit der Verbraucher abhängig sind.[431] Im Interesse des Verbraucherdatenschutzes ist die Stellung des betrieblichen Datenschutzbeauftragten im Unternehmen zu stärken und auszubauen.[432] Dies betrifft sowohl seine Kompetenzen im Unternehmen als auch seine Ausstattung.

## 12.2 Datenschutzaudit

Mit dem Datenschutzaudit wird der moderne Datenschutz um ein marktwirtschaftliches Instrument erweitert. Die Zertifizierung zielt auf die Prämierung der in den Datenschutz investierten Aufwendungen, mit der im Wettbewerb geworben werden kann.[433] Auf diese Weise sollen sich insbesondere Investitionen in eine datenschutzkonforme Technikgestaltung für die Unternehmen lohnen. Gleichzeitig profitieren die Verbraucher, weil durch die Zertifizierung eine Markttransparenz hergestellt wird. Voraussetzung ist allerdings, dass die Zertifizierung durch unabhängige Gutachter erfolgt, deren Arbeit durch eine vertrauenswürdige Stelle gegenüber den Verbrauchern bestätigt wird.

Nach der Bundesregelung zum *Datenschutzaudit* in § 9 a BDSG können Anbieter von Datenverarbeitungssystemen und -programmen sowie Daten verarbeitende Stellen „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“. Die Regelung der näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter bleibt einem besonderen Gesetz überlassen, das der Bund bislang aber nicht verabschiedet hat. Die Vorlage eines Ausführungsgesetzes zum Datenschutzaudit

---

[430] Kommentierung Bizer in: Simitis, BDSG, § 38 a.

[431] Vgl. bspw. Königshofen in: Bäumler, Der neue Datenschutz, S. 230 ff.

[432] Bspw. BvD, DuD 2005, 272 ff.

[433] Bizer in: Schulte, S. 595

wurde von der letzten Bundesregierung für die 15. Legislaturperiode angekündigt, ohne dass ein Entwurf vorgelegt worden wäre.[434]

### 12.2.1 Datenschutz-Audit von Verfahren

Von den Landesgesetzgebern, die neben dem Bund eine Regelung für ein Datenschutzaudit im Rahmen ihrer Gesetzgebungskompetenz[435] in das jeweilige Landesdatenschutzgesetz aufgenommen haben, hat *Schleswig-Holstein* für den öffentlichen Bereich eine Ausführungsregelung erlassen.[436] Nach dieser Regelung können öffentliche Stellen des Landes ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) prüfen und beurteilen lassen.[437] Methodische Elemente dieses Verfahrens sind eine Bestandsaufnahme, die Festlegung von Datenschutzzielen sowie die Einrichtung eines Managementsystems, die abschließend in einer Datenschutzerklärung zusammengefasst werden. Abgeschlossen wird das Verfahren durch ein zu veröffentlichendes Kurzgutachten des Datenschutzzentrums und der Verleihung eines Auditzeichens. In Schleswig-Holstein sind bereits zahlreiche Auditverfahren abgeschlossen worden.[438]

Von diesem behördlichen Beispiel abgesehen, gewinnen die Zertifizierungen von Verfahren in der Wirtschaft eine immer größere Bedeutung. Sie sind regelmäßig Bestandteile des Risikomanagments bzw. der Compliance-Strategie der Unternehmen, um in einem Soll-Ist-Vergleich den Stand der Organisation zu prüfen.[439] Eine Reihe von Unternehmen prüft bereits heute ihre Datenschutzorganisation im Rahmen unternehmenseigener Audits, wenngleich nach Verfahren, die für das Unternehmen auf der Basis bestehender Auditierungsschemata entwickelt worden sind.[440] Aus Effizienzgründen spielt die Anpassung an anerkannte und im Unternehmen praktizierte Managementsysteme eine große Rolle.[441]

Für den Verbraucherdatenschutz müssen derartige Auditverfahren erst noch fruchtbar gemacht werden. Eine Nachfrage insbesondere nach einem von den Aufsichtsbehörden anerkannten Prüfungsschema ist festzustellen. Erste Ansätze liegen in Form von Bausteinen vor,

---

[434] Staatssekretär Körper, BT-Prot. 14/248, S. 14 263 (D) vom 4. Juli 2002; siehe aber die Entschließung aus der 14. Legislaturperiode, BT-Dr S. 14/9709.

[435] Bizer/Petri DuD 2001, 97 ff.

[436] Bäumler, DuD 2002, 326; Behrendt, DuD 2006, 20 ff. Mittlerweile besteht eine vergleichbare Regelung auch in Bremen, Holst, DuD 2004, 710.

[437] Beiträge in Bäumler/von Mutius, Datenschutz als Wettbewerbsvorteil; Behrendt, Datenschutzaudit in der Praxis, DuD 2006, 20 ff.

[438] www.datenschutzzentrum.de/audit/.

[439] Vgl. Bizer, DuD 2006, 5 f.; Meints, DuD 2006, 13 ff.; Zwick, DuD 2006, 26 ff.; Reiländer/Weck, DuD 2003, 692 ff.

[440] Beispiele Neundorf, DuD 2002, 338 ff.; Königshofen in: Horster/Fox, Datenschutz und Datensicherheit, S. 180 ff.; Ulmer/Zwick, DuD, 84 ff.; Sievers/Weber, DuD 2002, 342 ff.; Bijok/Kling/Weibler, DuD 2004, 621 ff.

[441] Voßbein, DuD 2004, 92 ff; Völker, DuD 2004, 102 ff.; Voßbein, DUD 2006, 33 ff.; Bock/Rudolph, DuD 2006, 29 ff.

bedürfen aber noch einer Konsolidierung.[442] Für Verbraucher und Unternehmen bieten Auditverfahren eine große Chance, um die Einhaltung des Datenschutzstandards einer Organisation bzw. einer Dienstleistung im Unterschied zu anderen Wettbewerbern gegenüber den Verbrauchern zu kommunizieren. Dabei spielt eine große Rolle, dass sich das Unternehmen in einem Audit nicht nur zur Einhaltung von Datenschutzanforderungen verpflichtet, sondern ihre tatsächliche Umsetzung im Betrieb durch unabhängige Dritte bestätigen lässt. Damit gehen Audits in ihrer Aussagekraft für den Verbraucher weit über das hinaus, was deklaratorische Privacy Policies bewirken können.

### 12.2.2 Gütesiegel für Produkte

Eine Steuerungswirkung auf der Ebene der Technik übt das *Gütesiegel* nach dem Datenschutzrecht in Schleswig-Holstein aus. Es wird für IT-Produkte (Hard- und Software) verliehen, die mit den Vorschriften für den Datenschutz und die Datensicherheit vereinbar sind (§ 4 Abs. 2 SG LDSG).[443] Das Produkt muss besondere Eigenschaften, insbesondere im Hinblick auf die Datenvermeidung und die Datensparsamkeit, die Datensicherheit und die Revisionssicherheit der Datenverarbeitung sowie die Gewährleistung der Betroffenenrechte aufweisen (§ 2 Abs. 2 Nr. 4 SH GütesiegelVO). Eine unmittelbare Steuerungswirkung entfaltet das Gütesiegels zunächst nur für den Einsatz in der schleswig-holsteinischen Verwaltung. § 4 Abs. 2 SH LDSG verpflichtet die Behörden des Landes „vorrangig“ solche Produkte einzusetzen, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit „in einem förmlichen Verfahren“ festgestellt wurde. Eine mittelbare Steuerungswirkung entfaltet das Gütesiegel jedoch schon heute über die Grenzen Schleswig-Holsteins hinaus, weil Anbieter eines mit einem Gütesiegel versehenen Produkts nicht gehindert sind, gegenüber anderen öffentlichen und privaten Kunden auf die besondere Qualitätsauszeichnung durch das schleswig-holsteinische Gütesiegel zu verweisen.[444] Seit Bestehen ist das Datenschutz-Gütesiegel bereits über 30 Mal an Hersteller für die datenschutzfreundliche Gestaltung ihres Produktes verliehen worden.[445]

Neben dem gesetzlich geregelten Datenschutzaudit ist es Anbietern auch nicht verwehrt, privatrechtlich gestaltete Instrumente eines marktwirtschaftlichen Datenschutzes zu entwickeln und anzubieten. Das vielleicht bekannteste unter ihnen ist das Gütesiegel „Quid“.[446]

---

[442] Bizer, DuD 2006, 5 ff.

[443] Bäumler, DuD 2002, 325 ff.; Schläger, DuD 2004, 459 ff., http://www.datenschutzzentrum.de/guetesiegel/index.htm/.

[444] Die ehemalige Ministerpräsidentin des Landes Schleswig-Holstein Heide Simonis spricht vom Datenschutz als „Standortvorteil“ für das Land Schleswig-Holstein in: Bäumler/v. Mutius, Datenschutz als Wettbewerbsvorteil, S. 224. Der Ministerpräsident Carstensen hat auf der CeBIT 2006 einem Hersteller ein Datenschutz-Gütesiegel verliehen.

[445] Bizer/Körffer, Gütesiegel für IT-Produkte, WuM 2006, 24 ff.

[446] Wedde/Schröder, Quid, Das Gütesiegel für Qualität im betrieblichen Datenschutz 2001.

Ein weiteres Siegel wird für datenschutzkonforme Online-Dienste vergeben.[447] Im Rahmen der Gütesiegel der Initiative D21 ist auch der Datenschutz ein Prüfungskriterium.[448]

Für den Verbraucherschutz ist von Bedeutung, dass das Gütesiegel von einer anerkannten und unabhängigen Stelle verliehen wird. Eine Verleihung des Gütesiegels allein durch akkreditierte Gutachter läuft Gefahr, dass die Verbraucher seiner Aussage nicht die Bedeutung schenken, die es möglicherweise verdient. Dieser Aspekt ist deshalb von besonderer Bedeutung, weil bei der Vielfalt an Siegeln und Labels die Gefahr einer Verwässerung der Aussage besteht, der nur durch die Verleihung des Gütesiegels durch eine öffentliche und mit hohem Vertrauen belegter öffentlicher Einrichtung entgegengewirkt werden kann. Mit dem Verzicht auf das Ausführungsgesetz nach § 9 a BDSG versäumte der Gesetzgeber bisher eine wichtige Chance, den Verbraucherdatenschutz durch ein Instrument der Motivation mehr Geltung zu verschaffen.

[447] Bspw. Schaar/Stutz, DuD 2002, 330.

[448] www.initiative21.de.

# Literaturverzeichnis


| | |
|---|---|
| Ahrend, Volker / Bijok, Christoph / Dieckmann, Uwe / Eitschberger, Bernd / Guthmann, Markus / Eul, Harald / Schmidt, Mirko / Schwarzhaupt, Paul-Dieter | Modernisierung des Datenschutzes? DuD 2003, 433 – 438. |
| Arlt, Ute | Künftige Rechtsstellung der Kontrollstellen für den Datenschutz in: H. Bäumler (Hrsg.), Der neue Datenschutz, Neuwied 1998, S. 271 ff. |
| Auernhammer, Herbert | Bundesdatenschutzgesetz, 3. Auflage, Köln, Berlin, Bonn, München 1993. |
| Ayad, Patrick | E-Mail-Werbung – Rechtgrundlagen und Regelungsbedarf, CR 2001, 533 ff. |
| Baeriswyl, Bruno | Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?, RDV 2000, 6 ff. |
| Bauer, Matthias / Meints, Martin / Hansen, Marit (Eds.): | Structured Overview on Prototypes and Concepts of Identity Management Systems, V1.1, Deliverable 3.1 of the FIDIS (Future of Identity in the Information Society) Network of Excellence, 15. September 2005 www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf |
| Bäumler, Helmut | Marktwirtschaftlicher Datenschutz, Audit und Gütesiegel à la Schleswig-Holstein, DuD 2002, 325 ff. |
| Bäumler, Helmut | „AN-ON“ Projekt in Schleswig-Holstein zur Anonymität im Internet, DuD 2001, 316. |
| Bäumler, Helmut | Modernisierung des Datenschutzes in Schleswig-Holstein, DuD 2000, 20 ff. |
| Bäumler, Helmut / von Mutius, Albert (Hrsg.) | Datenschutz als Wettbewerbsvorteil, Braunschweig 2002. |
| Behrendt, Heiko | Datenschutzaudit in der Realität, DuD 2006, 20 ff. |
| Berghoff, Julia | Selbstregulierung im Marketing, RDV 2002, 78 ff. |
| Bergmann, Lutz / Möhrle, Roland / Herb, Armin | Datenschutzrecht, Kommentar zum Bundesdatenschutzgesetz, Datenschutzgesetz der Länder und Kirchen, Bereichsspezifischer Datenschutz, Stuttgart München Hannover Berlin Weimar Dresden 1977, Stand Mai 2005 |
| Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. | Benachteiligungsverbot zugunsten des Beauftragten für den Datenschutz, DuD 2005, 272 ff. |
| Bijok, Bernd-Christoph / Kling, Siegfried / Weibler, Martin | Informationssicherheits- und Datenschutz-Audit bei Bosch DuD 2004, 621 ff. |
| Bizer, Johann | Strukturplan modernes Datenschutzrecht, DuD 2004, 6 ff. |

| | |
|---|---|
| Bizer, Johann | Datenschutzrecht in: Michael Schulte (Hrsg), Handbuch des Technikrechts, Heidelberg 2003, S. 561-597. |
| Bizer, Johann | Ziele und Elemente der Modernisierung des Datenschutzrechts, DuD 2001, 274 ff. |
| Bizer, Johann | Ziele und Elemente der Modernisierung des Datenschutzrechts, DuD 2001, 274 – 277. |
| Bizer, Johann | Datenschutz durch Technikgestaltung, in: Bäumler / von Mutius (Hrsg.), Datenschutzgesetze der dritten Generation, Neuwied 1999, S. 28 ff. |
| Bizer, Johann | Zweckbindung durch Willenserklärung, DuD 1998, 558 ff. |
| Bizer, Johann | Forschungsfreiheit und Informationelle Selbstbestimmung, Baden-Baden 1992. |
| Bizer, Johann / Körffer, Barbara | Gütesiegel für IT-Produkte, Das Beispiel des Landesdatenschutzgesetzes Schleswig-Holstein, VuM 2006, 24 – 28. |
| Bizer, Johann / Lutterbeck, Bernd / Rieß, Joachim | Freundesgabe für Alfred Büllesbach, Stuttgart 2002, (Zitiert: FG Büllesbach) |
| Bizer, Johann / Petri, Thomas B. | Kompetenzrechtliche Fragen des Datenschutzaudits, DuD 2001, 97 ff. |
| Bock, Nobert / Rudolph, Daniel | IT-Sicherheitsmanagement als messbare Dienstleistung, DuD 2006, 29 ff. |
| Breinlinger, Astrid | Datenschutz im Marketing in: A. Roßnagel (Hrsg), Handbuch des Datenschutzrechts, München 2003, Kap. 7.6. |
| Breinlinger, Astrid | Datenschutzrechtliche Probleme bei Kunden- und Verbraucherbefragungen zu Marketingzwecken, RDV 1997, 247 ff. |
| Brönneke, Tobias / Bobrowski, Michael | Datenschutz als Kernanliegen des Verbraucherdatenschutzes im E-Commerce in: H. Bäumler (Hrsg.), E-Privacy 2000, S. 141 ff. |
| Brühann, Ulf | Selbstregulierungsinstrumente zur Liberalisierung des Datenexports, in: Freundesgabe für Büllesbach, Hrsg. von J. Bizer / B. Lutterbeck / J. Rieß, Stuttgart 2002, S. 289 – 300. |
| Büllesbach, Alfred | Die Kunst der Selbstregulierung in: Freundesgabe für Bäumler, hrsg. von J. Bizer / A. von Mutius / T.B. Petri / T. Weichert, Kiel 2004, S. 239 ff. |
| Büllesbach, Alfred | Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsvorteil, RDV 1997, 239 ff. |
| Büllesbach, Alfred / Höss-Löw, Petra | Vertragslösung, Safe Harbor oder Privacy Code, DuD 2001, 135 ff. |
| Buss, Julia | Wechselwirkung zwischen BDSG und UWG, RDV 2005, 260 ff. |

| | |
|---|---|
| Carblanc, Marie | Building bridges between different approaches of privacy in: FG Büllesbach, hrsg. von J. Bizer / J. Rieß / B. Lutterbeck, Umbruch von Regelungssystemen in der Informationsgesellschaft, Stuttgart 2002, S. 316 ff. |
| Diek, Anja | Gütesiegel nach dem schleswig-holsteinischen Landesdatenschutzgesetz in: Bäumler / v.Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil 2002, S. 157 ff. |
| Dörr, Erwin / Schmidt, Dietmar | Neues Bundesdatenschutzgesetz, Handkommentar; Die Arbeitshilfe für Wirtschaft und Verwaltung, 2. Auflage, Köln 1992 |
| Duhr, Elisabeth | Datenschutz in Auskunfteien in: A. Roßnagel (Hrsg), Handbuch des Datenschutzrechts, München 2003, Kap. 7.5. |
| Ehmann, Eugen / Helfrich, Marcus | EG-Datenschutzrichtlinie, Kurzkommentar, Köln 1999 |
| Ernestus, Walter | Konzept der Datensicherung, in: Roßnagel, Handbuch des Datenschutzrechts, München 2003, Kap. 3.2. |
| Fedderath, Hannes / Berthold, Oliver | Identitätsmanagement in: H. Bäumler (Hrsg.), Der neue Datenschutz, Wiesbaden 2000, S. 189 ff. |
| Garstka, Hansjürgen | Datenschutzkontrolle: Das Berliner Modell, DuD 2000, 289 ff. |
| Garstka, Hansjürgen | Synchronisation der Arbeit der Datenschutzbeauftragten und Aufsichtsbehörden in: H. Bäumler (Hrsg.), Der Neue Datenschutz, Neuwied 1998, S. 159 ff. |
| Gola, Peter | Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, RDV 2002, 109 ff. |
| Gola, Peter / Schomerus, Rudolf | Bundesdatenschutzgesetz BDSG, Kommentar, 8. Auflage, München 2005 |
| Gräfin von Westerholt, Margot / Döring, Wolfgang | Datenschutzrechtliche Aspekte der Radio Frequency Identification. Ein „Virtueller Rundgang“ durch den Supermarkt der Zukunft, CR 2004, 710 ff. |
| Groß, Thomas | Unabhängige Datenschutzaufsicht, DuD 2002, 684 ff. |
| Hansen, Marit | Mit dem Werkzeugkasten in die Informationsgesellschaft in: Freundesgabe für H. Bäumler, hrsg. von J.Bizer / A. von Mutius / T.B: Petri / T. Weichert, Kiel 2004, S. 283 ff. |
| Hansen, Marit | Privacy Enhancing Technologies in: A. Roßnagel (Hrsg), Handbuch des Datenschutzrechts, München 2003, Kap. 3.3. |
| Hansen, Marit / Probst, Thomas | Datenschutzgütesiegel aus technischer Sicht: Bewertungskriterien des schleswig-holsteinischen Datenschutzgütesiegels in: H. Bäumler / A. v. Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil 2002, S. 163 ff. |
| Heidemann-Peuser, Helke | Rechtskonforme Gestaltung von Datenschutzklauseln, DuD 2002, 389 – 394. |
| Heil, Helmut | Der Art. 31-Auschuss, DuD 1999, 655. |

| | |
|---|---|
| Hellermann, Johannes / Wieland, Joachim | Die Unabhängigkeit der Datenschutzkontrolle im nicht-öffentlichen Bereich, DuD 2000, 284 ff. |
| Herb, Armin | Datenschutzbeauftragte der öffentlich-rechtlichen Rundfunkanstalten in: A. Roßnagel (Hrsg.), Handbuch des Datenschutzrechts, München 2003, Kap. 5.3. |
| Hillenbrandt-Beck, Renate | Aufsichtsbehörden in: Roßnagel, Handbuch des Datenschutzrechts, München 2003, Kap. 5.4. |
| Hoeren, Thomas / Lütkemeier, Sven | Unlauterer Wettbewerb durch Datenschutzverstöße, in: B. Sokol (Hrsg.), Neue Instrumente im Datenschutz, Düsseldorf 1999, S. 115 ff. |
| Hoffmann-Riem, Wolfgang | Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), S. 513 ff. |
| Holst, Sven | Bremische Datenschutzauditverordnung in Kraft, DuD 2004, 710. |
| Holznagel, Bernd / Bonnekoh, Mareike | Radio Frequency Identification – Innovation vs. Datenschutz?, MMR 2006, 20 ff. |
| Hornung, Gerrit | Datenschutz für Chipkarten: Die Anwendung des § 6c BDSG auf Signatur- und Biometriekarten, DuD 2004, 15 ff. |
| Jacob, Joachim / Heil, Helmut | Datenschutz im Spannungsfeld von staatlicher Kontrolle und Selbstregulierung in: Freundesgabe für Büllesbach, hrsg. von J. Bizer / B. Lutterbeck / J. Rieß, Stuttgart 2002, S. 213 ff. |
| Jacob, Joachim / Jost, Tanja | Marketingnutzung von Kundendaten und Datenschutz – ein Widerspruch?, DuD 2003, 621 ff. |
| Kauß, Udo | Gerichtliche Kontrolle unabhängiger Datenschutzbeauftragter, DuD 2003, 370 f. |
| Kilian, Wolfgang / Scheja, Gregor | Freier Datenfluss im Allfinanzkonzern, RDV 2002, 177 ff. |
| Köhntopp, Marit | Das virtuelle Datenschutzbüro in: H. Bäumler (Hrsg.), E-Privacy, Wiesbaden 2000, S. 291 ff. |
| Kongehl, Gerhard (Hrsg.) | Datenschutz-Management (Loseblatt), Freiburg 2005. |
| Königshofen, Thomas | Betriebliche Datenschutzbeauftragte in: A. Roßnagel, Handbuch des Datenschutzrechts, München 2003, Kap. 5.5. |
| Königshofen, Thomas | Datenschutz-Audit bei der Deutschen Telekom in: P. Horster / D. Fox, Datenschutz und Datensicherheit, Wiesbaden 1999, S. 180 ff. |
| Königshofen, Thomas | Erwartungen eines betrieblichen Datenschutzbeauftragten an staatliche Datenschutzbeauftragte in: H. Bäumler (Hrsg.), Der neue Datenschutz 1998, S. 230 ff. |
| Körffer, Barbara | Datenschutzrechtliche Anforderungen an Kundenbindungssysteme, DuD 2004, 267 ff. |
| Lepper, Ulrich / Wilde, Christian Peter | Unabhängigkeit der Datenschutzkontrolle, CR 1997, 703 ff. |

| | |
|---|---|
| Lewinski, Kai von | Formelles und informelles Handeln der datenschutzrechtlichen Aufsichtsbehörden, RDV 2001 275 ff. |
| Lutterbeck, Bernd | Welches Personal braucht der Datenschutz morgen? in: H. Bäumler (Hrsg.), Der neue Datenschutz, Neuwied 1998, S. 246 ff. |
| Meints, Martin | Datenschutz nach BSI-Grundschutz, DuD 2006, 13 ff. |
| Meyer, Jan-Bernd | Wie RFID funktioniert – und wie nicht, Computerwoche, 25/2005, 25 f. |
| Müller, Jürgen / Handy, Matthias | RFID und Datenschutzrecht – Risiken, Schutzbedarf und Gestaltungsideen, DuD 2004, 655. |
| Neundorf. Lutz | Praxisbericht: Konzerninternes Datenschutzaudit, DuD 2002, 338 ff. |
| Opaschowski, Horst W. | Datenschutz in der Gesellschaft in: Roßnagel, Handbuch des Datenschutzrechts, München 2003, Kap. 2.1. |
| Opaschowski, Horst W. | Quo vadis, Datenschutz?, DuD 2001, 678 ff. |
| Opaschowski, Horst W. | Quo vadis, Datenschutz?, DuD 1998, 654 ff. |
| Palandt, Otto | Bürgerliches Gesetzbuch, 65. Auflage, München 2006. |
| Petri, Thomas B. | Datenschutz in der Privatwirtschaft, in: Freundesgabe für Bäumler, hrsg. von J. Bizer / A. von Mutius / T.B: Petri / T. Weichert, Kiel 2004, S. 221 - 239. |
| Pfitzmann, Andreas / Hansen, Marit | Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, V0.27, 20. Februar 2006, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml |
| Podlech, Adalbert | Art. 2 Abs. 1 GG in: Alternativ-Kommentar (AK-GG), Loseblatt, 3. Auflage, Neuwied 2003. |
| Rannenberg, Kai | Datenschutz nicht als Technikfeind, sondern als Innovationsmotor in: H. Bäumler (Hrsg.), Der neue Datenschutz, Neuwied 1998, S. 190 ff. |
| Reiländer, Frank / Weck, Gerhard | Datenschutzaudit nach IT-Grundschutz – Konvergenz zweier Welten, DuD 2003, 692 ff. |
| Roßnagel, Alexander | Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71 ff. |
| Roßnagel, Alexander | Datenschutzaudit in: ders., Handbuch des Datenschutzrechts, München 2003, Kap. 3.7. |
| Roßnagel, Alexander | Konzepte der Selbstregulierung, in: ders., Handbuch des Datenschutzrechts, München 2003, Kap. 3.6. |
| Roßnagel, Alexander (Hrsg.) | Recht der Multimedia-Dienste. Kommentar zum IuKDG und MDStV München, Stand August 2003 |
| Roßnagel, Alexander (Hrsg.) | Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung München 2003, (Zit: HdBDatSchR, Kapitel, Rn.) |

| | |
|---|---|
| Roßnagel, Alexander / Garstka, Hansjürgen / Pfitzmann, Andreas | Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesinnenministers, Berlin 2001. |
| Roßnagel, Alexander / Müller, Jürgen | Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR 2004, 625 ff. |
| Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen | Modernisierung des Datenschutzrechts, DuD 2002, 253 ff. |
| Schaar, Peter | Unabhängige Datenschutzaufsicht im Innenministerium? DuD 2005, 579. |
| Schaar, Peter | Die Möglichkeiten der Datenschutzaufsichtsbehörden in: H. Bäumler (Hrsg.), E-Privacy, Wiesbaden 2000, S. 73 ff. |
| Schaffland, Hans-Jürgen / Wiltfang, Noeme | Bundesdatenschutzgesetz (BDSG), ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Berlin 1977 |
| Schmehling, von, Margret | Datenschutz-Aufsicht: Vom Papiertiger zur Sonderordnungsbehörde, DuD 2002, 351 – 355. |
| Schröder, Christian | Verbindliche Unternehmensregelungen, DuD 2004, 462 ff. |
| Schulte, Martin (Hrsg.) | Handbuch des Technikrechts, Berlin, Heidelberg 2003. |
| Schwintowski, Hans-Peter | Rechtsgutachten zur Beurteilung der Datenweitergabeklausel in Antragsformularen der Versicherungswirtschaft im Geschäft mit Verbrauchern in Deutschland, Berlin 2004. |
| Schwintowski, Hans-Peter | Rechtliche Grenzen der Datenweitergabeklausel in Versicherungsverträgen, VuR 2004, S. 242 – 251. |
| Simitis, Spiros | Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Baden-Baden 2003, (Zitiert: Simitis-Bearbeiter, BDSG § Rn.) |
| Simitis, Spiros | Auf dem Weg zu einem neuen Datenschutzkonzept – Die zweite Novellierungsstufe des BDSG, DuD 2000, S. 714 – 726. |
| Simitis, Spiros / Dammann, Ulrich | EG-Datenschutzrichtlinie, Kommentar, 1. Auflage, Baden-Baden 1997 |
| Tauss, Jörg / Kollbeck, Johannes / Fazlic, Nermin | Modernisierung des Datenschutzes: Wege aus der Sackgasse in: Freundesgabe für Bäumler, hrsg. von J. Bizer / A. von Mutius / T.B: Petri / T. Weichert, Kiel 2004, S. 41 ff. |
| Tinnefeld, Marie-Theres / Ehmann, Eugen / Gerling, Rainer W. | Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 4. Auflage, München Wien 2005 |
| Trute, Hans-Heinrich | Der Schutz personenbezogener Daten in der Informationsgesellschaft, JZ 1998, 825 ff. |
| Ulmer, Claus D. / Zwick, Werner | Messung des Datenschutzniveaus, DuD 2004, 85 ff. |

| | |
|---|---|
| Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein | Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, Studie im Auftrag des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz, Kiel 2005. |
| Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Humboldt-Universität zu Berlin | Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS), Studie im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel / Berlin 2006 (noch nicht erschienen) |
| Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und Verbraucherzentrale Bundesverband e.V. | Kundenbindungssysteme und Datenschutz, Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) im Auftrag des Verbraucherzentrale Bundesverbandes e.V., Berlin 2003. |
| van Bocxlaer, Anja | Noch läuft das Fass nicht über, Card-Forum 04/2003, S. 24 – 32 |
| Völker, Jörg | BS 7799 - Von "Best Practice" zum Standard, DuD 2004, 102 ff. |
| Voßbein, Reinhard | BS 15000 – Neue Impulse für die IT-Sicherheit, DuD 2006, 33 ff. |
| Voßbein, Reinhard | Datenschutzauditierung, DuD 2004, 92 ff. |
| Walz, Stefan | EG-Datenschutzrichtlinie und Selbstregulierung – Umsetzungsdefizite beim Medienprivileg des BDGS in: FG Büllesbach, hrsg. von J. Bizer / B. Lutterbeck / J. Rieß, Stuttgart 2002 S. 301 ff. |
| Walz, Stefan | Selbstkontrolle versus Fremdkontrolle in: FS Simitis hrsg. von D. Simon / M. Weiss, Zur Autonomie des Individuums, Baden-Baden 2000, S. 455 ff. |
| Weber, Jürgen / Jacob, Harald / Rieß, Joachim / Ullmann, Alfons | Neue Wege der Kundenbindung aus Datenschutzsicht: Bonuskarten-Systeme, DuD 2003, S. 614 – 620. |
| Wedde, Peter / Schröder, Lothar | Quid, Das Gütesiegel für Qualität im betrieblichen Datenschutz 2001 |
| Weichert, Thilo | Datenschutzrechtliche Anforderungen an Verbraucher-Kredit-Scoring, DuD 2006, 582 - 587. |
| Weichert, Thilo | Kundenbindungssysteme – Verbraucherschutz oder der gläserne Konsument?, DuD 2003, S. 161 – 163. |
| Weichert, Thilo | Chipkarten, in A. Roßnagel (Hrsg.), Handbuch des Datenschutzrechts, München 2003. Kap. 9.5 |
| Weichert, Thilo | Datenschutz als Verbraucherschutz, DuD 2001, 264 ff. |
| Weichert, Thilo | Datenschutzberatung – Hilfe zur Selbsthilfe, in: H. Bäumler (Hrsg.), Der neue Datenschutz, Neuwied 1998, S. 213 ff. |

| | |
|---|---|
| Wittig, Petra | Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, S. 59 – 62. |
| Zwick, Werner | Standardisierung im Datenschutz, DuD 2006, 24 ff. |

# Anhang

Gekürzter Anhang:
Dieser Anhang enthält ausschließlich die Fragebögen zur empirischen Untersuchung der Studie.

# A1 Telefonische Verbraucherbefragung

## A1.1 Fragebogen für die telefonische Verbraucherbefragung

# *Produkt + Markt*

Marktforschung Marketingberatung

Otto-Lilienthal-Straße 15 – 49134 Wallenhorst

Tel.: 05407/885-100

| FORSCHUNGSPROJEKT | FRAGEBOGENNUMMER |
|---|---|
| 252262 | |

## Datenschutz

Nur vom Institut auszufüllen:

| Nr: | PC: | Interviewer: | Eingang am: |
|---|---|---|---|
| Code: | OK: | Bundesland: | Vereinnahmt durch: |

***Produkt + Markt*** Befragung zum Thema Datenschutz

## Repräsentative Cati-Befragung

Guten Tag, mein Name ist ....
Ich rufe im Auftrag der Datenschutz-Aufsichtsbehörde für Wirtschaft und Verwaltung in Schleswig-Holstein an.
Wir möchten Ihnen einige Fragen zu Ihren Datenschutzrechten als Verbraucher stellen, um zu erfahren, ob Sie ausreichend über Ihre Datenschutzrechte informiert sind. Ihre Antworten sollen uns helfen, Verbesserungsvorschläge zu erarbeiten. Die Ergebnisse der Studie werden Ende August 2005 auf unserer Webseite www.datenschutzzentrum.de veröffentlicht.
Das Interview dauert nur wenige Minuten.

INTERVIEWER: Möglichst immer auf Folgendes hinweisen:

Das Institut versichert Ihnen ausdrücklich, dass alle Ihre Angaben vertraulich behandelt und in zusammengefasster Form lediglich so ausgewertet werden, dass kein Rückschluss auf den einzelnen Befragten möglich ist.

### Screening (Das Bundesland wird über die Vorwahl gesteuert)

**1.„Aus statistischen Gründen möchte ich Sie zunächst um einige allgemeine Angaben bitten. Würden Sie mir bitte Ihr Alter nennen?“** (Quote)

|___|___| Jahre

**2.„Geschlecht“** (Quote)

INTERVIEWER: Frage nicht vorlesen!!

| | |
|---|---|
| männlich | ☐ 1 |
| weiblich | ☐ 2 |

**3.„Und nun geht es noch um die Größe Ihres Wohnortes. Wie viele Einwohner leben ungefähr in Ihrem Wohnort? Sollten Sie in einer Großstadt wohnen, beziehen Sie bitte diese Angabe *nicht* nur auf Ihren Stadtteil, sondern auf die ganze Stadt! Ich nenne Ihnen dazu im folgenden einige Ortsgrößenklassen. Bitte sagen Sie mir, zu welcher Ortsgrößenklasse Ihre Stadt gehört.“** (Quote)

INTERVIEWER: Vorlesen!

| | |
|---|---|
| bis 4.999 Einwohner | ☐ 1 |
| 5.000 bis 49.999 Einwohner | ☐ 2 |
| 50.000 bis 99.999 Einwohner | ☐ 3 |
| 100.000 bis 499.999 Einwohner | ☐ 4 |
| 500.000 und mehr | ☐ 5 |

***Produkt + Markt*** Befragung zum Thema Datenschutz

**4.„Wie bereits erwähnt, geht es in dieser kurzen Befragung um das Thema Datenschutz. Was fällt Ihnen spontan zum Thema Datenschutz ein? Bitte nennen Sie mir dazu 3 Stichworte."**

| INTERVIEWER: | Wie genannt nacheinander eintragen, aber natürlich nur unterschiedliche Nennungen! Nachfassen, aber nach 3 unterschiedlichen Nennungen weiter zur nächsten Frage. |
|---|---|

1. _____ |___|___|
2. _____ |___|___|
3. _____ |___|___|

**5.„Wenn Sie Fragen zum Thema Datenschutz hätten, wo würden Sie sich informieren?"**

| INTERVIEWER: | Nachfassen! Wo noch? |
|---|---|

_____ |___|___|

_____ |___|___|

_____ |___|___|

**„Bitte stellen Sie sich folgende Ausgangssituation vor:
Sie haben sich entschlossen, die Kundenkarte eines Handelsunternehmens zu nutzen. Zu diesem Zweck hat das Unternehmen Ihren Vor- und Nachnamen, Ihr Geburtsdatum und Ihre Anschrift erfasst. Alle Artikel, die Sie unter Vorlage dieser Kundenkarte kaufen, werden fortan in einem elektronischen Konto zusammengetragen. Ihre Nutzungsgewohnheiten können dadurch ausgewertet werden.
Zu dieser Situation möchte ich Ihnen nun einige Fragen stellen."**

**6.„Haben Sie grundsätzlich Bedenken bei der Nutzung einer solchen Kundenkarte?"**

| INTERVIEWER: | Vorlesen! Der Befragte muss sich entscheiden! |
|---|---|

Ja ☐ 1
Nein ☐ 2

**7.„Gehen Sie davon aus, dass das Unternehmen Sie darüber informieren muss, wenn es Ihre Kundendaten auswerten will, um Ihnen zielgerichtet Werbung schicken zu können?"**

| INTERVIEWER: | Vorlesen! |
|---|---|

Ja, das Unternehmen ist gesetzlich zur Information verpflichtet. ☐ 1
Nein, das Unternehmen ist gesetzlich hierzu nicht verpflichtet. ☐ 2
*(nicht vorlesen!)* Ich weiß es nicht. ☐ 3

**8.„Muss das Unternehmen Sie darüber informieren, wenn es Ihre Daten an Dritte verkaufen will?"**

| INTERVIEWER: | Vorlesen! |
|---|---|

Ja, das Unternehmen ist gesetzlich dazu verpflichtet. ☐ 1
Nein, das Unternehmen ist gesetzlich nicht dazu verpflichtet. ☐ 2
*(nicht vorlesen!)* Ich weiß es nicht. ☐ 3

***Produkt + Markt*** Befragung zum Thema Datenschutz

**9.„Muss das Unternehmen Sie über den Namen des Unternehmens informieren, an den es Ihre Daten verkaufen will?"**

INTERVIEWER: Vorlesen!

Ja, das Unternehmen ist gesetzlich zur Information verpflichtet. ☐ 1
Nein, das Unternehmen ist gesetzlich hierzu nicht verpflichtet. ☐ 2
*(nicht vorlesen!)* Ich weiß es nicht. ☐ 3

**10.„Muss ich akzeptieren, wenn das Unternehmen meine Daten zusammenfasst, um einen Überblick über meine Einkünfte zu bekommen?"**

INTERVIEWER: Vorlesen!

Ja, das muss ich akzeptieren. ☐ 1
Nein, ich kann dagegen Widerspruch einlegen. ☐ 2
*(nicht vorlesen!)* Ich weiß es nicht. ☐ 3

**11.„Darf das Unternehmen die Auskunft verweigern, wenn Sie von ihm wissen wollen, welche Daten über Sie gespeichert sind?"**

INTERVIEWER: Vorlesen!

Ja, das Unternehmen darf die Auskunft verweigern. ☐ 1
Nein, das Unternehmen muss die Auskunft erteilen. ☐ 2
*(nicht vorlesen!)* Ich weiß es nicht. ☐ 3

**12.„Stellen Sie sich folgende Situation vor:**
**Sie bekommen von der Bank, bei der Sie ein Konto führen, einen Anruf von einem Mitarbeiter, der Ihnen einen Versicherungsvertrag anbietet.**
**Hätte Ihre Bank fragen müssen, ob Sie mit einem solchen Anruf einverstanden sind?"**

INTERVIEWER: Vorlesen!

Ja, ich hätte einem solchen Anruf zuvor zustimmen müssen. ☐ 1
Nein, eine Zustimmung meinerseits ist für einen solchen Anruf nicht erforderlich. ☐ 2
Meine vorherige Zustimmung ist nicht erforderlich, ich kann aber darauf hinweisen, dass ich nicht mehr angerufen werden möchte. ☐ 3
*(nicht vorlesen!)* Ich weiß es nicht. ☐ 4

**13.„Abschließend möchte ich Sie noch um eine statistische Angabebitten.**
**Welchen Schulabschluss besitzen Sie?"**

INTERVIEWER: Vorlesen!

keinen Schulabschluss ☐ 1
Sonderschul-Abschluss ☐ 2
Hauptschul-Abschluss ☐ 3
Realschul-Abschluss ☐ 4
Fachabitur ☐ 5
Abitur ☐ 6
Sonstiges:_____

**Vielen Dank für die Teilnahme an dieser Befragung!**

- 3 -

# A2 Befragung der betrieblichen Datenschutzbeauftragten (bDSB-Befragung)

## A2.1 Fragebogen für die Befragung der betrieblichen Datenschutzbeauftragten (bDSB-Befragung)

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

# Befragung zur Wahrnehmung von Datenschutzrechten durch Verbraucher

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist vom Bundesamt für Ernährung und Landwirtschaft beauftragt worden, eine Studie zum ***Verbraucherdatenschutz*** durchzuführen. In diesem Rahmen wollen wir in Erfahrung bringen, ob die Verbraucher ihre Datenschutzrechte gegenüber den Anbietern und Unternehmen tatsächlich in Anspruch nehmen und welche Bedeutung Ihrer Einschätzung nach diese Rechte haben.

**Bitte unterstützen Sie uns** bei dieser Befragung. Die Ergebnisse der Befragung werden wir auf der DAFTA/RDV-Forum am 17./18. November 2005 in Köln vorstellen.

Bitte senden Sie den ausgefüllten Fragebogen an uns zurück:

per **Fax:** 0431 988 – 1223
oder
per **Post:** ULD, „Fragebogen", Holstenstraße 98, 24103 Kiel

**Einsendeschluss bis spätestens 15. Juli 2005**

**Sie haben Fragen?**

Für Rückfragen zum Fragebogen stehen wir Ihnen gerne unter der Telefonnummer **0431 / 988- 1651** oder per Email **fragebogen@datenschutzzentrum**.de zur Verfügung.

**Datenschutz:**

Der Fragebogen wird von uns anonym ausgewertet und ausschließlich für den Zweck dieser Untersuchung verwendet. Bei Faxeingängen wird die Journalzeile nach Eingang abgeschnitten. Der Speicher des Faxgerätes wird werktäglich gelöscht. Bei Posteingängen wird der Briefumschlag nach Öffnung unmittelbar vernichtet.

**Hinweis zum Ausfüllen des Fragebogens:**

Bitte kreuzen Sie die zutreffende Antwort an. Bitte **vermeiden Sie Mehrfachantworten**.

**Frage 1 - Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?**

- ❑ 1-50
- ❑ 51-200
- ❑ 201-500
- ❑ 501-1000
- ❑ mehr als 1000

**Frage 2 - Wie viele Kunden hat Ihr Unternehmen?**

- ❑ unter 10
- ❑ zwischen 10 und 100
- ❑ zwischen 100 und 1.000
- ❑ zwischen 1.000 und 10.000
- ❑ zwischen 10.000 und 100.000
- ❑ mehr als 100.000

**Frage 3 - In welcher Branche ist Ihr Unternehmen tätig?**

- ❑ Dienstleistungsgewerbe
- ❑ Produzierendes Gewerbe
- ❑ Verarbeitendes Gewerbe
- ❑ Verwaltung
- ❑ Andere Branchen

**Frage 4- Kommt Ihr Unternehmen aus einem der folgenden Bereiche?**

- ❑ Ja, aus
  - ❑ Einzelhandel
  - ❑ Finanzdienstleistungen
  - ❑ Versicherungen
  - ❑ Auskunfteien
  - ❑ Telekommunikation
- ❑ Nein

**Frage 5 - Welche Funktion nehmen Sie im Unternehmen ein?**

- ❑ Ich bin betrieblicher Datenschutzbeauftragter.
- ❑ Ich bin Leiter oder Mitarbeiter der Rechtsabteilung.
- ❑ Ich bin sowohl Leiter oder Mitarbeiter der Rechtsabteilung als auch betrieblicher Datenschutzbeauftragter.
- ❑ Ich bin Geschäftsführer des Unternehmens.
- ❑ Keine der vorangegangenen Funktionen, sondern _____

**Frage 6 - Bitte schätzen Sie - Gemessen an der Zahl der Kunden Ihres Unternehmens: wie häufig erhalten Sie im Jahr Anfragen Ihrer Kunden auf *Auskunft* über die zu ihren Kunden gespeicherten Daten?**

- ❑ Nie
- ❑ Weniger als 1% der Kunden fragen an.
- ❑ Zwischen 1% und 5% der Kunden fragen an.
- ❑ Mehr als 5% der Kunden fragen an.

**Frage 7 - Bitte schätzen Sie - Gemessen an der Zahl der Kunden Ihres Unternehmens: Wie oft erhalten Sie im Jahr *Widersprüche* von Kunden gegen die Nutzung oder Übermittlung personenbezogenen Daten für Zwecke der Werbung oder Marktforschung nach § 28 Abs. 4 BDSG?**

- ❑ Trotz der Möglichkeit zum Widerspruch keine.
- ❑ Weniger als 1% der Kunden legen Widerspruch ein.
- ❑ Zwischen 1% und 5% der Kunden legen Widerspruch ein.
- ❑ Mehr als 5% der Kunden legen Widerspruch ein.
- ❑ Diese Frage ist für unser Unternehmen nicht relevant.
  (Ein Widerspruch kommt nicht in Frage, da entweder das Unternehmen keine Kundendaten zu Werbe- oder Marktforschungszwecken nutzt oder diese Nutzung auf Grund einer expliziten Einwilligung erfolgt.)

**Frage 8 - Bitte schätzen Sie - Gemessen an der Zahl der Kunden Ihres Unternehmens: Wie oft erhalten Sie im Jahr Anfragen über die *Löschung* der zu einem Kunden gespeicherten Daten?**

- ❑ nie
- ❑ Weniger als ca. 1% der Kunden wünschen ein Löschen ihrer Daten.
- ❑ Zwischen 1% und 5% der Kunden wünschen ein Löschen ihrer Daten.
- ❑ Mehr als 5% der Kunden wünschen ein Löschen der Daten.

**Frage 9 - Welche weiteren Anfragen / Beschwerden werden von Kunden im Hinblick auf die Verarbeitung der Kundendaten gestellt (z.B. allgemeine Informationsanfragen oder Anfragen zur Übermittlungen von Daten an Dritte)?**

**Frage 10 - Bitte schätzen Sie: Wie verteilen sich die Kundenbegehren aus den vorherigen genannten Anfragen (Frage 6 bis Frage 8)?**

_____ % Auskunftsbegehren
_____ % Widersprüche
_____ % Löschungsbegehren
_____ % Weitere: _____

**100 % Summe**

**Beachten Sie:**
**Falls Sie Kundendaten auf der Grundlage einer Einwilligung erheben, verarbeiten und nutzen, möchten wir Ihnen hierzu gern noch einige Fragen stellen.**
Sollten Sie Kundendaten nicht auf Grund einer Einwilligung verarbeiten, lassen Sie bitte die folgenden Fragen aus und machen bitte *mit Frage 14 weiter*.

**Frage 11 - Wie ist die Erklärung über die datenschutzrechtliche Einwilligung, die der Kunde abgibt, ausgewiesen?**

- ❑ Die Erklärung muss gesondert und ausdrücklich abgegeben werden (Opt-In)
- ❑ Die Einwilligung wird automatisch mit der Abgabe einer anderen Erklärung (z.B. über den Vertragsschluss) abgegeben. Der Kunde hat die Möglichkeit, der Einwilligung durch Durchstreichen des Textes oder Setzen eines Kreuzes zu widersprechen (Opt-Out)

**Frage 12 - Wie hoch ist der Anteil der Kunden, die ihre Einwilligung verweigern?**

- ❑ Weniger als ca. 5% der Kunden verweigern die Einwilligung.
- ❑ Zwischen ca. 5% und 9% der Kunden verweigern die Einwilligung.
- ❑ Zwischen ca. 10% und 24% der Kunden verweigern die Einwilligung.
- ❑ Zwischen ca. 25% und 50% der Kunden verweigern die Einwilligung.
- ❑ Mehr als 50% der Kunden verweigern die Einwilligung.

**Frage 13 - Wie hoch ist der Anteil der Kunden, die eine bereits erklärte Einwilligung nachträglich doch widerrufen?**

- ❑ Weniger als ca. 1% der Kunden widerrufen.
- ❑ Zwischen ca. 1% und 4% der Kunden widerrufen.
- ❑ Zwischen ca. 5% und 10% der Kunden widerrufen.
- ❑ Mehr als 10% der Kunden widerrufen.

**Frage 14 - Wer ist bei Ihnen im Unternehmen für die Bearbeitung von Auskunftsersuchen der Kunden zuständig?**

- ❑ Der betriebliche Datenschutzbeauftragte ist zuständig.
- ❑ Die Rechtsabteilung ist zuständig.
- ❑ Der Kundenservice ist zuständig.
- ❑ Die Marketingabteilung ist zuständig.
- ❑ Andere: _____

**Frage 15 - Wer ist bei Ihnen im Unternehmen für die Bearbeitung von Kunden-Widersprüchen gegen die Nutzung ihrer Daten zu Werbe- oder Marktforschungszwecken zuständig?**

- ❑ Der betriebliche Datenschutzbeauftragte ist zuständig.
- ❑ Die Rechtsabteilung ist zuständig.
- ❑ Der Kundenservice ist zuständig.
- ❑ Die Marketingabteilung ist zuständig.
- ❑ Andere: _____

**Frage 16 - Wer ist bei Ihnen im Unternehmen ist für die Bearbeitung von Löschungsbegehren der Kunden zuständig?**

- ❑ Der betriebliche Datenschutzbeauftragte ist zuständig.
- ❑ Die Rechtsabteilung ist zuständig.
- ❑ Der Kundenservice ist zuständig.
- ❑ Die Marketingabteilung ist zuständig.
- ❑ Andere: _____

**Frage 17 - Wer ist bei Ihnen im Unternehmen für die Bearbeitung von Widerrufen der Einwilligungen zuständig?**

- ❑ Der betriebliche Datenschutzbeauftragte ist zuständig.
- ❑ Die Rechtsabteilung ist zuständig.
- ❑ Der Kundenservice ist zuständig.
- ❑ Die Marketingabteilung ist zuständig.
- ❑ Andere: _____

**Frage 18 – Welchen Eindruck haben Sie: Wie gut sind die Kunden Ihres Unternehmens über ihre Datenschutzrechte informiert?**

| ❑ | ❑ | ❑ | ❑ | ❑ | ❑ |
|---|---|---|---|---|---|
| gar nicht | | befrie-digend | | sehr gut | Kann ich nicht sagen. |

**Frage 19 - Wird der betriebliche Datenschutzbeauftragte des Unternehmens bei der Gestaltung der datenschutzrechtlichen Einwilligungserklärungen oder Allgemeinen Geschäftsbedingungen oder Datenschutzhinweise beteiligt?**

- ❑ Der betriebliche Datenschutzbeauftragte wird daran *nie* beteiligt.
- ❑ Der betriebliche Datenschutzbeauftragte wird daran *selten* beteiligt.
- ❑ Der betriebliche Datenschutzbeauftragte wird daran *zum Teil* beteiligt.
- ❑ Der betriebliche Datenschutzbeauftragte wird daran *meistens* beteiligt.
- ❑ Der betriebliche Datenschutzbeauftragte wird daran *immer* beteiligt.

**Frage 20 - Eine wichtige Bedeutung für den Verbraucherdatenschutz hat die Information der Kunden durch das Unternehmen über die Verarbeitung seiner Kundendaten und seine Rechte. Zu welchem Zeitpunkt wird der Kunde am Wirkungsvollsten über seine Rechte informiert?**

- ❑ Information zu Beginn des Vertragsverhältnisses.
- ❑ Information nur zu bestimmten Anlässen (z.B. bei der Zusendung von Werbung).
- ❑ Regelmäßige Information bei jedem Kundenkontakt
- ❑ Andere: _____

**Frage 21 – Welche Bedeutung haben die folgenden Informationen für einen guten Verbraucherdatenschutz?**

| | Informationen zu/über — Bewertung | un-wichtig | | | | sehr wichtig |
|---|---|---|---|---|---|---|
| a | Identität der verantwortlichen Stelle. | ❑ | ❑ | ❑ | ❑ | ❑ |
| b | Zweckbestimmung der Erhebung, sowie zur Verarbeitung und Nutzung von Kundendaten. | ❑ | ❑ | ❑ | ❑ | ❑ |
| c | Übermittlung der Kundendaten an Dritte. | ❑ | ❑ | ❑ | ❑ | ❑ |
| d | Recht des Kunden, die Einwilligung zu verweigern. | ❑ | ❑ | ❑ | ❑ | ❑ |
| e | Recht des Kunden, die Einwilligung nachträglich zu widerrufen. | ❑ | ❑ | ❑ | ❑ | ❑ |
| f | Recht des Kunden, der Nutzung und Übermittlung zu Werbe- und Marktforschungszwecken zu widersprechen. | ❑ | ❑ | ❑ | ❑ | ❑ |
| g | Existenz und Erreichbarkeit des betrieblichen Datenschutzbeauftragten. | ❑ | ❑ | ❑ | ❑ | ❑ |
| h | Recht des Kunden, von der verantwortlichen Stelle Auskunft über die zu seiner Person gespeicherten Daten zu verlangen. | ❑ | ❑ | ❑ | ❑ | ❑ |
| i | Aufbewahrungsdauer der Kundendaten | ❑ | ❑ | ❑ | ❑ | ❑ |

**Frage 22 - Welches Instrument ist Ihrer Ansicht nach am besten geeignet, damit in Ihrem Unternehmen ein guter Verbraucherdatenschutz erreicht wird?**

- ❑ Die Arbeit des betrieblichen Datenschutzbeauftragten
- ❑ Information der Kunden über ihre Rechte sowie zur Verarbeitung ihrer Daten
- ❑ Andere: _____

**Frage 23 -Bitte schätzen Sie: Sind die folgenden Maßnahmen aus Ihrer Sicht sinnvoll, um die Situation des Verbraucherdatenschutzes zu verbessern?**

| | Bewertung / Fragen | nicht sinnvoll | | neutral | | absolut sinnvoll |
|---|---|---|---|---|---|---|
| a | Mehr Information der Kunden seitens der Unternehmen | ❑ | ❑ | ❑ | ❑ | ❑ |
| b | Mehr staatliche Aufklärung der Verbraucher | ❑ | ❑ | ❑ | ❑ | ❑ |
| c | Strengere gesetzliche Vorgaben zum Verbraucherdatenschutz | ❑ | ❑ | ❑ | ❑ | ❑ |

**Vielen Dank für Ihre Teilnahme an der Befragung.**

Bitte senden Sie den ausgefüllten Fragebogen bis zum 15. Juli 2005 zurück an folgende Adresse:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
„Fragebogen"
Holstenstraße 98
24103 Kiel

Fax: 0431/988-1223
E-Mail: fragebogen@datenschutzzentrum.de

# A3 Befragung der Verbraucherberaterinnen und Verbraucherberater (vzbv-Befragung)

## A3.1 Fragebogen für die Befragung der Verbraucherberaterinnen und Verbraucherberater (vzbv-Befragung)

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

# Befragung zur Wahrnehmung von Datenschutzrechten durch Verbraucher

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist vom Bundesamt für Ernährung und Landwirtschaft beauftragt worden, eine Studie zum ***Verbraucherdatenschutz*** durchzuführen. In diesem Rahmen wollen wir mit Ihrer Hilfe in Erfahrung bringen, ob die Verbraucher ihre Datenschutzrechte gegenüber den Anbietern und Unternehmen tatsächlich in Anspruch nehmen und welche Bedeutung diese Rechte Ihrer Einschätzung als Verbraucherberater nach haben.

**Bitte unterstützen Sie uns** bei dieser Befragung. Die Ergebnisse der Befragung werden wir Ende August auf den Internetseiten des ULD unter www.datenschutzzentrum.de veröffentlichen.

Bitte senden Sie den ausgefüllten Fragebogen an uns zurück:

per **Fax:** 0431 988 – 1223
oder
per **Post:** ULD, „Fragebogen", Holstenstraße 98, 24103 Kiel

**Einsendeschluss ist der 15. Juli 2005**

**Sie haben Fragen?:**

Für Rückfragen zum Fragebogen stehen wir Ihnen gerne unter der Telefonnummer **0431 / 988- 1651** oder per Email **fragebogen@datenschutzzentrum**.de zur Verfügung.

**Datenschutz:**

Der Fragebogen wird von uns anonym ausgewertet und ausschließlich für den Zweck dieser Untersuchung verwendet. Bei Faxeingängen wird die Journalzeile des Einganges nach Eingang abgeschnitten. Der Speicher des Faxgerätes wird täglich gelöscht. Bei Posteingängen wird der Briefumschlag nach Öffnung unmittelbar vernichtet.

**Hinweis zum Ausfüllen des Fragebogens:**

Bitte kreuzen Sie die zutreffende Antwort an. Bitte **vermeiden Sie Mehrfachantworten**.

**Frage 1 – In welchem Maße spielen Anfragen zum Datenschutz in Ihrer Beratungspraxis eine relevante Rolle?**
(Beispiele für datenschutzrelevante Themen können sein: Auskunft über Kundendaten, Einwilligung in die Verarbeitung von Verbraucherdaten, Nutzung oder Übermittlung von Verbraucherdaten zu Werbezwecken.)

Etwa _____ % der Anfragen beinhalten Datenschutz-Themen.

**Frage 2 - Hat sich die Zahl der Anfragen mit datenschutzrelevantem Inhalt in den letzten Jahren in Ihrer Beratungspraxis verändert?**

| ❑ | ❑ | ❑ | ❑ | ❑ |
|---|---|---|---|---|
| stark gesunken | gesunken | gleich | gestiegen | stark gestiegen |

**Frage 3 – Wenn Sie in Frage 2 eine Veränderung festgestellt haben, worauf ist diese aus Ihrer Sicht zurückzuführen?**

_____

_____

_____

**Frage 4 - Wenn Sie in Frage 2 eine Veränderung festgestellt haben, in welchen Bereichen haben diese stattgefunden?**

_____

_____

_____

**Frage 5 – Auf welche Themenbereiche beziehen sich die Anfragen mit Datenschutzrelevanz am häufigsten?** Bitte maximal 3 Antworten ankreuzen.

- ❑ Auskunfteien (z.B. Schufa, creditreform, Bürgel etc.)
- ❑ Versicherungen
- ❑ Banken
- ❑ Einzelhandel (insbes. Kundenkarten)
- ❑ Techniken zur Markierung von Waren (z.B. RFID)
- ❑ Telekommunikation (incl. Mobilfunk)
- ❑ Internetdienste (z.B. ebay, amazon) und Internetprovider
- ❑ Andere:

  _____

**Frage 6 - Bitte schätzen Sie aus Ihrer Beratungspraxis: Wie viele der Verbraucher mit Fragen zum Datenschutz haben vor Ihrer Beratung eigene Schritte zur Lösung ihres Problems unternommen, d.h. ihre Datenschutzrechte gegenüber dem Unternehmen geltend gemacht (z.B. Ansprüche auf Auskunft, Löschung oder Korrektur ihrer Daten, Widerspruch gegen Werbung)?**

Etwa _____ % der Verbraucher haben zuvor eigene Schritte unternommen.

**Frage 7 – Aus Ihrer Beratungspraxis: Worin liegt Ihrer Meinung nach der Hauptgrund, warum Verbraucher ihre Datenschutzrechte generell eher nicht wahrnehmen?** Bitte nur eine Antwort ankreuzen.

- ❑ Dem Verbraucher ist nicht bewusst, dass sein Problem einen datenschutzrechtlichen Bezug hat.
- ❑ Der Verbraucher ist über seine Rechte (z.B. auf Auskunft, Widerspruch oder Löschung) nicht informiert.
- ❑ Dem Verbraucher ist die Ursache seines Problems (Verarbeitung seiner Daten) bewusst, er ist auch über die entsprechenden Rechte unterrichtet, verspricht sich von deren Wahrnehmung aber keinen Erfolg.
- ❑ Der Verbraucher ist mit der Lösung seines Problems überfordert.
- ❑ Andere Gründe:

  _____

**Frage 9 - Welche Maßnahmen sind aus Ihrer Sicht sinnvoll, um die Situation des Verbraucherdatenschutzes zu verbessern?**

_____

_____

_____

_____

_____

**Vielen Dank für Ihre Teilnahme an der Befragung.**
Bitte senden Sie den ausgefüllten Fragebogen bis zum 15. Juli 2005 zurück an folgende Adresse:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
„Fragebogen“
Holstenstraße 98
24103 Kiel

Fax: 0431/988-1223
E-Mail: fragebogen@datenschutzzentrum.de

## A3.2 Befragung der Aufsichtsbehörden der Bundesländer für die Einhaltung des Datenschutzes im nichtöffentlichen Bereich

## A3.3 Fragebogen für die Befragung der Aufsichtsbehörden der Bundesländer für die Einhaltung des Datenschutzes im nichtöffentlichen Bereich

# Befragung zur Wahrnehmung von Datenschutzrechten durch Verbraucher bei Aufsichtsbehörden

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist vom Bundesamt für Ernährung und Landwirtschaft beauftragt worden, eine Studie zum ***Verbraucherdatenschutz*** durchzuführen. In diesem Rahmen sind wir auch an Ihren Erfahrungen interessiert, ob die Verbraucher ihre Datenschutzrechte gegenüber den Anbietern und Unternehmen tatsächlich in Anspruch nehmen und welche Bedeutung Ihrer Einschätzung nach diese Rechte haben.

**Bitte unterstützen Sie uns** bei dieser Befragung.

per **Fax:** 0431 988 – 1223
oder
per **Post:** ULD, „Fragebogen", Holstenstraße 98, 24103 Kiel
oder
per **E-Mail**: fragebogen@datenschutzzentrum.de

## Einsendeschluss bis spätestens Mittwoch, den 23.11.2005

**Sie haben Fragen?**

Für Rückfragen zum Fragebogen stehen wir Ihnen gerne unter der Telefonnummer **0431 / 988- 1651** oder per E-Mail **fragebogen@datenschutzzentrum.de** zur Verfügung.

Dieser Fragebogen ist als ein standardisiertes, qualitatives Experteninterview gestaltet, bei dem Rückfragen durch uns möglich sein sollen, um einen höchst möglichen Informationsgehalt zu erreichen. Bitte teilen Sie uns neben Ihrem Namen und der Behörde vor allem Ihre Telefonnummer und Ihre Mailadresse mit, um die möglicherweise auftretenden Unklarheiten möglichst rasch beseitigen zu können:

Behörde

Name

Telefon

E-Mailadresse

Bitte scheuen Sie sich auch nicht, Kommentare zu ergänzen.

Vielen Dank für Unterstützung!

**Frage 1 – Wie ist Ihre Behörde in die Verwaltung eingebunden?**
(Weil es komplizierte Konstruktionen gibt, mussten wir auf für Sie bequeme Antwortvorgaben verzichten.)

_____

_____

_____

**Frage 2 – Wie viele Mitarbeiter üben bei Ihnen speziell die Kontrolle des Privatbereichs im Sinne einer Aufsichtsbehörde aus?**

___ Mitarbeiterinnen bzw. Mitarbeiter

**Frage 3 – Führen Sie Statistiken über diejenigen Eingaben, die speziell den Privatbereich betreffen?**

- ❑ Wir führen eine Statistik über Eingaben im Privatbereich.
- ❑ Wir führen *keine* Statistik über Eingaben im Privatbereich.
- ❑ Wir führen *noch keine* Statistik über Eingaben im Privatbereich, planen aber für die nahe Zukunft deren Einführung.

**Frage 4 – Wie viele Anfragen aus dem Privatbereich bekommen Sie als Aufsichtsbehörde im Durchschnitt wöchentlich neu zur Bearbeitung vorgelegt?**

Wir bekommen im Durchschnitt _____ Anfragen pro Woche.

**Frage 5 – Zu welchen Themengebieten erhalten Sie aktuell die meisten Anfragen?**
(Bitte wählen Sie aus den nachfolgenden Themen die ***wichtigsten*** heraus, die insgesamt 90% Ihrer Anfragen ausmachen. Bitte verteilen Sie diese 90% auf die entsprechenden Themen-/Anfragenbereiche.
Unser Ziel besteht darin, die *wichtigsten Themen und deren Anteile untereinander* zu identifizieren.)

| | |
|---|---|
| Adresshandel und Direktwerbung | ____ % |
| Auskunfteien, zentrale Warndateien und Inkassounternehmen | ____ % |
| Industrie, Handel und Handwerk | ____ % |
| Kreditwirtschaft | ____ % |
| Markt- und Meinungsforschung | ____ % |
| SCHUFA | ____ % |
| Vereine und Verbände | ____ % |
| Versandhandel | ____ % |
| Versicherungen | ____ % |
| DV-Dienstleistungen | ____ % |
| Telekommunikation und neue Medien, Internetsicherheit | ____ % |
| Wohnungswirtschaft | ____ % |
| Freie Berufe | ____ % |
| Videoüberwachung, Videoaufzeichnung | ____ % |
| Andere: _____ | ____ % |

**Frage 6 – Haben Sie den Eindruck (oder können Sie statistisch belegen), dass die Anzahl der Anfragen gegenüber dem Vorjahr bis zum gegenwärtigen Zeitpunkt in den von Ihnen in der vorigen Frage ausgewählten wichtigsten Themenbereichen gestiegen sind?**
(Wenn die Anfragen ***gestiegen*** sind, geben Sie bitte einen *positiven* Prozentwert an. Wenn die Anfragen sich ***nicht oder kaum verändert*** haben, geben Sie eine 0 an. Wenn die Anfragen ***zurückgegangen*** sind, vergeben Sie bitte den entsprechenden *negativen* Prozentwert.)

Nach unserem Eindruck (bzw. der Statistik), hat sich die Zahl der Anfragen insgesamt um ___ % verändert.

**Frage 7 – Bitte beantworten Sie diese Frage nur, wenn Sie in *Frage 6 einen Zuwachs an Anfragen* festgestellt haben.**

**Zu welchen der oben aufgeführten Themenbereiche verzeichnen Sie derzeit die größten Zuwächse an Anfragen im Vergleich zum Vorjahr?**
Bitte geben Sie die drei Spitzenreiter an.

- ❑ Adresshandel und Direktwerbung
- ❑ Auskunfteien, zentrale Warndateien und Inkassounternehmen
- ❑ Industrie, Handel und Handwerk
- ❑ Kreditwirtschaft
- ❑ Markt- und Meinungsforschung
- ❑ SCHUFA
- ❑ Vereine und Verbände
- ❑ Versandhandel
- ❑ Versicherungen
- ❑ DV-Dienstleistungen
- ❑ Telekommunikation und neue Medien, Internetsicherheit
- ❑ Wohnungswirtschaft
- ❑ Freie Berufe
- ❑ Videoüberwachung, Videoaufzeichnung
- ❑ Andere: _____

**Frage 8 – Welchen Eindruck haben Sie: Wie gut sind Ihre *Petenten bzw. die Kunden* über ihre Datenschutzrechte informiert?**

| | Kenntnis der Kunden / Datenschutzrecht | sehr gut | gut | mittel-mäßig | schlecht | sehr schlecht |
|---|---|---|---|---|---|---|
| a | Auskunftsanspruch | ❑ | ❑ | ❑ | ❑ | ❑ |
| b | Widerspruchsrecht | ❑ | ❑ | ❑ | ❑ | ❑ |
| c | Übermittlung der eigenen Kundendaten an Dritte | ❑ | ❑ | ❑ | ❑ | ❑ |
| d | Löschungsanspruch | ❑ | ❑ | ❑ | ❑ | ❑ |
| e | Unterrichtungspflichten der Unternehmen (Identität der verantwortlichen Stelle, Zweckbestimmung, Übermittlung an Dritte) | ❑ | ❑ | ❑ | ❑ | ❑ |
| f | Sperrungsanspruch | ❑ | ❑ | ❑ | ❑ | ❑ |
| g | Berichtigungsanspruch | ❑ | ❑ | ❑ | ❑ | ❑ |

**Frage 9 – Welchen Eindruck haben Sie: Wie gut sind die *Unternehmen* über ihre Datenschutzpflichten gem. BDSG informiert?**

| | Kenntnis der Unternehmen / Pflichten | sehr gut | gut | mittel-mäßig | schlecht | sehr schlecht |
|---|---|---|---|---|---|---|
| a | Auskunftspflicht (§ 34) | ❑ | ❑ | ❑ | ❑ | ❑ |
| b | Information über das Widerspruchsrecht bei Verwendung zu Werbezwecken (§ 28 IV) | ❑ | ❑ | ❑ | ❑ | ❑ |
| c | Unterlassen der Verwendung zu Werbezwecken nach Ausübung des Widerspruches (§ 28 IV) | ❑ | ❑ | ❑ | ❑ | ❑ |
| d | Unterrichtungspflichten nach § 4 III (Identität der verantwortlichen Stelle, Zweckbestimmung, Übermittlung an Dritte) | ❑ | ❑ | ❑ | ❑ | ❑ |
| e | Löschungspflicht (§ 35 II) | ❑ | ❑ | ❑ | ❑ | ❑ |
| f | Sperrungspflicht (§ 35 III) | ❑ | ❑ | ❑ | ❑ | ❑ |
| g | Berichtigungspflicht (§ 35 I) | ❑ | ❑ | ❑ | ❑ | ❑ |
| h | Benachrichtigungspflicht bei Speicherung von Daten ohne Kenntnis des Betroffenen (§33) | ❑ | ❑ | ❑ | ❑ | ❑ |

**Frage 10 – Wie schätzen Sie es ein: Wie viele der anfragenden Verbraucher haben vor der Eingabe eigene Schritte zur Lösung ihres Problems unternommen, d.h. ihre Datenschutzrechte gegenüber dem Unternehmen versucht geltend zu machen?**

Nach meinem Eindruck haben etwa ____ % der Anfragenden zuvor eigene Schritte unternommen.

**Frage 11 – Wie schätzen Sie den Kenntnisstand der Verbraucher allgemein in Bezug auf die in den einzelnen Branchen genutzten operativen Verarbeitungsprozesse ein?**

| | Kenntnis der Kunden / Branche | sehr gut | gut | mittel-mäßig | schlecht | sehr schlecht |
|---|---|---|---|---|---|---|
| a | Adresshandel und Direktwerbung | ❑ | ❑ | ❑ | ❑ | ❑ |
| b | Auskunfteien, zentrale Warndateien und Inkassounternehmen | ❑ | ❑ | ❑ | ❑ | ❑ |
| c | Industrie, Handel und Handwerk | ❑ | ❑ | ❑ | ❑ | ❑ |
| d | Kreditwirtschaft | ❑ | ❑ | ❑ | ❑ | ❑ |
| e | Markt- und Meinungsforschung | ❑ | ❑ | ❑ | ❑ | ❑ |
| f | SCHUFA | ❑ | ❑ | ❑ | ❑ | ❑ |
| g | Vereine und Verbände | ❑ | ❑ | ❑ | ❑ | ❑ |
| h | Versandhandel | ❑ | ❑ | ❑ | ❑ | ❑ |
| i | Versicherungen | ❑ | ❑ | ❑ | ❑ | ❑ |
| j | DV-Dienstleistungen | ❑ | ❑ | ❑ | ❑ | ❑ |
| k | Telekommunikation und neue Medien, Internetsicherheit | ❑ | ❑ | ❑ | ❑ | ❑ |
| l | Wohnungswirtschaft | ❑ | ❑ | ❑ | ❑ | ❑ |
| m | Freie Berufe | ❑ | ❑ | ❑ | ❑ | ❑ |
| n | Videoüberwachung, Videoaufzeichnung | ❑ | ❑ | ❑ | ❑ | ❑ |
| o | Andere: _____ | ❑ | ❑ | ❑ | ❑ | ❑ |

**Frage 12 – Wie schätzen Sie den Kenntnisstand von Verbrauchern allgemein in Bezug auf die tatsächlich in der Praxis anzutreffenden operativen Verwendungen ihrer Daten ein?**

| | Kenntnis der Kunden / Operative Verarbeitungsprozesse | sehr gut | gut | mittel-mäßig | schlecht | sehr schlecht |
|---|---|---|---|---|---|---|
| a | e-Commerce-Strategien allgemein (wie z.B. Kundendaten befinden sich in Übersee und sind somit dem dt. Rechtszugriff entzogen, Data-Mining als Organisationsform, hochauflösende Profilbildung, statische Aufbereitungen gem. Scoring) | ❑ | ❑ | ❑ | ❑ | ❑ |
| b | Adresssammlung durch Preisausschreiben mit nachfolgendem Adresshandel | ❑ | ❑ | ❑ | ❑ | ❑ |
| c | Kundenkarte (Speicherung der Einkäufe, Zusammenführung von Kundendaten der „Partnerunternehmen" beim Systembetreiber, Kundenprofilerstellung) | ❑ | ❑ | ❑ | ❑ | ❑ |
| d | Click-Stream Auswertung nach persönlichem Login oder differenzierte Cookie-Anwendungen | ❑ | ❑ | ❑ | ❑ | ❑ |
| e | Durchführung und Ausgestaltung eines Scoring-Verfahrens (entweder intern oder extern) nach Kreditantragsstellung, Handyvertrag, Versandhandel | ❑ | ❑ | ❑ | ❑ | ❑ |
| f | Übermittlung von Daten an zentrale Datenbanken der Versicherungswirtschaft (z.B. UNIWAGNIS) | ❑ | ❑ | ❑ | ❑ | ❑ |

**Frage 13 – In welchem Maße stimmen Sie der These zu, dass die Verbraucher im Großen und Ganzen über die Auskunftspflichten der Unternehmen und ihren Auskunftsanspruch informiert sind, sie ihre Rechte aber nur zu einem verschwindend geringen Anteil auch wahrnehmen.**

- ❑ Dieser These *stimme ich vollkommen* zu.
- ❑ Dieser These *stimme ich überwiegend* zu.
- ❑ Ich bin *unschlüssig*, ob ich zustimmen kann oder nicht.
- ❑ Ich *stimme überwiegend nicht* zu.
- ❑ Ich halte diese These für *Unsinn*.

**Frage 14 – Welche Maßnahmen wären aus Ihrer Erfahrung heraus geeignet, um den Verbraucherdatenschutz wesentlich zu verbessern?**

**Frage 15 – Falls Sie uns noch einen Kommentar gleich welcher Art zukommen lassen möchten:**

**Vielen Dank für Ihre Teilnahme an der Befragung.**

Bitte senden Sie den ausgefüllten Fragebogen bis zum 23. November 2005 zurück an die folgende Adresse:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
„Fragebogen"
Holstenstraße 98
24103 Kiel

Oder faxen Sie uns den Fragebogen zu:
Fax: 0431/988-1223

Oder schicken Sie uns den Fragebogen im Anhang per E-Mail zu:
fragebogen@datenschutzzentrum.de