FORUM Wirtschaftsrecht - Band 12

Institut für Wirtschaftsrecht

Dennis Hoss

Callcenter aus der Perspektive des Datenschutzes

Rechtlicher Rahmen und Gestaltungsvorschläge für ein automatisiertes Gesprächsmanagement-System

kassel university press

FORUM Wirtschaftsrecht

Band 12

Herausgegeben vom
Institut für Wirtschaftsrecht an der Universität Kassel

Callcenter aus der Perspektive des Datenschutzes

Rechtlicher Rahmen und Gestaltungsvorschläge für ein automatisiertes Gesprächsmanagement-System

Dennis Hoss

kassel university press

Die vorliegende Arbeit wurde vom Fachbereich Wirtschaftswissenschaften der Universität Kassel als Dissertation zur Erlangung des akademischen Grades eines Doktors der Rechtswissenschaften (Dr. jur.) angenommen.

Erster Gutachter: Prof. Dr. Alexander Roßnagel
Zweiter Gutachter: Prof. Dr. Dr. Walter Blocher

Tag der mündlichen Prüfung 9. Mai 2012

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

Zugl.: Kassel, Univ., Diss. 2012
ISBN print: 978-3-86219-324-0
ISBN online: 978-3-86219-325-7
URN: http://nbn-resolving.de/urn:nbn:de:0002-33250

Druck und Verarbeitung: Unidruckerei der Universität Kassel
Umschlaggestaltung: Heike Arend, Unidruckerei der Universität Kassel
Printed in Germany

Vorwort

Sowohl Unternehmen als auch Behörden gehen zunehmend dazu über, ihre Routinekommunikation mit ihren Kunden oder Klienten auf verselbständigte Organisationseinheiten innerhalb oder außerhalb der Unternehmen oder Behörden zu verlagern. Durch die Auslagerung der Kommunikationsschnittstelle auf „Callcenter“ soll die Massenabwicklung von Dienstleistungen, die über das Telefon erbracht werden, professionalisiert, verbessert, rationalisiert und effektiviert werden und die Erreichbarkeit erhöht und ausgeweitet werden.

Callcenter können eingesetzt werden, sowohl um aktiv aktuelle oder potenzielle Kunden anzurufen, etwa um Marketing zu betreiben, Kunden zurückzugewinnen, sie zu erinnern oder ihnen Hinweise zu geben (Outbound-Telefonie), als auch um passiv Anrufe entgegenzunehmen, etwa zu Zwecken der Bestellabwicklung, des Beschwerdemanagements, der Beratung oder des Kundendienstes (Inbound-Telefonie). In beiden Bereichen bestehen bestimmte Vorgaben zur Qualität und Quantität der Telefonate. Die Kontakte werden – soweit möglich – durch Informations- und Kommunikationstechnologie unterstützt wie zum Beispiel durch Customer Relationship Management- (CRM-) oder Gesprächsmanagement-Systeme.

Die Sicherstellung von Qualität und Wirtschaftlichkeit der Callcenter-Dienstleistungen erfordert Kontrollen der Telefonate der Beschäftigten, um diese zu schulen und in ihrer Leistung zu verbessern. Die richtige Ansprache der Kunden und Klienten sowie die zeitgerechte Kenntnis ihrer spezifischen Vertrags- oder Antragssituation und ihrer individuellen Angelegenheiten erfordert eine intensive Verarbeitung und schnelle Bereitstellung ihrer relevanten personenbezogenen Daten. Die Arbeit mit den Kontroll- und Kundendaten erzeugt eine Vielfalt von Fragen des Beschäftigten- und Kundendatenschutzes. Diese Fragen werden verschärft, wenn derzeit in der Entwicklung befindliche Gesprächsmanagement-Systeme zum Einsatz kommen, die eine gesprächsbegleitende, situative Echtzeitunterstützung der Callcenter-Beschäftigten anbieten. Sie analysieren automatisch das Verhalten der Kunden und Berater, den Gesprächsgegenstand und den Kontext des Kundenkontakts und bieten dem Berater seiner Gesprächssituation angepasste Informationen an.

Um diese Gesprächsmanagement-Systeme in Callcentern überhaupt nutzen zu können, müssen sie die rechtlichen Rahmenvorgaben einhalten. Damit sie für Beschäftigte und Kunden akzeptabel sind und einen Fortschrift in der rechtsadäquaten Technikgestaltung darstellen, sollten sie so konzipiert und gestaltet werden, dass sie die Grundprinzipien des Datenschutzrechts mehr als nur minimal erfüllen. Die Qualitätssicherung der Kommunikationshandlungen von Beschäftigten durch den Arbeitgeber und die Datenverarbeitung für eine zulässige kommerzielle Ansprache von Kunden und potenziellen Kunden sind für den Datenschutz im Beschäftigungsverhältnis und im Kundenverhältnis gleichermaßen hochaktuelle und praktisch drängende Herausforderungen einer interdisziplinär orientierten Rechtswissenschaft, deren Lösung beispielgebend für viele ähnliche Konstellationen sein kann.

Eine solche Lösung bietet die vorliegende Arbeit von Herrn Hoss an. Ihre Zielsetzung ist zum einen, „den bestehenden datenschutzrechtlichen Rahmen“ aufzuzeigen, der beim Betrieb des Gesprächsmanagement-Systems eingehalten werden muss, und zum anderen, Vorschläge zur datenschutzgerechten Gestaltung des Systems anhand einer systembezogenen Projektion und erweiterten Umsetzung des datenschutzrechtlichen Schutzkonzepts zu entwickeln. Diese Zielsetzung ist methodisch und fachlich eine große Herausforderung, die in der Arbeit aber souverän bewältigt wird. Mit ihr füllt Herr Hoss eine Lücke im Daten-

schutzrecht. Indem er die geltenden Datenschutzregelungen für die Tätigkeit von Callcentern untersucht, bietet er wertvolle Hinweise sowohl für die Datenschutzrechtsdogmatik als auch für die Praxis. Indem er zeigt, wie technische Gestaltungsvorschläge aus verfassungs- und einfachrechtlichen Vorgaben abgeleitet werden können, trägt er zur Bewältigung schwieriger grundlegender methodischer Fragen der rechtswissenschaftlichen Technikgestaltung bei. Indem er Vorschläge für die Rechtsfortbildung zu diesem Querschnittsthema entwickelt, liefert er einen wichtigen Beitrag für die Rechtspolitik.

Die Arbeit entstand zu großen Teilen im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten interdisziplinären Forschungsprojekts „Semantik- und emotionsbasiertes Gesprächsmanagement in der Kundenberatung (SIGMUND)“. In diesem Forschungsprojekt konzipierte und entwickelte ein Konsortium aus den Partnern Ubiquitous Knowledge Processing Lab des Fachbereichs Informatik der Technischen Universität Darmstadt, itCampus Software- und Systemhaus GmbH, CAS Software AG, TEMIS Deutschland GmbH und Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel ein Gesprächsmanagement-System, das ein automatisiertes Gesprächs-Monitoring durchführt, gesprächsrelevante Informationen auswählt und die Tätigkeit der Callcenter-Agenten durch gesprächsbegleitende, situationsadäquate Bereitstellung von Informationen optimiert. In diesem Forschungsprojekt hat Herr Hoss die rechtlichen Fragen bearbeitet.

Es ist der Arbeit zu wünschen, dass sie von denjenigen ebenso zur Kenntnis genommen wird, die für die Entwicklung und Gestaltung von Gesprächsmanagement-Systemen und ihren Einsatz in Callcentern verantwortlich sind, wie auch von denjenigen, die für die Fortentwicklung des Datenschutzrechts Verantwortung tragen.

Kassel, September 2012

Prof. Dr. Alexander Roßnagel

Vorwort des Autors

Die vorliegende Dissertation wurde im Wintersemester 2011/2012 von der Universität Kassel angenommen. Literatur- und Gesetzesstand konnten bis zum Oktober 2011 berücksichtigt werden.

Die Dissertation ist während meiner Tätigkeit als wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel entstanden. Mein Arbeitsschwerpunkt lag dabei im Forschungsprojekt „Semantik- und emotionsbasiertes Gesprächsmanagement in der Kundenberatung (SIGMUND)“. Die wesentlichen Erkenntnisse aus diesem Forschungsprojekt bilden die Grundlage meiner Dissertation.

Dank sagen möchte ich allen Personen, die in irgendeiner Form zum Gelingen dieser Arbeit beigetragen haben. Sie alle namentlich zu nennen, ist an dieser Stelle nicht möglich.

Mein ganz besonderer Dank gilt Herrn Prof. Dr. Alexander Roßnagel, der mich zum einen als Doktorvater, zum anderen als Vorgesetzter jederzeit mit Rat und Tat hilfreich unterstützt und die Fertigstellung meiner Dissertation in vielfältiger Weise gefördert hat. Hohe Freiheitsgrade bei der Ausübung meiner Tätigkeit als wissenschaftlicher Mitarbeiter waren wichtiger Motivator und stellten Ausdruck von Vertrauen und Wertschätzung dar.

Herrn Prof. Dr. Dr. Walter Blocher danke ich für die Erstellung des Zweitgutachtens.

Bedanken möchte ich mich darüber hinaus bei meinen Projektpartnern im Forschungsprojekt SIGMUND für die hervorragende Zusammenarbeit. Erst durch ihre stete Bereitschaft und Geduld, mir die komplexen Zusammenhänge der eingesetzten Informationstechnik in einer - für einen „Nicht-Informatiker“ - verständlichen Form näher zu bringen, ermöglichte mir das Erfassen sämtlicher relevanter Verarbeitungsprozesse.

Meinen Arbeitskolleginnen und -kollegen in der Projektgruppe verfassungsverträgliche Technikgestaltung danke ich für nahezu drei Jahre vorbildliche kollegiale Zusammenarbeit in einer freundschaftlichen Arbeitsatmosphäre, in der ich mich sehr wohl gefühlt habe. Zahlreiche Fachdiskussionen konnten fruchtbare Impulse zu meiner Dissertation beisteuern.

Besonders herzlicher Dank gilt meinen Eltern, denen ich die Arbeit widme. Ihre Unterstützung und ihr unerschütterliches Vertrauen in meine Fähigkeiten haben meinen Ausbildungsweg – und nicht zuletzt die Dissertation – erst ermöglicht.

Kassel, Oktober 2012

Dennis Hoss

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

a. A.	anderer Ansicht
Abb.	Abbildung
Abs.	Absatz
ACD	Automatic Call Distribution
a. F.	alte Fassung
AGB	Allgemeine Geschäftsbedingungen
AnwBl	Anwaltsblatt (Zeitschrift)
AO	Abgabenordnung
AP	Nachschlagewerk des Bundesarbeitsgerichts – Arbeitsrechtliche Praxis (Zeitschrift)
ArbSchG	Arbeitsschutzgesetz
ArbuR	Arbeit und Recht (Zeitschrift, frühere Abkürzung)
Art.	Artikel
AuA	Arbeit und Arbeitsrecht (Zeitschrift)
Aufl.	Auflage
AuR	Arbeit und Recht (Zeitschrift, aktuelle Abkürzung)
BAG	Bundesarbeitsgericht
BB	Betriebs-Berater (Zeitschrift)
BDG	Bundesdisziplinargesetz
BDSG	Bundesdatenschutzgesetz
BeamtStG	Beamtenstatusgesetz
BeckOK	Beck'scher Online-Kommentar
BeckRS	Beck-Rechtsprechung
Beil.	Beilage
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BildscharbV	Bildschirmarbeitsverordnung
BKR	Zeitschrift für Bank- und Kapitalmarktrecht (Zeitschrift)
BlnDSG	Berliner Datenschutzgesetz
BMBF	Bundesministerium für Bildung und Forschung
BNotO	Bundesnotarordnung
BPersVG	Bundespersonalvertretungsgesetz
BRAO	Bundesrechtsanwaltsordnung
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht

CR	Computer und Recht (Zeitschrift)
CRM	Customer Relationship Management
CTI	Computer Telephony Integration
DB	Der Betrieb (Zeitschrift)
ders.	derselbe
dies.	dieselben
DIN	Deutsches Institut für Normung
Diss.	Dissertation
DÖD	Der Öffentliche Dienst (Zeitschrift)
Dok.	Dokument
DSB	Datenschutz-Berater (Zeitschrift)
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DStR	Deutsches Steuerrecht (Zeitschrift)
DTMF	Dual-tone Multifrequency
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVD	Digital Versatile Disc
Ed.	Edition
EG	Europäische Gemeinschaft
ehem.	ehemals
E-Mail	Electronic Mail
EMRK	Europäische Menschenrechtskonvention
ErfK	Erfurter Kommentar zum Arbeitsrecht
et al.	et alii
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
e. V.	eingetragener Verein
f.	folgende
ff.	fortfolgende
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GewO	Gewerbeordnung
GG	Grundgesetz
GRC	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
HDSG	Hessisches Datenschutzgesetz
HK	Handkommentar
HK-GS	Handkommentar Gesamtes Strafrecht
h. M.	herrschende Meinung
HmbDSG	Hamburgisches Datenschutzgesetz
Hrsg.	Herausgeber
hrsg. v.	herausgegeben von

ISDN	Integrated Services Digital Network
IT	Information Technology
ITRB	Der IT-Rechts-Berater (Zeitschrift)
IuK-	Informations- und Kommunikations-
i. V. m.	in Verbindung mit
IVR	Interactive Voice Response
JURA	JURA: Juristische Ausbildung (Zeitschrift)
jurisPR-ITR	juris Praxis-Report IT-Recht (Zeitschrift)
JZ	Juristenzeitung
KG	Kammergericht
KJ	Kritische Justiz (Zeitschrift)
KSchG	Kündigungsschutzgesetz
K&R	Kommunikation und Recht (Zeitschrift)
LDSG	Landesdatenschutzgesetz Baden-Württemberg
lit.	littera
LPVG	Personalvertretungsgesetz für das Land Baden-Württemberg
m. Anm.	mit Anmerkung
MIR	Medien Internet und Recht (Zeitschrift)
MMR	Multimedia und Recht (Zeitschrift)
MRRG	Melderechtsrahmengesetz
m. w. N.	mit weiteren Nachweisen
NJOZ	Neue Juristische Online-Zeitschrift (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NK	Nomos-Kommentar
Nr.	Nummer(n)
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht (Zeitschrift)
NZA-RR	Neue Zeitschrift für Arbeitsrecht – Rechtsprechungs-Report Arbeitsrecht (Zeitschrift)
NZS	Neue Zeitschrift für Sozialrecht (Zeitschrift)
OECD	Organisation for Economic Co-operation and Development
o. J.	ohne Jahr
OLG	Oberlandesgericht
o. V.	ohne Verfasser
PersVG	Personalvertretungsgesetz für das Land Brandenburg
PIN	Persönliche Identifikationsnummer

RdA	Recht der Arbeit (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
Rn.	Randnummer(n)
Rspr.	Rechtsprechung
S.	Seite(n)
s.	siehe
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
Session-ID	Session Identifier
SigG	Signaturgesetz
SIGMUND	Semantik- und emotionsbasiertes Gesprächsmanagement in der Kundenberatung
SSL	Secure Sockets Layer
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
str.	strittig
StrÄndG	Strafrechtsänderungsgesetz
st. Rspr.	ständige Rechtsprechung
TK-	Telekommunikations-
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TÜV	Technischer Überwachungs-Verein
TVG	Tarifvertragsgesetz
UN	United Nations
Unterabs.	Unterabsatz
URL	Uniform Resource Locator
Urt. v.	Urteil vom
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom/von
vgl.	vergleiche
VoIP	Voice over IP
VPN	Virtual Private Network
VR	Verwaltungsrundschau (Zeitschrift)
vs.	versus
VuR	Verbraucher und Recht (Zeitschrift)
WiPrO	Wirtschaftsprüferordnung
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht (Zeitschrift)
WWW	World Wide Web
ZAW	Zentralverband der deutschen Werbewirtschaft e. V.
Ziff.	Ziffer(n)
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)

ZUM	Zeitschrift für Urheber- und Medienrecht (Zeitschrift)
ZUM-RD	Zeitschrift für Urheber- und Medienrecht – Rechtsprechungsdienst (Zeitschrift)

1 Einführung

Steigender Wettbewerbsdruck, das Streben nach Effizienzgewinnen und die Möglichkeit zur Kostenreduzierung veranlassen nichtöffentliche Unternehmen hauptsächlich, ihre Kommunikationsschnittstelle zu den (potenziellen) Kunden[1] auf unternehmensinterne oder -externe Callcenter zu übertragen.

Im Zusammenhang mit den Schlagworten Bürgerfreundlichkeit und Verwaltungseffizienz ist derselbe Verlagerungsprozess bei Organisationen des öffentlichen Rechts festzustellen. Der Kontakt beispielsweise zu Behörden soll durch den Einsatz von Callcentern vereinfacht werden. Ein wesentlicher Vorteil für Bürger[2] besteht etwa in der durchgängigen Erreichbarkeit einer Behörde. Somit lassen sich bestimmte Verwaltungsvorgänge auch außerhalb der regulären Geschäftszeiten erledigen, während dagegen zu den üblichen Geschäftszeiten eine Vielzahl der Bürger ihrer Beschäftigung nachgehen muss.

Allgemein sind unter den Begriff „Callcenter“ selbstständige Organisationseinheiten zu fassen, deren Mitarbeiter unter Einsatz moderner Informations- und Kommunikationstechnik serviceorientierte und effiziente Dialoge mit den Gesprächspartnern führen.[3] Diese Kommunikation der Callcenter-Mitarbeiter ist durch einen hohen Grad an Wirtschaftlichkeit geprägt. In vielen Fällen existieren präzise Vorgaben zur Qualität und Quantität der Telefonate. Das Zusammenspiel von Technik und Organisation erlaubt eine rationalisierte Massenabwicklung von über das Telefon angebotenen Dienstleistungen und die Ausweitung der Erreichbarkeit der Organisation.[4]

Callcenter bieten ihre Telefondienste vorrangig in den Bereichen Bestellabwicklung, Beschwerdemanagement, Kundenrückgewinnung, Beratung, Werbung, Kundendienst und Verkauf an. Grundsätzlich voneinander zu unterscheiden sind Callcenter, die aktiv (potenzielle) Kunden anrufen (Outbound-Telefonie), und Callcen-

[1] Der verwendete Terminus „Kunden“, etwa im Zusammenhang mit „Kundendaten“, steht als Synonym für alle denkbaren Gesprächspartner des Callcenters. Die Gesprächspartner müssen nicht zwangsläufig Kunden im engeren Sinne sein. Das Gesprächsmanagement-System soll gleichermaßen in der öffentlichen Verwaltung – mit einer völlig anderen Zielgruppe – eingesetzt werden.
[2] Wegen der einfacheren Lesbarkeit wird auf die Differenzierung zwischen weiblicher und männlicher Form verzichtet; die jeweilige Nennung der männlichen Form umfasst stets beide Geschlechter.
[3] *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 21.
[4] *Menzler-Trott/Hasenmaile,* Arbeitnehmer im Call-Center, 2000, 24.

ter, die Anrufe entgegennehmen (Inbound-Telefonie), sowie Mischformen der genannten Ausprägungen.[5]

Zur Systematisierung der Kundenbeziehungen kommen Customer Relationship Management-Systeme (CRM-Systeme) zum Einsatz. Dazu werden die gesammelten Daten miteinander verknüpft und nach verschiedenen Kriterien ausgewertet. Auch die Anreicherung der Kundendaten im CRM-System mit Informationen aus externen Datenquellen stellt eine Möglichkeit dar, weitere für das Unternehmen nutzbringende Erkenntnisse zu gewinnen.[6]

Das Anbieten von Callcenter-Dienstleistungen und die Nutzung von CRM-Systemen werfen bereits jeweils für sich eine Vielzahl datenschutzrechtlicher Fragen auf. Die Besonderheit des zu untersuchenden Gesprächsmanagement-Systems besteht in der innovativen Verknüpfung der beiden Elemente, die eine gesprächsbegleitende, situative Echtzeitunterstützung des Beraters, primär auf Grundlage der Informationen aus der CRM-Datenbank, realisieren soll. Dies erfordert in erheblichem Umfang die automatisierte Analyse des Verhaltens der Kunden und Berater, des Gesprächsgegenstands sowie des gesamten Kontexts des Kundenkontakts (wie Bestellhistorie des Kunden, frühere Kommunikation mit dem Kunden).

1.1 Untersuchungsgegenstand und Ziel der Arbeit

Das Datenschutzrecht dient allgemein dem Schutz der informationellen Selbstbestimmung des Einzelnen: Jedermann soll selbst über die Preisgabe und Verwendung seiner Daten bestimmen können.[7] Datenschutzgesetze sind sowohl Schutzgesetze, die dem Schutz natürlicher Personen dienen, als auch Eingriffsgesetze, die unter bestimmten Voraussetzungen Eingriffe in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG gestatten.[8]

Die folgende Untersuchung zeigt einerseits den bestehenden datenschutzrechtlichen Rahmen auf, der beim Betrieb des Gesprächsmanagement-Systems eingehalten werden muss. Die Beachtung der gesetzlichen Rahmenbedingungen ist zunächst unabdingbare Voraussetzung für den praktischen Einsatz des Gesamtsystems. Ein hohes Maß an Datenschutz dient ferner der Akzeptanzsicherung bei einer mittlerweile in Bezug auf den Datenschutz sensibilisierten Bevölkerung. Gerade vor dem Hinter-

[5] Gola, Datenschutz im Call Center, 2. Aufl. 2006, 4.
[6] *Baumgärtner et al.*, DSB 4/2004, 9.
[7] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 1 Rn. 23 ff.
[8] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 1 Rn. 4 f.

grund einer anzustrebenden Zertifizierung ist größter Wert auf die strikte Einhaltung datenschutzrechtlicher Regelungen zu legen.

Andererseits erfolgt die Ableitung von Vorschlägen zur datenschutzgerechten Gestaltung des Systems anhand einer systembezogenen Projektion und erweiterten Umsetzung des datenschutzrechtlichen Schutzkonzepts.[9] Das Datenschutzrecht enthält zentrale Grundsätze, deren Realisierungsgrad im konkreten Fall sich auf die gewährleistete Intensität des Schutzes der informationellen Selbstbestimmung der Betroffenen auswirkt. So soll durch geeignete Vorschläge zur technischen und organisatorischen Verwirklichung des Systems – unter Einhaltung eines verhältnismäßigen Aufwands – das größtmögliche Maß an Datenschutz erzielt werden.

An den genannten zwei wesentlichen Intentionen der vorliegenden Arbeit lässt sich erkennen, dass es zunächst darum geht, den Betrieb des gesamten Gesprächsmanagement-Systems rechtmäßig, das heißt ohne Verstöße gegen Gesetze, einzurichten. Darüber hinaus ist die eingesetzte Technik dahingehend zu optimieren, dass sie sich nicht nur als nicht rechtswidrig auszeichnet, sondern vielmehr ein Idealmaß an Rechtsverträglichkeit erreicht.

Die nachfolgend durchgeführte rechtliche Beurteilung für den Einsatz des Gesprächsmanagement-Systems in nichtöffentlichen Organisationen sowie in öffentlichen Stellen des Bundes erfolgt auf Grundlage der Vorschriften des Bundesdatenschutzgesetzes. Daneben existieren öffentlich-rechtliche Callcenter, die von Landeseinrichtungen betrieben werden. Für sie gelten die jeweiligen Landesdatenschutzgesetze. Diese sind zwar nicht deckungsgleich mit dem Bundesdatenschutzgesetz, dennoch enthalten sie dasselbe Schutzprogramm wie das bundesgesetzliche Pendant, sodass stets ein einheitliches Schutzniveau gegeben ist. Es werden nur dort exemplarisch Landesregelungen zum Datenschutz aufgezeigt, wo sich wesentliche Unterschiede zum Bundesdatenschutzgesetz ergeben.

1.2 Gang der Untersuchung

Die vorliegende Arbeit gliedert sich in neun Kapitel.

[9] Zur systematischen Konkretisierung allgemeiner gesetzlicher Vorgaben zu technischen Gestaltungsvorschlägen wurde von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) die Methode KORA entwickelt. S. grundlegend zu KORA *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993.

Im nachfolgenden Kapitel 1.3 ist die strukturelle Zusammensetzung des Gesprächsmanagement-Systems dargestellt, um ein Verständnis für dessen Grundkonzeption herzustellen. Darüber hinaus werden die vorgesehenen Einsatzszenarien des Systems benannt.

Rechtliche Grundlagen zum Datenschutz beleuchtet Kapitel 2. Dabei wird zunächst auf die bedeutendsten internationalen Regelungen Bezug genommen. Die völkerrechtlichen Vorgaben sind in vielen Fällen zwar nicht verbindlich, dennoch gelten sie als richtungsweisend im Hinblick auf die nationale Datenschutzgesetzgebung. An die internationalen Grundlagen schließt sich die Darstellung der wichtigsten europäischen Vorschriften zum Datenschutz an. Ferner ist der rechtliche Rahmen des Datenschutzes in Deutschland dargelegt, der für die vorliegende Dissertation als maßgeblich gilt.

Kapitel 3 behandelt die datenschutzrechtlichen Regelungen, die eingehalten werden müssen, um das Gesprächsmanagement-System gegenüber der Kundenseite zulässig einzusetzen. Ausgehend von den unterschiedlichen Rechtfertigungsgrundlagen, die den Umgang mit personenbezogenen Kundendaten grundsätzlich legitimieren können, werden die datenschutzrechtlichen Zulässigkeitsvoraussetzungen für den Einsatz der einzelnen Systemkomponenten aufgezeigt. In diesem Kontext sind auch die komponentenspezifisch ablaufenden Datenverarbeitungsprozesse beschrieben. Die einzelnen datenschutzrechtlichen Anforderungen an die jeweiligen Systemkomponenten lassen sich aggregieren. Diese in Kapitel 3 enthaltene Zusammenführung gilt als Voraussetzung für die Zulässigkeit des Einsatzes des gesamten Systems. Im dritten Kapitel sind darüber hinaus bestimmte Informationspflichten des Callcenters, die Rechte der Kunden sowie geeignete Maßnahmen zur Authentifizierung von Kunden beschrieben. Neben den datenschutzrechtlichen Vorgaben werden weitere kundenschützende Regelungen aufgezeigt, die im Zusammenhang mit Callcenter-Dienstleistungen Relevanz erlangen.

In Kapitel 4 sind die Vorschriften dargelegt, die allgemein beim Umgang mit personenbezogenen Daten der Beschäftigten beachtet werden müssen. Dabei wird zwischen der aktuellen und der zu erwartenden Rechtslage differenziert – die Regelungsmaterie des Beschäftigtendatenschutzes steht vor ihrer Novellierung. Neben den Informationspflichten, denen der Callcenter-Betreiber gegenüber den Beschäftigten unterliegt, und den Rechten der Beschäftigten sind die bedeutsamsten Kontrollmaßnahmen hinsichtlich des Verhaltens oder der Leistung der Beschäftigten – zusammen mit einer datenschutzrechtlichen Beurteilung – dargestellt. Darüber hinaus werden weitere Vorschriften behandelt, die es im Kontext der Einführung und

Nutzung des Gesprächsmanagement-Systems zum Schutz der Beschäftigten zu beachten gilt. Daran schließt sich die Erläuterung der Rechte des Arbeitgebers an.

Kapitel 5 zeigt zunächst auf, unter welchen Voraussetzungen der Callcenter-Betreiber das Fernmeldegeheimnis bei der Telekommunikation seiner Beschäftigten beachten muss. Neben den allgemeinen Datenschutzvorschriften existieren bereichsspezifische Regelungen zum Datenschutz im Hinblick auf die Telekommunikation; diese werden ebenfalls im fünften Kapitel beleuchtet. Weitergehend ist das grundsätzliche Verbot der Rufnummerunterdrückung durch Callcenter bei der Durchführung von Werbekampagnen Gegenstand der Betrachtung. Überdies wird das strafrechtlich abgesicherte Verbot des heimlichen Abhörens und Mitschneidens von Telefonaten behandelt.

Die erforderlichen technischen und organisatorischen Vorkehrungen, die ein hohes Maß an Datenschutz und Datensicherheit herstellen sollen, sind in Kapitel 6 erläutert. Neben dem Erfordernis der Verpflichtung der Mitarbeiter zur Einhaltung des Datengeheimnisses sind bestimmte, gesetzlich verankerte Schutzmaßnahmen durch den Callcenter-Betreiber zu treffen.

Um die von Datenverarbeitungsvorgängen Betroffenen bei der Ausübung ihrer Rechte zu unterstützen, existieren institutionalisierte Kontrollorgane. Sie kontrollieren die Einhaltung des Datenschutzes und sollen das informationelle Selbstbestimmungsrecht der Betroffenen sicherstellen. Grundlegend voneinander zu unterscheiden sind organisationsinterne Kontrollorgane und den verantwortlichen Stellen übergeordnete externe Kontrolleinrichtungen. Die Aufgaben und die Charakteristika der jeweiligen Kontrollinstitutionen werden in Kapitel 7 dargelegt.

Kapitel 8 zeigt zunächst Vorschläge für die technische Gestaltung des Gesprächsmanagement-Systems und für die Implementierung organisatorischer Vorkehrungen innerhalb des Callcenter-Betriebs auf, die beiderseits zur Einhaltung eines hohen Datenschutzniveaus bei der Nutzung des Systems führen. Überdies thematisiert dieses Kapitel das im Rahmen der Untersuchung erkannte Optimierungspotenzial in Bezug auf das geltende Datenschutzrecht. Es werden Empfehlungen für rechtliche Regelungen ausgesprochen.

In Kapitel 9 erfolgt eine Schlussbetrachtung. Hier sind grundlegende Erkenntnisse, die aus der vorliegenden Arbeit resultieren, prägnant zusammengefasst.

1.3 Grundlagen zum Gesprächsmanagement-System

Das Gesprächsmanagement-System soll sowohl bei Callcentern zur Anwendung gelangen, die privatwirtschaftlich organisiert sind, als auch bei solchen, die zur öffentlichen Verwaltung gehören. Die Callcenter-Dienstleistung kann dabei grundsätzlich im Bereich der Inbound- oder Outbound-Kommunikation sowie in einer Mischform bestehen, wobei der hauptsächliche Anwendungsbereich des Gesprächsmanagement-Systems in der Unterstützung der Callcenter-Agenten im Rahmen der Inbound-Telefonie liegt.

Während bei der Outbound-Kommunikation in der Regel bereits Kundeninformationen existieren, die zur Unterstützung des Gesprächs genutzt werden können oder das Kampagnenmanagement eine bestimmte Vorgehensweise vorgibt, sind es gerade beim Callcenter eingehende Telefonate, die Schwierigkeiten bereiten; dies gilt insbesondere dann, wenn im Vorfeld des Anrufs noch kein Kontakt bestanden hat.[10] Das ideale Anwendungsgebiet des Gesprächsmanagement-Systems ist ein solches, bei dem der Gesprächsablauf nicht oder kaum standardisiert werden kann. Exemplarisch lassen sich hierzu die telefonisch realisierbaren Dienstleistungen

- Beratung,
- Kundendienst,
- Beschwerdemanagement sowie
- Kundenbetreuung

anführen.

Die gesprächsbegleitende, situationsabhängige Bereitstellung von Informationen für den Callcenter-Agenten stellt einen innovativen Ansatz zur Optimierung von Callcenter-Prozessen dar. Wenn dem Mitarbeiter des Callcenters während des gesamten Gesprächskontakts ständig aktualisierte gesprächsrelevante Informationen vorlägen, führte dies zu erheblichen Effizienzsteigerungen. Diese technologische Lücke versucht das Gesprächsmanagement-System zu schließen.[11]

Die Zwecksetzung des Einsatzes des Gesprächsmanagement-Systems besteht in der automatisierten Erkennung der für das Kundengespräch relevanten Informationen, die dem Callcenter-Berater in Echtzeit während des laufenden Kundengesprächs zur Verfügung gestellt werden sollen.

[10] *o. V.*, Vorhabensbeschreibung des Forschungsprojekts SIGMUND, 2008, 1.
[11] *o. V.*, Vorhabensbeschreibung des Forschungsprojekts SIGMUND, 2008, 1.

Die nachstehende Abbildung veranschaulicht den strukturellen Zusammenhang der einzelnen Komponenten, die das Gesprächsmanagement-System umfasst:

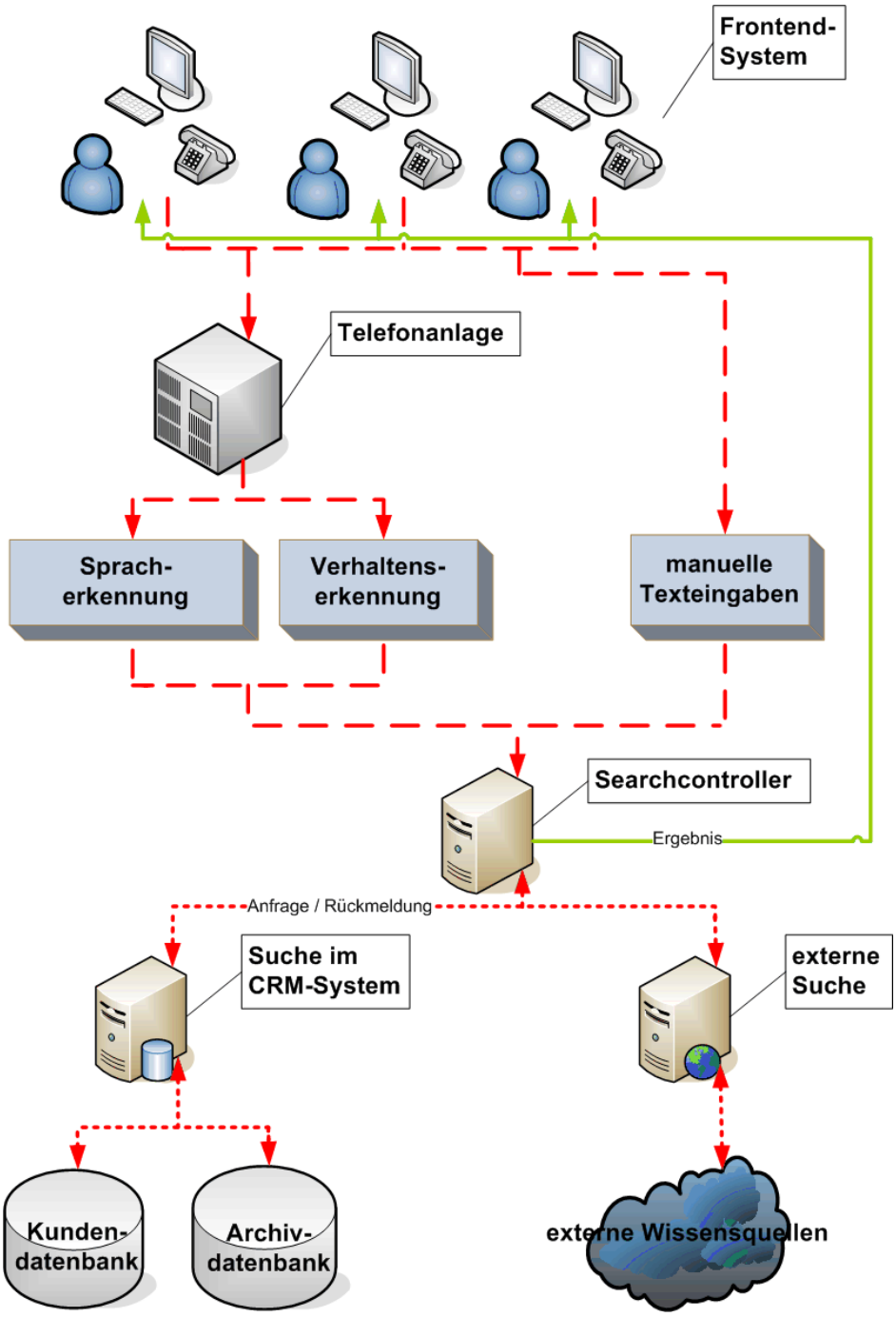

Abb. 1: Struktur des Gesprächsmanagement-Systems.
Quelle: Der Verfasser.

In der Darstellung sind oben die Callcenter-Agenten an ihrem Frontend-System im Callcenter-Betrieb abgebildet. Die zentrale Steuerung und Koordination ein- und ausgehender Telefongespräche übernimmt die Telefonanlage: Mit der sogenannten

ACD-Funktion lassen sich Anrufe nach vorab bestimmbaren Regeln auf die Mitarbeiter verteilen. Als systeminterne Signalübertragungstechnik gelangt VoIP (Voice over IP) zum Einsatz. Der Livestream der laufenden Telefongespräche wird an der Telefonanlage abgegriffen und der Sprach- sowie Verhaltenserkennung zugeführt. Von diesen automatisierten Analysen sind sowohl der Agenten- als auch der Kundenkanal betroffen. Die Callcenter-Agenten besitzen darüber hinaus jederzeit die Möglichkeit, mittels Freitextsuche nach relevanten Informationen zu recherchieren. Die durch Sprach- und Emotionserkennung extrahierten Informationen sowie gegebenenfalls die manuellen Eingaben der Callcenter-Agenten werden an den Searchcontroller geleitet, der Suchaufträge im angeschlossenen CRM-System und in externen Wissensquellen auslöst. Das CRM-System umfasst eine Kundendatenbank und eine Archivdatenbank. In der Kundendatenbank sind kundenindividuelle Informationen, von beispielsweise Bestellhistorie und Kontaktdaten bis hin zum verdichteten Kundenprofil, gespeichert. Die Archivdatenbank dagegen kann Dokumente jeglicher Art enthalten, die zum Beispiel einzelnen Geschäftsvorgängen oder Kunden zugeordnet oder nicht referenziert sind; sie dient im Wesentlichen der Ablage relevanter Dokumente. Der Suchprozess erstreckt sich überdies auf bestimmte öffentlich zugängliche Wissensquellen, die über das Internet erreichbar sind.

Die im Rahmen des Suchvorgangs in den angeschlossenen Quellen gefundenen „Treffer“ werden an den Searchcontroller zurückgeliefert, der die gefundenen Ergebnisse nach Relevanz sortiert und eine Ergebnisliste in Form aufrufbarer Weblinks erstellt, die auf dem Frontend-System der Callcenter-Mitarbeiter angezeigt wird. Durch Anklicken der von den Callcenter-Agenten für einschlägig erachteten Weblinks erhalten sie die gewünschten Informationen an ihrem Frontend-System dargestellt.

Der aufgezeigte Suchprozess mit Präsentation der gefundenen Suchergebnisse am Frontend-System setzt sich kontinuierlich während des laufenden Gesprächs zwischen Callcenter-Agent und Kunde fort.

Die technische Infrastruktur des Gesprächsmanagement-Systems kann sich grundsätzlich entweder vollständig beim Callcenter-Betrieb selbst befinden oder in der Form eines verteilten Systems[12] bestehen, bei dem beispielsweise sämtliche Sys-

[12] Ein „verteiltes System“ besteht aus mehreren Systemkomponenten, die erst in ihrer Gesamtheit ein System bilden. Nur durch das Zusammenspiel sämtlicher Bestandteile ist das System funktionsfähig. Es liegt eine Kopplung seiner Bestandteile vor, die durch Kooperation oder Integration eine Arbeitsweise über Rechnergrenzen und räumliche Distanzen hinweg erlaubt. *Schill/Springer*, Verteilte Systeme, 2007, 5.

temkomponenten bei spezialisierten Dienstleistungsunternehmen untergebracht sind und von diesen betrieben werden.

2 Rechtliche Grundlagen des Datenschutzes

2.1 Internationale Grundlagen

Regelungen zum Datenschutz auf internationaler Ebene sind deshalb so wichtig, weil der Datenaustausch nicht an Landesgrenzen haltmacht. Die nahezu jeden Lebensbereich durchdringende Digitalisierung von Informationen und der weltumspannende Datentransfer in Kommunikationsnetzen, insbesondere über das Internet, lässt dem globalen Datenschutz wachsenden Stellenwert zukommen. Nachfolgend sind die bedeutendsten internationalen Regelungen zum Datenschutz kurz dargestellt.

Das Übereinkommen über die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) trat für die Bundesrepublik Deutschland im Jahr 1961 in Kraft. Die OECD umfasst derzeit weltweit 32 Mitgliedstaaten und hat die zentralen Aufgaben, den Welthandel, das Wirtschaftswachstum sowie den Lebensstandard zu fördern, andere Länder in ihrer Entwicklung zu unterstützen und darüber hinaus zur finanziellen Stabilität beizutragen.[13]

Die Wichtigkeit von Regelungen zum Datenschutz auf internationaler Ebene wurde bereits früh erkannt. Die Etablierung des Datenschutzes sollte keinesfalls zu einem Handelshemmnis führen.[14] Im Jahr 1980 wurden die „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“ von der OECD verabschiedet. Diese Leitlinien beinhalten materielle und verfahrensrechtliche Regelungen in Bezug auf den Datenverkehr und die grenzüberschreitenden Datenübermittlungen.[15] Es handelt sich allerdings nicht um bindendes Völkerrecht. Die Mitgliedstaaten können somit selbst entscheiden, ob und inwieweit sie die Leitlinien in nationales Datenschutzrecht umsetzen.[16]

In der darauf folgenden Zeit verabschiedete die OECD aufgrund der technischen Entwicklung weitere Leitlinien, die sich mit den Themen der Kryptografie, dem Datenschutz in globalen Netzwerken, der Datenschutzerklärung, dem grenzüberschreitenden Datenaustausch sowie der Datensicherheit befassen.[17]

---

[13] *OECD*, About the Organisation for Economic Co-operation and Development (OECD), (abrufbar unter: http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html).
[14] *Burkert*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.3 Rn. 23.
[15] *Taeger/Schmidt*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, Einführung Rn. 44; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, 98.
[16] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, 98.
[17] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, 99; *Burkert*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.3 Rn. 32.

Die Vereinten Nationen (UN) setzen sich aktuell aus dem Zusammenschluss von 192 Staaten zusammen und verkörpern ein eigenständiges Völkerrechtssubjekt.[18] Zu den Hauptaufgaben der im Jahr 1945 gegründeten Organisation zählen die Sicherung des Weltfriedens, die Beschleunigung des sozialen Fortschritts, der Aufbau guter Beziehungen zwischen Nationen, die Förderung des Lebensstandards sowie die Einhaltung der Menschenrechte.[19]

Im Jahr 1990 konnten die „Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien" auf den Weg gebracht werden. Sie gelten als Empfehlungen zur Herstellung eines adäquaten Datenschutzrechts; jedoch sind auch diese Regelungen nicht rechtsverbindlich.[20]

Der Europarat mit Sitz in Straßburg umfasst mit 47 Mitgliedstaaten nahezu sämtliche Staaten Europas. Seine Gründung geht auf den 5. Mai 1949 zurück. Primäre Zielsetzungen des Europarats bestehen darin, in Europa gemeinsame und demokratische Prinzipien zu entwickeln sowie den Schutz der Menschenrechte und der Rechtsstaatlichkeit zu gewährleisten. Grundlage für diese Aufgaben stellt insbesondere die Europäische Konvention für Menschenrechte (EMRK) dar.[21]

Die „Konvention zum Schutz der Menschenrechte und Grundfreiheiten" vom 4. November 1950 enthält in Art. 8 Abs. 1 eine Regelung zum Schutz des Privat- und Familienlebens. Art. 8 Abs. 2 EMRK regelt die Voraussetzungen, unter denen eine Behörde in das Recht auf Achtung des Privat- und Familienlebens eingreifen darf.

Das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" aus dem Jahr 1981 ist ein weiterer völkerrechtlicher Vertrag des Europarats. Die Konvention wurde als verbindliches Abkommen von sämtlichen Mitgliedstaaten der EG ratifiziert. In dieser Konvention enthaltene Grundsätze bildeten teilweise die Grundlage für die EU-Datenschutzrichtlinie.[22] Weitergehende Empfehlungen ergänzen die Datenschutzkonvention in spezifischen Problemfeldern. Am 1. Juli 2004 trat ein Zusatzprotokoll zur Datenschutzkonventi-

[18] *United Nations*, UN at a Glance (abrufbar unter: http://www.un.org/en/aboutun/index.shtml).
[19] *United Nations*, UN at a Glance (abrufbar unter: http://www.un.org/en/aboutun/index.shtml); *Stein/von Buttlar*, Völkerrecht, 11. Aufl. 2005, Rn. 393 ff.
[20] *Taeger/Schmidt*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, Einführung Rn. 45; *Moos*, in: Kröger/Gimmy (Hrsg.), Handbuch zum Internetrecht, 2. Aufl. 2002, 757 (775).
[21] *Europarat*, Der Europarat in Kürze (abrufbar unter: http://www.coe.int/aboutCoe/index.asp?page= nepasconfondre&l=de und http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=de).
[22] *Gola/Klug*, Grundzüge des Datenschutzrechts, 2003, 31.

on in Kraft, das die Einrichtung von Kontrollstellen und den grenzüberschreitenden Datenverkehr zum Gegenstand hat.[23]

2.2 Europäische Grundlagen

Europäische Rechtsvorschriften sind im Bereich des Datenschutzes von zunehmender Bedeutung. Sie regeln den grenzüberschreitenden Austausch personenbezogener Daten innerhalb der EU und versuchen der Tatsache Rechnung zu tragen, dass die ausgetauschte Datenmenge innerhalb des europäischen Binnenmarkts künftig weiter anwachsen wird.

Nachfolgend werden die bedeutendsten Vorschriften zum Datenschutz auf europäischer Ebene skizziert.

2.2.1 Grundrechtecharta der EU

Auf der Ebene des primären europäischen Rechts sind in der Charta der Grundrechte der EU sämtliche bürgerlichen, politischen, wirtschaftlichen und sozialen Rechte zusammengefasst, die europäischen Bürgern sowie allen im Hoheitsgebiet der EU lebenden Personen zustehen.[24] Die Charta wurde mit dem Vertrag von Lissabon zur Änderung des Vertrages über die EU und des Vertrages zur Gründung der EG am 1. Dezember 2009 für die Institutionen der EU sowie die einzelnen Mitgliedstaaten verbindlich. Die EU erkennt die in der Charta der Grundrechte der EU verankerten Rechte, Freiheiten und Grundsätze an.[25]

Die Charta der Grundrechte der EU enthält in Art. 8 eine eigenständige Vorschrift zum Datenschutz. Nach Art. 8 Abs. 1 GRC hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Art. 8 Abs. 2 GRC enthält weitergehend eine grundlegende Vorschrift zur Verarbeitung personenbezogener Daten: Die personenbezogene Datenverarbeitung darf nur nach Treu und Glauben und für festgelegte Zwecke erfolgen. Darüber hinaus muss eine Legitimation entweder aus einer Einwilligung des Betroffenen oder aus einer gesetzlichen Grundlage vorliegen. Überdies besteht ein Auskunfts- und Berichtigungsrecht des Betroffenen.

[23] *Siemen*, Datenschutz als europäisches Grundrecht, 2006, 41 f.
[24] *Europäisches Parlament*, Charta der Grundrechte der Europäischen Union (abrufbar unter: http://www.europarl.europa.eu/charter/default_de.htm).
[25] *Polenz*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Rn. 2.

Die Regelung des Art. 8 GRC hat engen Bezug zu Art. 7 GRC, der die Achtung des Privat- und Familienlebens unter Schutz stellt.[26]

2.2.2 Datenschutzrichtlinie

Richtlinien zählen insbesondere neben Verordnungen und Entscheidungen zum sogenannten sekundären Gemeinschaftsrecht. Sie gelten gemäß Art. 249 EG für die Mitgliedstaaten, an die sie adressiert sind, als verbindlich im Hinblick auf die Zielerreichung. Über die Form und Mittel zur Erreichung dieser Ziele können die innerstaatlichen Stellen selbst entscheiden.

Da ein einheitliches Schutzniveau die Grundlage für den grenzüberschreitenden Datenverkehr in der Gemeinschaft ist, wurde ein solches mit der Datenschutzrichtlinie[27] hergestellt. Die unterschiedlichen Datenschutzgesetze auf nationaler Ebene behinderten zuvor den freien Datenaustausch. Sie boten weder ausreichenden Grundrechtsschutz noch Rechtssicherheit für die Beteiligten.[28] In Deutschland erfolgte die Umsetzung der Datenschutzrichtlinie mit dem Bundesdatenschutzgesetz (BDSG 2001).[29]

Die Datenschutzrichtlinie gilt nach Art. 3 Abs. 1 für die vollständig oder nur teilweise automatisierte Verarbeitung personenbezogener Daten. Ebenso ist die nicht automatisierte Verarbeitung personenbezogener Daten, die in Dateien gespeichert sind oder werden sollen, von ihr erfasst.

Erwägungsgrund Nr. 10 der Datenschutzrichtlinie verdeutlicht, dass die Angleichung der einzelstaatlichen Rechtsvorschriften zum Datenschutz nicht zur Unterschreitung des bereits bestehenden Schutzniveaus führen darf. Vielmehr soll ein höherer Schutzstandard erreicht werden. Die Richtlinie lässt also eine Öffnung nach oben hin zu, während die Reduzierung des existierenden Datenschutzniveaus unzulässig ist.[30]

---

[26] *Bernsdorff*, in: Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 2003, Art. 8 Rn. 13.
[27] Richtlinie 95/46/EG v. 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
[28] *Polenz*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Rn. 3.
[29] *Polenz*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Rn. 3.
[30] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 132.

2.2.3 Datenschutzrichtlinie für elektronische Kommunikation

Die Datenschutzrichtlinie für elektronische Kommunikation[31] vom 12. Juli 2002 dient gemäß ihres Art. 1 Abs. 1 und Abs. 2 der Sicherstellung eines einheitlichen Schutzniveaus der Mitgliedstaaten im Bereich der elektronischen Kommunikation sowie der Gewährleistung des freien Datenverkehrs und freien Verkehrs von Kommunikationsgeräten und -diensten. Der Schutz der Privatsphäre soll dabei im Vordergrund stehen. Die Datenschutzrichtlinie für elektronische Kommunikation präzisiert und ergänzt die allgemeine Datenschutzrichtlinie, indem sie bereichsspezifische Detailregelungen enthält.[32]

Ein bedeutendes Charakteristikum dieser Richtlinie ist ihre Technologieoffenheit: Ihr primäres Ziel ist, ein einheitliches Datenschutzniveau für sämtliche denkbaren Arten der elektronischen Kommunikation sicherzustellen. Dieses Anliegen wird in Erwägungsgrund Nr. 4 der Richtlinie hervorgehoben.[33]

Durch Art. 3 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation ist vorgesehen, dass die Vorschriften der Richtlinie nur für die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste gelten, die in öffentlichen Kommunikationsnetzen angeboten werden. Vom deutschen Telekommunikationsgesetz wird hingegen auch der Datenschutz gegenüber geschlossenen Benutzergruppen erfasst. Insoweit bietet das deutsche telekommunikationsspezifische Datenschutzrecht einen höheren Schutzstandard als die Richtlinie.[34]

Die Datenschutzrichtlinie für elektronische Kommunikation beinhaltet insbesondere Regelungen über die Sicherheit der Kommunikationsnetze und die Vertraulichkeit der Kommunikation, über Verkehrsdaten, über den Einzelgebührennachweis, die Rufnummeranzeige und -unterdrückung, über Standortdaten, Teilnehmerverzeichnisse, die automatische Anrufweiterleitung sowie über unerbetene Nachrichten.

[31] Richtlinie 2002/58/EG v. 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.
[32] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 135.
[33] *Büttgen*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 28. Ergänzungslieferung 2011, Teil 16.3 Rn. 23; *Zilkens*, RDV 2007, 196 (198).
[34] *Büttgen*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 28. Ergänzungslieferung 2011, Teil 16.3 Rn. 24.

2.3 Nationale Grundlagen

2.3.1 Verfassungsrechtliche Ebene

Grundrechte stellen in erster Linie Abwehrrechte der Bürger gegenüber dem Staat dar; dennoch enthalten sie eine objektive Wertordnung, die in sämtliche Bereiche des Rechts hineinwirkt.[35] Die im Grundgesetz verankerten Wertvorstellungen gilt es daher auch bei der Anwendung zivilrechtlicher Vorschriften zu berücksichtigen. Möglich und geboten ist dies besonders bei der Konkretisierung von Generalklauseln und der Auslegung unbestimmter Rechtsbegriffe. Derartige Einbruchstellen im Privatrecht erlauben es, dass Grundrechte eine mittelbare Wirkung in privatrechtlichen Beziehungen entfalten.[36]

Die Thematik der vorliegenden Arbeit wird insbesondere von vier Grundrechten umfasst:

- Recht auf informationelle Selbstbestimmung,
- Recht am eigenen Wort,
- Recht auf kommunikative Selbstbestimmung und
- Fernmeldegeheimnis.

Diese Grundrechte werden nachfolgend betrachtet.

2.3.1.1 Recht auf informationelle Selbstbestimmung

Im Volkszählungsurteil[37] leitete das *BVerfG* das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG ab. Dieses für den Datenschutz bedeutsame Urteil bestimmt das Grundrecht auf informationelle Selbstbestimmung grundlegend; weitere Entscheidungen haben dieses Recht bestätigt und konkretisiert.[38]

Eine Gesellschaftsordnung, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“, wäre mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Wer unsicher ist, ob sein abweichendes

[35] *BVerfG* v. 15.1.1958, NJW 1958, 257 ff.
[36] MüKo-BGB/*Koch*, Band 7/1, Einleitung Rn. 196.
[37] *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[38] *Schmitz*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 28. Ergänzungslieferung 2011, Teil 16.2, Rn. 17 f.; *Trute*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.5 Rn. 7.

Verhalten zu negativen Konsequenzen führt, wird unter Umständen auf die Ausübung seiner Grundrechte verzichten.[39]

Das informationelle Selbstbestimmungsrecht wird allerdings nicht unbeschränkt gewährleistet: Einschränkungen kommen bei Vorliegen eines überwiegenden Allgemeininteresses in Betracht. Darüber hinaus bedürfen die Beschränkungen einer verfassungsgemäßen gesetzlichen Grundlage, die dem Gebot der Normenklarheit genügen muss und den Grundsatz der Verhältnismäßigkeit beachtet.[40]

Unter den Bedingungen der modernen Datenverarbeitung hat der Schutz jedes Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten als Voraussetzung für die freie Persönlichkeitsentfaltung zu gelten. Das informationelle Selbstbestimmungsrecht garantiert diesen Schutz: Es „gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Auf die Art der Daten kommt es dabei nicht an; ihre Nutzbarkeit und Verwendungsmöglichkeit stellen die ausschlaggebenden Faktoren dar. Diese werden bestimmt durch den Zweck der Datenerhebung sowie durch die Verknüpfungs- und Verarbeitungsmöglichkeiten der Informationstechnologie. Daher gilt es zu berücksichtigen, dass unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum mehr existiert. Einem für sich gesehen belanglosen Datum kann ein vollkommen höherer Stellenwert zukommen.[41]

Im Regelfall wird der Einzelne gar nicht wissen, welche Daten bei welchen Stellen über ihn gesammelt werden und wo er elektronische Spuren hinterlässt. Eine systematische Datensammlung und -auswertung kann ihn zum bloßen Objekt staatlicher Stellen oder wirtschaftlicher Marketingstrategen degradieren.[42]

Aufgrund seiner Bedeutung wird teilweise gefordert, das Recht auf informationelle Selbstbestimmung als eigenständiges Grundrecht im Grundgesetz zu verankern.[43]

[39] *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[40] *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[41] *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[42] Maunz/Dürig-*Di Fabio*, GG, Band I, 61. Ergänzungslieferung, Stand: Januar 2011, Art. 2 Rn. 173.
[43] So etwa die Bundestagsfraktion Bündnis 90/Die Grünen, s. http://www.gruene-bundestag.de/cms/archiv/dok/275/275880.fundamente_der_freiheit_staerken-print~11.html.

2.3.1.2 Recht am eigenen Wort

Auch das Recht am eigenen Wort ist eine spezifische Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 und 1 Abs. 1 GG. Es umfasst die grundsätzliche Befugnis, selbst zu entscheiden, ob Gesprächsinhalte oder Inhalte von Schriftstücken nur dem Gesprächspartner beziehungsweise dem Adressaten oder weitergehend einem bestimmten Kreis von Personen oder sogar der Öffentlichkeit zugänglich sein sollen.[44] Erst recht beinhaltet es das grundsätzlich alleinige Bestimmungsrecht einer Person darüber, ob ihr nichtöffentlich gesprochenes Wort mittels Tonträger festgehalten und ob und von wem diese Aufzeichnung angehört werden darf.[45]

Die Vertraulichkeit des nichtöffentlich gesprochenen Wortes zählt zum Schutz der Selbstdarstellung und der Integrität der Privatsphäre. Eine Störung des Kommunikationsprozesses liegt insbesondere vor, wenn kein unbefangener Austausch zwischen den Beteiligten stattfinden kann, weil zu befürchten steht, dass unbedachte oder spontane Äußerungen aufgenommen und gegebenenfalls später veröffentlicht oder verwertet werden.[46]

Das Recht am gesprochenen Wort bietet Schutz vor dem Anbringen und Nutzen einer Mithöreinrichtung, die ein Kommunikationspartner einem nicht am Gespräch Beteiligten bereitstellt.[47] Ferner schützt dieses Recht vor Falschzitaten:[48] Der Grundrechtsträger ist davor geschützt, dass ihm Äußerungen zugeschrieben werden, die er nicht getätigt hat und die seinen sozialen Geltungsanspruch schädigen.[49]

2.3.1.3 Recht auf kommunikative Selbstbestimmung

Jede Kommunikation enthält prinzipiell die Komponente der individuellen Selbstdarstellung. Dies gilt selbst für betrieblich oder dienstlich motivierte Kommunikationsvorgänge. Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG schützt nicht nur die Privat- und Intimsphäre von Individuen, sondern enthält

[44] *BGH* v. 18.2.2003, NJW 2003, 1727 ff.; *Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BGB, § 823 Rn. 30; *Kläver*, DuD 2003, 228 (229 f.).
[45] Maunz/Dürig-*Di Fabio*, GG, Band I, 61. Ergänzungslieferung, Stand: Januar 2011, Art. 2 Rn. 196; *BVerfG* v. 31.1.1973, NJW 1973, 891 ff.
[46] Maunz/Dürig-*Di Fabio*, GG, Band I, 61. Ergänzungslieferung, Stand: Januar 2011, Art. 2 Rn. 196.
[47] *BVerfG* v. 9.10.2002, ZUM-RD 2003, 57 ff.
[48] Maunz/Dürig-*Di Fabio*, GG, Band I, 61. Ergänzungslieferung, Stand: Januar 2011, Art. 2 Rn. 199.
[49] *BVerfG* v. 3.6.1980, NJW 1980, 2072 ff.

auch einen Anspruch auf Schutz im Hinblick auf die wesentlichen Voraussetzungen für das Agieren in Beziehungen mit bekannten und unbekannten Dritten sowie in der Öffentlichkeit.[50]

Das kommunikative Selbstbestimmungsrecht[51] ist eine Konkretisierung des allgemeinen Persönlichkeitsrechts als dogmatische Weiterentwicklung für den spezifischen Fall der Telekommunikation.[52] Dieses Recht schützt die Identitätsbildung und Selbstdarstellung von Personen im Telekommunikationsprozess. Die eingesetzte Telekommunikationstechnik hat unmittelbare Auswirkungen auf die sozialen Bedingungen für die freie Entscheidungs- und Entfaltungsmöglichkeit ihrer Nutzer, weil sie in die konkrete Kommunikation eingreift und diese bestimmt. Aus diesem Grund umfasst das allgemeine Persönlichkeitsrecht in seinem kommunikativen und sozialen Aspekt das Recht zur autonomen Selbstdarstellung in der Kommunikation.[53]

Autonome Selbstdarstellung, Entscheidungs- und Entfaltungsfreiheit setzen Selbstbestimmung in der Kommunikation mit anderen voraus. Das kommunikative Selbstbestimmungsrecht umfasst daher nicht nur das Recht eines jeden Einzelnen, sich für oder gegen einen Kommunikationsvorgang zu entscheiden, in dem sich das Individuum selbst darstellen kann, und den Inhalt der Kommunikation selbst zu bestimmen. Es beinhaltet weiterreichend die freie Wahl

- des Kommunikationspartners,
- des Kommunikationsorts,
- der Kommunikationsart und
- des Kommunikationsmediums.[54]

Genau wie bei der Kommunikation ohne technisches Medium muss bei einer Telekommunikation sichergestellt sein, dass über ihre konkreten Umstände selbstbestimmt entschieden werden kann. Die eingesetzte Kommunikationstechnik darf eine generell gewährleistete Freiheit nicht einschränken.[55]

[50] *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 58 f.
[51] Dazu ausführlich *Roßnagel*, KJ 1990, 267 ff.
[52] *Hornung*, MMR 2004, 3 (4).
[53] *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 58.
[54] *Brisch/Laue*, MMR 2009, 813 (816); *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 59.
[55] *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 59.

2.3.1.4 Fernmeldegeheimnis

Art. 10 Abs. 1 GG dient unter anderem dem Schutz des Fernmeldegeheimnisses. Dieses Grundrecht gewährleistet die freie Entfaltungsmöglichkeit der Persönlichkeit durch einen privaten – und damit der Öffentlichkeit verborgenen – Austausch von Informationen. Wenn sich die an der Kommunikation Beteiligten nicht an demselben Ort befinden und auf die Informationsübermittlung durch andere angewiesen sind, schafft das Fernmeldegeheimnis Vertraulichkeit der individuellen Kommunikation. Die private Fernkommunikation ist vor dem Zugriff Dritter und dem staatlicher Stellen geschützt.[56]

Die Verletzlichkeit des Fernmeldegeheimnisses erfährt dadurch eine Steigerung, dass Eingriffe regelmäßig heimlich und für den Grundrechtsträger nicht erkennbar stattfinden können. Der Schutzbereich des Fernmeldegeheimnisses erstreckt sich auf die gesamten Umstände der Kommunikation.[57] Dabei ist es vollkommen unerheblich, welche Übermittlungsart (zum Beispiel über Funk, kabelgebunden, analog oder digital) zum Einsatz gelangt und welche konkrete Ausdrucksform (etwa Sprache, Töne oder Bilder) gewählt wird.[58] Erfasst sind nicht nur die Kommunikationsinhalte selbst, sondern auch sämtliche äußeren Umstände der Kommunikation. Dazu zählen hauptsächlich Informationen darüber, wer, wann, wie oft und wie lange mit wem kommuniziert hat oder versucht hat, zu kommunizieren.[59] Die Kommunikationsverbindungsdaten besitzen einen eigenen Aussagegehalt und ermöglichen grundsätzlich Rückschlüsse auf das Kommunikations- und Bewegungsverhalten: Informationen über die Häufigkeit und Dauer sowie die Zeitpunkte der Kommunikation lassen die Art und Intensität von Beziehungen erkennen und erlauben sogar unter Umständen Schlussfolgerungen in Bezug auf die ausgetauschten Inhalte.[60]

Der Schutz des Fernmeldegeheimnisses endet in dem Moment, in dem der Übermittlungsvorgang beendet wurde und die Nachricht in den Herrschaftsbereich des Empfängers gelangt ist.[61] Es wird also nur der laufende Übertragungsvorgang vom Fernmeldegeheimnis umfasst, soweit die Kommunizierenden nach Abschluss des

[56] *BVerfG* v. 2.3.2006, NJW 2006, 976 ff.; BeckOK/*Baldus*, GG, Ed. 11, Stand: 1.7.2011, Art. 10 Rn. 1.
[57] Maunz/Dürig-*Durner*, GG, Band II, 61. Ergänzungslieferung, Stand: Januar 2011, Art. 10 Rn. 43 f.
[58] BeckOK/*Baldus*, GG, Ed. 11, Stand: 1.7.2011, Art. 10 Rn. 7.
[59] Maunz/Dürig-*Durner*, GG, Band II, 61. Ergänzungslieferung, Stand: Januar 2011, Art. 10 Rn. 60.
[60] Maunz/Dürig-*Durner*, GG, Band II, 61. Ergänzungslieferung, Stand: Januar 2011, Art. 10 Rn. 44; *BVerfG* v. 2.3.2006, NJW 2006, 976 ff.
[61] *BVerfG* v. 2.3.2006, NJW 2006, 976 ff.

Telekommunikationsvorgangs selbst Schutzvorkehrungen treffen können, die einen ungewollten Zugriff auf die im Gerät gespeicherten Daten verhindern.[62]

2.3.2 Einfachgesetzliche Ebene

Allgemeine und grundsätzliche Vorschriften zum Datenschutz finden sich im Bundesdatenschutzgesetz und in den Datenschutzgesetzen der Länder. Daneben existiert eine Vielzahl von bereichsspezifischen Datenschutzregelungen, die im Verhältnis zum generellen Datenschutzrecht vorrangig anzuwenden ist. Dennoch nehmen die allgemeinen Datenschutzgesetze durch ihre grundlegenden Regelungsstrukturen und Begriffe erheblichen Einfluss auf das bereichsspezifische Datenschutzrecht.[63]

2.3.2.1 Bundesdatenschutzgesetz und Landesdatenschutzgesetze

Deutschland ist ein föderativer Staat, deshalb besitzen sowohl der Bund als auch die einzelnen Länder bestimmte Kompetenzen zur Regelung des Datenschutzes.[64] Das Bundesdatenschutzgesetz wurde am 1. Februar 1977 im Bundesgesetzblatt verkündet. Vorreiter im Bereich Datenschutz war allerdings das Land Hessen, das das erste Datenschutzgesetz weltweit am 30. September 1970 verabschiedet hat.[65]

Die Etablierung des Datenschutzrechts in Deutschland stellte einen ständigen Prozess dar, der durch mehrere Umstände beeinflusst wurde. Bedeutende Ereignisse, die Anpassungsbedarf hervorgerufen haben, waren das Volkszählungsurteil[66] des *BVerfG*, in dem das Recht auf informationelle Selbstbestimmung entwickelt wurde, und das Umsetzungserfordernis der EG-Datenschutzrichtlinie. So wurde das Bundesdatenschutzgesetz aufgrund der genannten Ereignisse jeweils novelliert. Die überarbeiteten Fassungen des Gesetzes traten am 1. Juni 1991 beziehungsweise am 23. Mai 2001 in Kraft.[67]

Die Regelungen des Bundesdatenschutzgesetzes gelten gem. § 1 Abs. 2 Nr. 1 - 3 BDSG für öffentliche Stellen des Bundes, für bestimmte öffentliche Stellen der Länder und für nichtöffentliche Stellen, soweit sie personenbezogene Daten mittels

[62] *Gurlit*, NJW 2010, 1035 (1037).
[63] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Einleitung Rn. 67.
[64] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, 156.
[65] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, Einleitung Rn. 1.
[66] *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[67] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, Einleitung Rn. 1 ff.; zu der am 1. Juni 1991 in Kraft getretenen Fassung ausführlich *Büllesbach*, NJW 1991, 2593 ff.

Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder diese Vorgänge in oder aus nicht automatisierten Dateien erfolgen.

Die Landesdatenschutzgesetze regeln die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch öffentliche Stellen der Länder.[68] Die Vorschriften der einzelnen Landesbestimmungen sind vergleichbar mit denen des Bundesdatenschutzgesetzes und enthalten im Grundsatz dasselbe Schutzniveau wie ihr bundesgesetzliches Pendant.

2.3.2.2 Bereichsspezifischer Datenschutz

Mit bereichsspezifischen Datenschutzregelungen begegnet der Gesetzgeber immer komplexer werdenden Datenverarbeitungsprozessen.[69] Das Volkszählungsurteil enthält die Forderung, gesetzliche Grundlagen zu schaffen, aus denen für die Bürger klar und erkennbar hervorgehen muss, welche Beschränkungen des informationellen Selbstbestimmungsrechts sich ergeben können. Dies führte im Laufe der Zeit dazu, dass mittlerweile eine kaum mehr überschaubare Zahl an Datenschutzvorschriften existiert, die sich an den Erfordernissen ausrichten, die die jeweiligen Verarbeitungskontexte mit sich bringen.[70]

Bereichsspezifische Datenschutzregelungen gehen den Vorschriften des Bundesdatenschutzgesetzes gemäß § 1 Abs. 1 Satz 1 BDSG vor. Auch auf Landesebene existieren bereichsspezifische Regelungen zum Datenschutz.[71]

Als Normenkataloge, die bereichsspezifische Vorschriften zum Datenschutz enthalten, lassen sich beispielhaft das

- Telekommunikationsgesetz,
- Telemediengesetz,
- Melderechtsrahmengesetz,
- Passgesetz,
- Bundeszentralregistergesetz,

[68] *Helfrich*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 28. Ergänzungslieferung 2011, Teil 16.1 Rn. 25.
[69] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, 156.
[70] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, Einleitung Rn. 48 f.; *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[71] *Helfrich*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 28. Ergänzungslieferung 2011, Teil 16.1 Rn. 25.

- Bundesstatistikgesetz,
- Sozialgesetzbuch X und
- Umweltinformationsgesetz

benennen.[72]

Besondere Relevanz für die vorliegende Arbeit haben die Datenschutzbestimmungen des Telekommunikations- und des Telemediengesetzes.

2.3.3 Untergesetzliche Ebene

Im deutschen Datenschutzrecht ist vorgesehen, dass auch „andere Rechtsvorschriften" den Datenschutz reglementieren können. Als derartige andere Rechtsvorschriften sind Tarifverträge und Betriebs- oder Dienstvereinbarungen einzustufen.

2.3.3.1 Tarifverträge

Kollektivvereinbarungen können in Form von Tarifverträgen vorliegen, die gemäß § 1 Abs. 1 TVG sowohl Rechte und Pflichten der Tarifvertragsparteien regeln als auch Rechtsnormen bezüglich Fragen zu Arbeitsverhältnissen sowie bezüglich betrieblicher und betriebsverfassungsrechtlicher Aspekte enthalten können. Insoweit handelt es sich um Vereinbarungen mit schuldrechtlichem und normativem Charakter.[73]

Unter die Tarifvertragsparteien sind gemäß § 2 Abs. 1 TVG zum einen Gewerkschaften, zum anderen einzelne Arbeitgeber oder Arbeitgebervereinigungen zu fassen. Die Vorschriften eines Tarifvertrags gelten nach § 4 Abs. 1 Satz 1 TVG unmittelbar und zwingend zwischen den beiderseits Tarifgebundenen, wenn sie vom Geltungsbereich des Tarifvertrags erfasst sind.

In der Normenhierarchie stehen Tarifverträge über Betriebs- oder Dienstvereinbarungen.[74] Ihnen kommt jedoch bei der Regelung von Fragen des Datenschutzes in der Praxis kaum Bedeutung zu: Die betriebs- oder dienststellenspezifischen Gege-

[72] *Helfrich*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 28. Ergänzungslieferung 2011, Teil 16.1 Rn. 98 ff.
[73] *Kilian*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Kollektivvereinbarungen, Rn. 4.
[74] ErfK/*Franzen*, TVG, 11. Aufl. 2011, § 1 Rn. 17.

benheiten und die zur Anwendung gelangende Hard- und Software sind in der Regel derart unterschiedlich, dass ein Tarifvertrag allenfalls einen groben Rahmen vorgeben kann, der zum Beispiel anhand einer Betriebsvereinbarung zu konkretisieren ist.

2.3.3.2 Betriebs- oder Dienstvereinbarungen

Betriebs- oder Dienstvereinbarungen besitzen einen ähnlichen Charakter wie Tarifverträge. Betriebsvereinbarungen sind zweiseitige kollektive Normenverträge und beinhalten einerseits einen schuldrechtlichen Teil, der die Vertragsparteien gegenseitig verpflichtet oder berechtigt. Andererseits kommt auch ihnen normative Wirkung zu. Somit können etwa betriebsspezifische Fragen geregelt werden.[75]

Unterscheiden lassen sich Betriebsvereinbarungen in erzwingbare Vereinbarungen – für Angelegenheiten, in denen ein Mitbestimmungsrecht des Betriebsrats gegeben ist –, in freiwillige und in teilmitbestimmte Betriebsvereinbarungen.[76] Ein Mitbestimmungsrecht steht dem Betriebsrat gemäß § 87 Abs. 1 BetrVG nur insoweit zu, als keine gesetzliche oder tarifliche Regelung besteht.

Die für Betriebsvereinbarungen im privaten Bereich geltenden Grundsätze lassen sich auf Dienstvereinbarungen bei öffentlichen Stellen übertragen. In den Personalvertretungsgesetzen der Länder finden sich teilweise unterschiedliche Regelungen zur Zulässigkeit von Dienstvereinbarungen.[77]

[75] MHA/*Matthes*, Band 2, 3. Aufl. 2009, § 239 Rn. 1 ff.
[76] MHA/*Matthes*, Band 2, 3. Aufl. 2009, § 239 Rn. 3.
[77] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 77; *Kilian*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Kollektivvereinbarungen, Rn. 42.

3 Kundenbezogene Vorgaben

3.1 Kundendatenschutz

Nachfolgend ist dargestellt, was beim Umgang mit personenbezogenen Daten gemäß § 3 Abs. 1 BDSG, welche Kunden betreffen, beachtet werden muss. Unter dem Begriff „Kundendaten" sind sämtliche, einem Klienten unmittelbar und mittelbar zurechenbare Informationen zu verstehen. Bei einem unmittelbaren Kundenbezug ergibt sich die Information aus dem Datum selbst; hierbei steht fest, dass sich die Angabe nur auf eine ganz bestimmte Person bezieht.[78] Liegt hingegen ein nur mittelbarer Bezug vor, so ist die Verbindung über Zusatzwissen herstellbar.[79]

3.1.1 Zulässigkeit der Erhebung, Verarbeitung oder Nutzung von Kundendaten

Der Terminus „Umgang" mit personenbezogenen Daten, wie er in § 1 Abs. 1 BDSG verwendet wird, schließt die Vorgänge des Erhebens, Verarbeitens oder Nutzens mit ein und versteht sich somit als Oberbegriff. In § 3 BDSG sind wichtige Begriffsbestimmungen, die dem Verständnis des Bundesdatenschutzgesetzes dienen, zu Grunde gelegt. Es gilt zunächst aufzuzeigen, welche einzelnen Tätigkeiten sich hinter den Bezeichnungen „Erhebung", „Verarbeitung" und „Nutzung" verbergen, da sich diese nicht unmittelbar erschließen.

Abs. 3 des § 3 BDSG enthält die Definition der „Erhebung"; unter ihr ist das zielgerichtete Beschaffen von Daten über den Betroffenen zu verstehen. Es ist insoweit eine eigene Aktivität der verantwortlichen Stelle notwendig, mittels der sie Kenntnis von den Daten erlangt oder Verfügung über diese begründet. Keine Datenerhebung ist hingegen gegeben, wenn der verantwortlichen Stelle die Daten lediglich ohne ihr eigenes Zutun zufallen, etwa durch unverlangte Zusendung. Die Erhebung von personenbezogenen Daten muss nicht zwangsläufig zu einer Speicherung führen. Für ihr Vorliegen ist es darüber hinaus unerheblich, ob die beschafften Informationen inhaltlich genutzt werden sollen. Beispiele für Datenerhebungen sind Beobachtung einer bestimmbaren Person, Feststellung persönlicher Umstände im Rahmen einer Beratung oder Anamnese durch einen Arzt.[80] Eine Erhebung liegt

[78] *Lindner*, ZUM 2010, 292 (296).
[79] Vgl. dazu die Begriffsdefinition aus § 3 Abs. 1 BDSG: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)".
[80] Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 3 Rn. 100 ff.

vor, wenn ein Callcenter-Berater mit einem Kunden telefonisch verbunden ist, um beispielsweise einen Bestellvorgang abzuwickeln.

Unter „Verarbeiten“ ist gemäß § 3 Abs. 4 Satz 1 BDSG das Speichern, Verändern, Sperren, Löschen sowie Übermitteln von personenbezogenen Daten zu subsumieren. Der Begriff stellt eine Zusammenfassung der verschiedenen Datenverarbeitungsphasen dar.[81]

Zur Speicherung gehört das Erfassen, Aufnehmen oder Aufbewahren von Daten mit Personenbezug vor dem Hintergrund einer anschließenden Verarbeitung oder anderweitigen Nutzung. Die Erfassung und Aufnahme gilt als Fixierung der Information, beispielsweise handschriftliches Festhalten oder Aufzeichnung auf Tonband. Auch bloßes Lagern von Daten erfüllt die Tatbestandsvoraussetzung. Die Daten müssen überdies auf einem Datenträger gespeichert werden, also auf einem Medium abgelegt sein, was eine spätere Wahrnehmung ermöglicht. Darüber hinaus ist erforderlich, dass die Datenspeicherung aufgrund einer bezweckten Verarbeitung oder Nutzung der Daten erfolgt; dies ist in der Regel unproblematisch, da eine Datenspeicherung als Selbstzweck praktisch nicht vorkommen dürfte.[82] Eine Datenspeicherung im Zusammenhang mit dem Gesprächsmanagement-System vollzieht sich zum Beispiel mit der Ablage von Kundeninformationen im CRM-System.

Die inhaltliche Umgestaltung personenbezogener Daten, die etwa durch Hinzufügen neuer Informationen, teilweiser Löschung bestehender oder Verknüpfung mit anderen Daten realisiert werden kann, verkörpert eine Veränderung im Sinne des Bundesdatenschutzgesetzes. Erforderlich ist in diesem Zusammenhang ferner, dass die Veränderung Auswirkungen auf den Informationswert der Daten hat.[83] Die Anwendung von Data-Mining-Methoden stellt zum Beispiel eine solche Umgestaltung dar, da hier völlig neue Beziehungen zwischen einzelnen Informationen aufgedeckt werden.

Eine Übermittlung liegt vor, wenn gespeicherte oder anhand von Datenverarbeitung generierte Daten an einen Dritten weitergegeben werden oder eine Einsichtnahme oder ein Abruf durch einen Dritten erfolgt. Keine Datenübermittlung ist demgegenüber gegeben, wenn eine Überlassung der personenbezogenen Daten an einen Auf-

[81] Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 3 Rn. 111.
[82] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 26 ff.; *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 3 Rn. 17 ff.
[83] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 3 Rn. 22; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 30.

tragnehmer im Sinne des § 11 BDSG oder an andere Abteilungen der gleichen verantwortlichen Stelle stattfindet.[84]

Die Einschränkung einer weitergehenden Verarbeitung oder Nutzung personenbezogener Daten ist unter Sperrung zu subsumieren. Dazu werden einzelne Daten, ganze Datensätze oder sämtliche Daten eines Betroffenen mit einem Sperrvermerk gekennzeichnet. Die Sperre kann sich auch auf einen gesamten Datenbestand erstrecken.[85] Gesetzliche Sperrpflichten sind für nichtöffentliche Stellen in § 35 Abs. 3 und 4 und für öffentliche Einrichtungen in § 20 Abs. 3 und 4 BDSG festgeschrieben.[86]

Wurden gespeicherte personenbezogene Daten vollkommen unkenntlich gemacht, gelten sie als gelöscht. Der Informationsgehalt der Daten darf dabei nicht mehr reproduzierbar sein.[87]

Kann die Verwendung der Daten keinem der dargestellten Verarbeitungsschritte zugeordnet werden, stellt sie gemäß § 3 Abs. 5 BDSG eine Nutzung dar. Der Begriff „Nutzung" gilt insofern als umfassender Auffangtatbestand.[88] Jeder Gebrauch von und jedes Arbeiten mit personenbezogenen Daten, der beziehungsweise das keine Datenverarbeitung ist, fällt in die Kategorie der Nutzung.[89]

Zusammenfassend lässt sich festhalten, dass die Funktionsweise des Gesprächsmanagement-Systems ohne jeden Zweifel bedingt, dass personenbezogene Daten der Kunden sowie der Callcenter-Agenten automatisiert erhoben, verarbeitet und unter Umständen genutzt werden.

[84] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 3 Rn. 87 ff.; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 32 ff.; zur Zulässigkeit der Übermittlung von Patientendaten im Rahmen eines Arztpraxisübergangs *BGH* v. 11.12.1991, NJW 1992, 737; *Roßnagel*, NJW 1989, 2303 ff.; *Körner-Damman*, NJW 1992, 1543 ff.
[85] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 3 Rn. 26.
[86] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 38.
[87] *Gräff/Günzel*, DuD 1990, 77; *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 3 Rn. 27; zur Notwendigkeit der Vernichtung von Datenträgern mit personenbezogenen medizinischen Daten *Jürgens*, DuD 1998, 449 ff.
[88] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 3 Rn. 120 ff.; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 42.
[89] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 3 Rn. 106.

3.1.1.1 Zulässigkeitsalternativen im nichtöffentlichen Bereich

Anders als für öffentliche Stellen des Bundes gilt das Bundesdatenschutzgesetz nicht per se für privatwirtschaftliche Organisationen. Sein Anwendungsbereich ist gegenüber nichtöffentlichen Stellen grundsätzlich erst dann eröffnet, wenn in solchen gemäß §§ 1 Abs. 2 Nr. 3, 27 Abs. 1 BDSG der Umgang mit personenbezogenen Daten unter Einsatz von Datenverarbeitungsanlagen oder in oder aus Dateien erfolgt.[90] Die Vorschriften des Bundesdatenschutzgesetzes erfassen sämtliche nichtöffentlichen Callcenter-Betriebe, die das Gesprächsmanagement-System einsetzen. Dasselbe gilt für potenzielle Auftragnehmer im Sinne des § 11 BDSG, die im Rahmen eines Auftrags mit in den personenbezogenen Datenverarbeitungsprozess involviert sind.

Der Umgang mit den im Gespräch und durch das Gespräch anfallenden Daten muss zulässig sein; umfasst sind somit neben dem eigentlichen Gesprächsgegenstand sämtliche weiteren Informationen zum Kontakt, wie Gesprächszeitpunkt und -dauer. Gemäß § 1 Abs. 1 BDSG soll der Einzelne vor Beeinträchtigungen in seinem Persönlichkeitsrecht geschützt werden, die durch den Umgang mit seinen Daten entstehen können.

Unter welchen Voraussetzungen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zulässig ist, regelt § 4 BDSG. Gemäß § 4 Abs. 1 BDSG kann sich der erlaubte Datenumgang aus drei verschiedenen Rechtfertigungsgründen ergeben: Die erste Legitimation besteht darin, dass das Bundesdatenschutzgesetz den Umgang mit den Daten erlaubt oder anordnet. Dasselbe gilt zweitens für andere Rechtsvorschriften. Die dritte Alternative liegt schließlich in der Zustimmung des Betroffenen. Die genannten Erlaubnistatbestände werden nachfolgend ausführlich dargestellt.

3.1.1.1.1 Erlaubnis aus dem Bundesdatenschutzgesetz

§ 28 BDSG regelt die Datenerhebung und -speicherung für eigene Geschäftszwecke nichtöffentlicher und öffentlich-rechtlicher Wettbewerbsunternehmen. Nach Abs. 1 ist das Erheben, Speichern, Verändern, Übermitteln oder Nutzen personenbezogener Daten für eigene Geschäftszwecke bei Vorliegen verschiedener Voraussetzungen zulässig. Die Differenzierung nach der Art der betroffenen personenbezogenen Daten – also nach nicht sensitiv und sensitiv – ist von erheblicher Bedeutung, da für

[90] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 1 Rn. 22a.

den Umgang mit sensitiven Daten strengere Vorschriften als für den Umgang mit nicht sensitiven Daten zu beachten sind.[91]

Ebenso wichtig ist der dem Datenschutzrecht innewohnende Grundsatz der Zweckbindung des Datenumgangs. Dieser kommt auch in § 28 Abs. 1 Satz 2 BDSG zum Ausdruck: Hiernach sind die Zwecke der Verarbeitung oder Nutzung der personenbezogenen Daten schon bei ihrer Erhebung konkret festzulegen. Das Zweckbindungserfordernis kann – wie noch zu zeigen sein wird – insbesondere bei der Datenauswertung einer Kundendatenbank eine Schwierigkeit in der praktischen Anwendung darstellen.

§ 28 Abs. 1 Satz 1 Nr. 1 - 3 BDSG enthält drei Zulässigkeitsvarianten, bezogen auf nicht sensitive Daten[92], aus denen sich ein erlaubter Datenumgang ergeben kann. Die drei unterschiedlichen Rechtfertigungsgründe dürfen jedoch nicht alternativ zueinander gesehen werden. Liegt beispielsweise eine Vertragsbeziehung vor, richtet sich die Zulässigkeit im Regelfall nur nach Nr. 1, und die verantwortliche Stelle kann sich nicht beliebig auf eine andere Zulässigkeitsvariante berufen.[93] Zumindest vermag die Hinzuziehung des Rechtfertigungsgrunds aus Nr. 2 nicht etwas zu gestatten, was nicht bereits durch die Vertragsbeziehung gedeckt ist. Nr. 2 kann nur dann – und unter enger Auslegung – parallel zu Nr. 1 zur Anwendung gelangen, wenn dadurch keine vertraglichen Schutzpflichten beeinträchtigt sind.[94] Der dritte Grund, mit dem sich der Datenumgang gemäß Nr. 3 gegebenenfalls legitimieren lässt, kann bei Daten zum Tragen kommen, die entweder allgemein zugänglich sind, wie die aus Telefonbüchern, oder die die Stelle veröffentlichen dürfte.[95]

Darüber hinaus existiert eine weitere Legitimationsgrundlage für die Verarbeitung oder Nutzung personenbezogener Daten aus § 28 Abs. 3 ff. BDSG, die insbesondere den Zweck der Werbung umfasst.

[91] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 28 Rn. 1.
[92] Die Zulässigkeit des Umgangs mit sensitiven personenbezogenen Daten wird gesondert im Kapitel 3.1.1.3 „Besonderheit beim Umgang mit sensitiven personenbezogenen Daten“ dargestellt.
[93] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BDSG, § 28 Rn. 3.
[94] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 9; *BAG* v. 22.10.1986, RDV 1987, 129, in Bezug auf das Arbeitnehmerpersönlichkeitsrecht.
[95] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 145 ff.

3.1.1.1.1.1 Erlaubnis aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG

Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist der Datenumgang zur Erfüllung eigener Geschäftszwecke zulässig, wenn er für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Eine Verwendung der Daten zu eigenen Geschäftszwecken liegt dann vor, wenn die Daten ein Hilfsmittel zur Durchführung bestimmter unternehmensnotwendiger Tätigkeiten, wie die Abwicklung von Verträgen oder Betreuung von Kunden und Interessenten, darstellen. Die Erreichung des hinter der Datenverarbeitung stehenden Geschäftszwecks ist Intention des Unternehmens; die Verarbeitungsprozesse sind also „Mittel zum Zweck". Die Datenverarbeitung selbst darf nicht den Geschäftszweck darstellen.[96]

Entscheidend dafür, welche personenbezogenen Daten und in welchem Umfang personenbezogene Daten verarbeitet werden dürfen, ist das Kriterium der Erforderlichkeit. Mit der Bundesdatenschutzgesetz-Novelle II[97] vollzog der Gesetzgeber eine Klarstellung in Bezug auf den Umgang mit personenbezogenen Daten im Rahmen von Verträgen: Vormals war der Datenumgang zulässig, wenn er der Zweckbestimmung des Vertrags oder vertragsähnlichen Vertrauensverhältnisses „diente". Im Schrifttum bestanden erhebliche Diskrepanzen im Hinblick auf die Interpretation dieser Vorschrift. So reichten die Meinungen darüber, wann eine legitimierte Datenverarbeitung vorliegt, von wenn sie „…geeignet ist, der Erfüllung der Pflichten aus dem Vertragsverhältnis oder der Wahrnehmung der Rechte aus dem Vertragsverhältnis zu dienen"[98] bis „…mit Rücksicht auf den Zweck eines zwischen der verantwortlichen Stelle und den Betroffenen bestehenden Vertragsverhältnisses benötigt werden"[99]. Nach der ersten Ansicht sollten also bereits dann Datenverwendungen erlaubt sein, wenn sie das Ziel der Vertragsdurchführung verfolgten, ohne dass weitere Einschränkungen zu beachten waren.[100] Dieser äußerst datenverarbeitungsfreundlichen Meinung konnte nicht zugestimmt werden. Der dem gesamten Datenschutzrecht innewohnende Grundsatz der Erforderlichkeit war auch im Zusammenhang mit dem, was der Zweckbestimmung des Vertrags „diente", mit heranzuziehen.[101] Damit darf kein milderes und gleich geeignetes Mittel zur Erreichung des Zwecks zur Verfügung stehen. Daraus lässt sich folgern, dass Daten, die zwar der Vertragserfüllung dienen, auf die jedoch ebenso gut verzichtet werden

[96] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 28 Rn. 6; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 4.
[97] Diese trat weitestgehend am 1.9.2009 in Kraft.
[98] So *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 28 Rn. 18.
[99] So Simitis/*Simitis*, BDSG, 6. Aufl. 2006, § 28 Rn. 79.
[100] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 194.
[101] So auch *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 194 f.

könnte, keinesfalls erforderlich sein können. In der aktuellen Vorschrift des § 28 Abs. 1 Satz 1 Nr. 1 BDSG kommt die Bedeutung der Erforderlichkeit ausdrücklich dadurch zum Ausdruck, dass der Umgang mit den personenbezogenen Daten nunmehr nur noch zulässig ist, wenn er für die Begründung, Durchführung oder Beendigung des Schuldverhältnisses „erforderlich" ist. Diese Verdeutlichung lässt wenig Interpretationsspielraum. Überdies wird in der Gesetzesbegründung zur Bundesdatenschutzgesetz-Novelle II ausdrücklich darauf hingewiesen, dass keine „überschießenden Daten" verarbeitet werden dürfen.[102]

Die Erforderlichkeit stellt ein – unter vernünftiger Betrachtungsweise erkanntes – Angewiesensein auf das in Frage stehende Mittel dar. Der Datenumgang ist mithin gerechtfertigt, wenn er ein geeignetes Mittel zur Zweckerreichung verkörpert und keine zumutbare Alternative existiert.[103]

Die aufgezeigten Grundsätze gelten ebenso für rechtsgeschäftsähnliche Schuldverhältnisse, etwa im Rahmen einer Vertragsanbahnung. Bereits in dieser frühen Phase eines potenziellen Vertragsverhältnisses sind bestimmte Vertrauens- und beiderseitige Sorgfaltspflichten zu beachten.[104] Ein vertragsähnliches Vertrauensverhältnis kann auch nach Beendigung einer bestehenden Vertragsbeziehung fortbestehen. Dies gilt besonders im Zusammenhang mit Arbeitsverhältnissen: Hier kann es notwendig sein, bestimmte Daten, die zur Durchführung des Vertrags notwendig waren, weiterhin zu verwenden, um nachträglich etwa Bescheinigungen ausstellen zu können.[105] Nach der aktuellen Fassung des § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist der Umgang mit personenbezogenen Daten – sofern dieser dem Kriterium der Erforderlichkeit genügt – neben der Durchführung auch zur Begründung und Beendigung von Schuldverhältnissen ausdrücklich zulässig.

§ 28 Abs. 1 Satz 1 Nr. 1 BDSG kommt als Rechtfertigungsgrundlage für den personenbezogenen Datenumgang im Gesprächsmanagement-System hohe Relevanz zu. Inwieweit diese Zulässigkeitsvariante für den Datenumgang innerhalb der verschiedenen Systemkomponenten des Gesprächsmanagement-Systems, wie dem Frontend- oder dem CRM-System, im Einzelnen zu dienen vermag, ist in Kapitel 3.1.1.4 „Zulässigkeit des Datenumgangs in den einzelnen Systemkomponenten" dargestellt.

[102] S. BT-Drs. 16/13657, 30.
[103] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 15.
[104] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 28 Rn. 66 f.
[105] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 90.

3.1.1.1.1.2 Erlaubnis aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Ein zulässiger Umgang mit personenbezogenen Daten kann sich darüber hinaus aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG ergeben, soweit er zur Wahrung berechtigter Interessen des Datenverarbeiters erforderlich ist und überdies kein Grund zur Annahme besteht, dass schutzwürdige Interessen von Betroffenen überwiegen, die gegen die Verarbeitung oder Nutzung der Daten sprechen.

Die Zulässigkeit oder Unzulässigkeit der Datenverwendung resultiert aus einer Interessenabwägung zwischen den schutzwürdigen Belangen der Betroffenen und den berechtigten Interessen der verantwortlichen Stelle. Diese im Widerstreit zueinander stehenden Interessen können jeweils keinen unbedingten Vorrang für sich beanspruchen.[106] Welche Position überwiegt, muss einzelfallabhängig eruiert werden. Eine durchzuführende Interessenabwägung hat dem Verhältnismäßigkeitsgrundsatz zu genügen.[107]

Berechtigte Interessen des Datenverarbeiters können etwa wirtschaftlicher oder ideeller Natur sein.[108] Sie müssen sich nach vernünftiger Erwägung der Sachlage als gerechtfertigtes, also tatsächliches Interesse darstellen.[109] Wichtig in diesem Zusammenhang ist die Tatsache, dass es sich bei den berechtigten Interessen um eigene Belange der verantwortlichen Stelle handelt.[110] Der hauptsächliche Zweck der Verwendung des Gesprächsmanagement-Systems im Callcenter besteht in der Unterstützung des Callcenter-Mitarbeiters zur Gesprächsoptimierung in fachlicher, methodischer, sozialer und personaler Hinsicht. Die genannte Zwecksetzung lässt sich ohne weiteres als berechtigtes Interesse des Callcenters einstufen.

Das dem entgegenstehende schutzwürdige Interesse der Betroffenen besteht insbesondere im Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG. Ob schutzwürdige Belange vorliegen, kann nur anhand einer Betrachtung der spezifischen Verarbeitungssituation festgestellt werden. Die Verarbeitungsbedingungen bestimmen letztendlich die Konsequenzen und somit den Grad der Beeinträchtigung der Interessen. Mit steigender Beeinträchtigung der Interessen erhöht sich die Schutzwürdigkeit der Interessen. Anders ausgedrückt: Der Umgang mit den personenbezogenen Daten ist nicht mehr hinnehmbar, wenn Betroffene mit

[106] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 125; *Podlech/Pfeifer*, RDV 1998, 139 (148 f.).
[107] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 24 ff.
[108] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BDSG, § 28 Rn. 6; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 104.
[109] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 24.
[110] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 105.

Rücksicht auf die verwendeten Daten, Verfahren, verfolgten Zwecke sowie die Intensität der Datenverarbeitung Folgen ausgesetzt werden, die inakzeptabel sind; in einem solchen Fall überwiegen unbestritten die schutzwürdigen Interessen.[111] Dies ist in vollem Umfang für personenbezogene Daten der Kunden, die im Rahmen des Gesprächsmanagement-Systems erhoben, verarbeitet oder genutzt werden, zu beachten.

Der Datenumgang muss ferner erforderlich sein, das heißt seine Geeignetheit oder Zweckmäßigkeit zur Erfüllung der beabsichtigten Zwecke reichen nicht aus. Als erforderlich können nur Verwendungen angesehen werden, für die es keine objektiv zumutbare Alternative gibt. Damit vermag sich die Verwendungsmöglichkeit nicht nur auf Konstellationen zu beschränken, in denen die Daten zwingend notwendig sind.[112] So kann es in einigen Fällen nicht einfach sein, die verwendeten Daten auf das wirklich Notwendige zu reduzieren; dies gilt insbesondere bei der Akquisition von Interessentendaten oder bei der Anreicherung von Kundendaten mit zusätzlichen Informationen. Das berechtigte Interesse des Callcenters liegt diesbezüglich eindeutig vor. Ob jedoch jede der zusätzlichen Angaben tatsächlich erforderlich ist, lässt sich nur schwer abschätzen, da nur im Einzelfall bestimmt werden kann, wo die Grenze zu einer zulässigen Verarbeitung genau verläuft.[113]

Einer besonderen Restriktion unterliegen besonders schutzwürdige Daten im Sinne des § 3 Abs. 9 BDSG, wie Angaben über die Gesundheit oder zur Religionszugehörigkeit. Der Umgang mit solchen sensitiven Daten darf keinesfalls auf die Rechtfertigungsgrundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden.[114]

3.1.1.1.1.3 Erlaubnis aus § 28 Abs. 1 Satz 1 Nr. 3 BDSG

Nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG ist der Umgang mit personenbezogenen Daten grundsätzlich erlaubt, wenn sie allgemein zugänglich sind oder deren Veröffentlichung durch die verantwortliche Stelle gestattet wäre. Ausnahmsweise gilt diese Zulässigkeitsbedingung nicht für Daten, bei denen das schutzwürdige Interesse des Betroffenen an der Verhinderung des Umgangs offensichtlich größer ist als das be-

[111] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 26 f.; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 127.
[112] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 108; zum Kriterium der Erforderlichkeit s. obenstehende Ausführungen zu § 28 Abs. 1 Satz 1 Nr. 1 BDSG.
[113] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 115.
[114] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 132; zum Umgang mit besonders schutzwürdigen Daten s. Kapitel 3.1.1.3 „Besonderheit beim Umgang mit sensitiven personenbezogenen Daten“.

rechtigte Interesse der verantwortlichen Stelle. Da ein schutzwürdiges Interesse des Betroffenen „offensichtlich“ überwiegen muss, kann eine intensive Einzelfallüberprüfung unterbleiben.[115]

Die Zulässigkeitserleichterung gilt für Daten, die allgemein und öffentlich zugänglich sind. Ableiten lässt sich dieses Recht aus der Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 GG: Wem es gestattet ist, sich aus allgemein zugänglichen Quellen zu informieren, dem muss im Grundsatz auch eine Speicherung der gewonnenen Informationen erlaubt sein.[116] Allgemeine Zugänglichkeit liegt vor, wenn die Datenquelle technisch dazu bestimmt und geeignet ist, einen unbestimmbaren Personenkreis zu erreichen.[117] Beispielhaft können Webseiten, Telefon- und Adressbücher, Flugblätter, Plakatanschläge, Beiträge in Massenmedien – etwa im Rahmen des Web 2.0 – sowie öffentliche Register, die ohne berechtigtes Interesse eingesehen werden dürfen, ins Feld geführt werden.[118] Über das Internet abrufbare Personensuchmaschinen zählen ebenfalls zu derartigen Informationsressourcen.

Auch in Bezug auf Daten, die die verantwortliche Stelle zugänglich machen dürfte, sind die erleichterten Zulässigkeitsvoraussetzungen anzuwenden. Hierunter sind etwa Fachinformationsdienste für Literatur zu fassen, die Angaben zu Autoren speichern dürfen, da die Autoren davon auszugehen haben, dass ihre Autoreneigenschaft weiterverbreitet wird.[119]

Die Zulässigkeitsvariante aus Nr. 3 wird im Rahmen der vorgesehenen Anwendungsszenarien des Gesprächsmanagement-Systems regelmäßig nicht in Betracht kommen. Aus Gründen der Vollständigkeit wurde sie dennoch kurz aufgezeigt.

3.1.1.1.1.4 Erlaubnis aus § 28 Abs. 3 ff. BDSG

Das Aufgabenspektrum von Callcentern ist vielfältig: Neben beispielsweise der Bereitstellung eines Beschwerdemanagements oder einer Beratungs-Hotline fällt insbesondere die Durchführung von Werbekampagnen in ihren Aufgabenbereich.

[115] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 31 ff.
[116] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 28 Rn. 10; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 32; *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 28 Rn. 133.
[117] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BDSG, § 28 Rn. 7.
[118] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 28 Rn. 10; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 32.
[119] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 157; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 33.

Auch im Anwendungsfeld Werbung lässt sich das Gesprächsmanagement-System zur Unterstützung der Callcenter-Mitarbeiter einsetzen.

§ 28 Abs. 3 BDSG gilt als Rechtfertigungsgrundlage für die Verarbeitung oder Nutzung personenbezogener Daten zum Zweck der Werbung oder des Adresshandels. Diese Vorgänge sind gemäß § 28 Abs. 3 Satz 1 BDSG zulässig, soweit eine diesbezügliche Einwilligung der (potenziellen) Kunden vorliegt. Die Einwilligung bedarf grundsätzlich der Schriftform und ist gemäß § 28 Abs. 3a Satz 2 BDSG drucktechnisch deutlich hervorzuheben, wenn sie mit anderen Erklärungen zusammen abgegeben werden soll. Sie kann jedoch nach § 28 Abs. 3a Satz 1 BDSG auch in anderer Form – zum Beispiel mündlich per Telefon – erteilt werden. In diesem Fall muss das Callcenter allerdings den Inhalt der Einwilligung schriftlich bestätigen.

Als Alternative zur Schriftform gilt in diesem Zusammenhang – unter weitergehenden Voraussetzungen – die elektronische Form. Soll sie Verwendung finden, muss das Callcenter gewährleisten, dass eine Protokollierung der Einwilligung erfolgt und die Kunden deren Inhalt zu jeder Zeit abrufen können. Darüber hinaus muss es den Kunden möglich sein, die erteilte Einwilligung jederzeit zu widerrufen. Bei der elektronischen Einwilligung in Werbemaßnahmen werden die in § 13 Abs. 2 TMG und § 94 TKG enthaltenen Forderungen aufgegriffen.[120]

Die inhaltlichen Anforderungen, die an eine Einwilligung in Werbemaßnahmen gestellt werden, sind grundsätzlich dieselben wie die durch § 4 Abs. 3 BDSG geforderten. Insofern gilt es, nachvollziehbare Angaben – insbesondere zur verantwortlichen Stelle, zu den notwendigen Daten und den Verarbeitungszwecken sowie zu einer gegebenenfalls erfolgenden Datenübermittlung – zu machen.[121]

§ 28 Abs. 3b BDSG enthält ein Kopplungsverbot, nach dem der Abschluss eines Vertrags nicht an eine Einwilligung gekoppelt werden darf, wenn den Kunden ein anderer Zugang zu gleichwertigen Leistungen ohne die Einwilligung nicht oder nur in unzumutbarer Weise möglich ist. Von dem Kopplungsverbot sind nicht nur marktbeherrschende Unternehmen betroffen.[122] Absprachen zwischen sämtlichen marktbeteiligten Unternehmen könnten dazu führen, dass die Leistung marktweit nur unter Abgabe der Einwilligung zu erwerben wäre.[123] Noch keine Unzumutbarkeit liegt vor, wenn eine vergleichbare Leistung bei anderen Anbietern zu einem

[120] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 222; *Plath/Frey*, BB 2009, 1762 (1766).
[121] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 216.
[122] *Plath/Frey*, BB 2009, 1762 (1767).
[123] BT-Drs. 16/12011, 30.

höheren Preis erhältlich ist.[124] Wird das Kopplungsverbot nicht eingehalten, ist die Einwilligung gemäß § 28 Abs. 3b Satz 2 BDSG rechtsunwirksam.[125]

Den Kunden steht aus § 28 Abs. 4 BDSG ein Widerspruchsrecht zu, mit dem sie die Verarbeitung oder Nutzung ihrer personenbezogenen Daten unter anderem zu Werbezwecken unterbinden können. Selbst für Fälle, in denen das Callcenter beispielsweise aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG durchaus dazu berechtigt ist, die Daten zu verarbeiten oder zu nutzen, greift dieses Widerspruchsrecht, wenn solche Vorgänge zum Zwecke der Werbung erfolgen sollen.[126] § 28 Abs. 4 Satz 2 BDSG sieht vor, dass Kunden über ihr Widerspruchsrecht aufgeklärt werden müssen. Diese Aufklärung hat vor der Verarbeitung oder Nutzung der personenbezogenen Daten von (potenziellen) Kunden zu Werbezwecken zu erfolgen, also beispielsweise zum Zeitpunkt des Abschlusses eines rechtsgeschäftlichen Schuldverhältnisses.[127]

In bestimmten Fällen dürfen personenbezogene Daten von (potenziellen) Kunden für Werbezwecke auch ohne die Rechtfertigung aus deren Einwilligung verwendet werden. Diese Ausnahmefälle sind in § 28 Abs. 3 Satz 2 Nr. 1 - 3 und Satz 5 BDSG geregelt und betreffen die Werbung

- für eigene Angebote,
- gegenüber freiberuflich oder gewerblich Tätigen,
- für Spenden und
- für fremde Angebote neben Eigenwerbung.

Allerdings beschränken sich die Daten, die einwilligungsfrei für Werbezwecke verarbeitet oder genutzt werden dürfen, auf sogenannte Listendaten. Unter diese fallen ausschließlich

- Angaben über die Zugehörigkeit zu einer bestimmten Personengruppe (etwa „langjährige Bestandskunden“),
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Name,
- Titel,
- akademischer Grad,
- Anschrift und

[124] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 46.
[125] Zum Datenumgang für Werbezwecke s. *Roßnagel*, NJW 2009, 2716 (2720 f.).
[126] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 248.
[127] BT-Drs. 16/12011, 30.

- Geburtsjahr.

§ 28 Abs. 3 Satz 6 BDSG verlangt für die einwilligungsfreien Erlaubnistatbestände eine Interessenabwägung: Die personenbezogene Datenverarbeitung oder -nutzung ist hiernach nur insoweit zulässig, als keine schutzwürdigen Interessen der Betroffenen entgegenstehen.[128] Schutzwürdige Interessen können etwa dann berührt sein, wenn durch die besondere Art der Zusammenstellung der Listendaten weitergehende Informationen über die Betroffenen offengelegt würden. Die Angabe, ob jemand beispielsweise Bewohner eines Pflegeheims ist, stellt einen solchen Fall dar.[129]

Zulässig ist die Verarbeitung oder Nutzung der personenbezogenen Listendaten für Zwecke der Werbung für eigene Angebote, soweit gemäß § 28 Abs. 3 Satz 2 Nr. 1 BDSG Erforderlichkeit dafür besteht. Die Listendaten müssen dabei nicht zwangsläufig beim Betroffenen selbst erhoben worden sein, sondern können ausnahmsweise aus allgemein zugänglichen Verzeichnissen, wie Adress-, Rufnummern- oder Branchenverzeichnissen, stammen.

Die Vorschrift des § 28 Abs. 3 Satz 3 BDSG enthält überdies die Erlaubnis, bei Werbung für eigene Angebote weitere Daten hinzuzuspeichern. Damit wird zum Beispiel der Betrieb eines werbespezifischen Data-Warehouse unter weiteren Voraussetzungen erlaubt.[130] Ein eigenes Angebot im Sinne der Regelung liegt auch dann vor, wenn ein Unternehmen im Wege der Auftragsdatenverarbeitung gemäß § 11 BDSG ein selbstständiges Callcenter mit der Durchführung einer Werbekampagne beauftragt.

Der gesetzliche Erlaubnistatbestand aus § 28 Abs. 3 Satz 2 Nr. 1 BDSG erscheint gerechtfertigt, da den (potenziellen) Kunden die Erhebung ihrer Daten im Kontext des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses bekannt ist und sie davon ausgehen müssen, dass die verantwortliche Stelle für weitere eigene Angebote werben wird.[131]

(Potenzielle) Geschäftskunden dürfen nach § 28 Abs. 3 Satz 2 Nr. 2 BDSG unter ihrer beruflichen Adresse beworben werden. Geschäftliche Werbung wird von der Vorschrift nur insoweit erfasst, als die dafür herangezogenen Daten einer bestimmten oder bestimmbaren Person zugeordnet werden können. Beispielsweise die Fir-

[128] *Peifer*, MMR 2010, 524 (526).
[129] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 245.
[130] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 54; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 240.
[131] So BT-Drs. 16/12011, 27.

mierung oder die Größe des Unternehmens können hierbei Indikatoren darstellen.[132] Die konkrete Werbeansprache hat sich ausschließlich auf die berufliche Tätigkeit des Betroffenen zu beziehen.[133]

§ 28 Abs. 3 Satz 2 Nr. 3 BDSG enthält eine weitere Ausnahme, die die Datenverarbeitung oder -nutzung zu Zwecken der Spendenwerbung erlaubt. Diese spezielle Regelung begünstigt das Fortbestehen bestimmter Organisationen, die auf steuerbegünstigte Spenden angewiesen sind.[134]

Die Vorschrift des § 28 Abs. 3 Satz 5 BDSG betrifft hauptsächlich den Fall der sogenannten Beipackwerbung, einer besonderen Werbeform in Bezug auf fremde Angebote. Diese Werbung wird insbesondere bei Konzernen oder im Unternehmensverbund eingesetzt. Die Werbeansprache erfolgt hier im Regelfall derart, dass sie beispielsweise im Zusammenhang mit der Erfüllung eines Schuldverhältnisses ergeht: Der dem Kunden zugesandten Rechnung liegt ein Prospekt des Fremdangebots bei. Erlaubt kann darüber hinaus die Werbung für fremde Angebote sein, wenn sie zusammen mit der Eigenwerbung nach § 28 Abs. 3 Satz 2 Nr. 1 BDSG erfolgt. Weitergehend muss die verantwortliche Stelle selbst die Listendaten bei den (potenziellen) Kunden im Rahmen eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben haben.[135]

Grundlage für die Werbung sind dieselben Listendaten wie die in § 28 Abs. 3 Satz 2 BDSG aufgezählten. Diese Listendaten sind zwar unstreitig die Grundlage für die an eigenen Angeboten ausgerichteten Werbekampagnen, können allerdings gleichzeitig für Werbemaßnahmen zu Gunsten Dritter verwendet werden.[136] Weitere Voraussetzung für die Zulässigkeit ist die Erkennbarkeit der für die Nutzung der Listendaten verantwortlichen Stelle. Die besondere Form der Werbung für Fremdangebote lässt sich auch durch Callcenter ausführen. Diese können zum Beispiel die Aufgabe haben, in erster Linie eigene Angebote zu bewerben, gleichzeitig jedoch auf weitere, potenziell interessante Angebote von Fremdanbietern hinweisen. Werden die genannten Anforderungen erfüllt, ist ein solches Vorgehen zulässig.

§ 47 BDSG enthält eine Übergangsregelung zur Datenverarbeitung oder -nutzung für Werbezwecke: Für Daten, die vor dem 1. September 2009 erhoben oder gespeichert wurden, bleibt bis zum Stichtag 31. August 2012 § 28 BDSG a. F. anwendbar.

[132] BT-Drs. 16/12011, 27 f.
[133] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 241.
[134] BT-Drs. 16/12011, 28.
[135] BT-Drs. 16/12011, 28 f.
[136] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 244.

Somit besteht für solche personenbezogenen Daten kein grundsätzliches Einwilligungserfordernis, wenn sie für Werbung verarbeitet oder genutzt werden.[137] Die Nutzung oder Verwendung dieser Daten von Bestandskunden für Zwecke der Werbung ist nach Ablauf der Frist verboten, sodass entweder die nochmalige Erhebung der Daten zu erfolgen hat, oder eine Einwilligung in die weitere Nutzung oder Verwendung der bereits vorliegenden Daten für Werbezwecke eingeholt werden muss.[138]

Im Hinblick auf die praktische Umsetzung der Werbeaktivitäten durch Callcenter ist allerdings zu beachten, dass – neben den Vorschriften des Datenschutzrechts – die Regelungen des Gesetzes gegen den unlauteren Wettbewerb und die des Telekommunikationsgesetzes mit herangezogen werden müssen. Ein Callcenter, das eine Outbound-Kampagne durchführen will, hat keinen Nutzen vom rechtmäßigen Besitz von Kundendaten, wenn es diese nicht dazu einsetzen darf, die Kunden anzurufen.[139] Nach den wettbewerbsrechtlichen Vorschriften ist nämlich eine Einwilligung der (potenziellen) Kunden in Telefonwerbung erforderlich.[140] Handelt es sich bei den (potenziellen) Kunden um Verbraucher, muss gemäß § 7 Abs. 2 Nr. 2 UWG deren vorherige ausdrückliche Einwilligung in die Werbeanrufe eingeholt werden.[141] Bei sonstigen Marktteilnehmern gilt bereits eine mutmaßliche Einwilligung als ausreichend. Darüber hinaus unterliegen werbende Callcenter aus § 102 Abs. 2 TKG der Verpflichtung, ihre Rufnummer zu übertragen, sodass es den Angerufenen ermöglicht wird, bei unerlaubten Werbeanrufen gegen das Callcenter vorzugehen.[142]

Insbesondere die wettbewerbsrechtlichen Anforderungen an Outbound-Telefonie zu Werbezwecken stellen eine hohe Hürde dar. Werbetreibende Callcenter können jedoch dazu übergehen, die (potenziellen) Kunden dazu zu bewegen, selbst beim Callcenter anzurufen.[143] Praktisch lässt sich dies zum Beispiel mittels einer schriftlichen „Aufforderung“ vollziehen – in Form der grundsätzlich erlaubten Briefwerbung.[144] Denkbar ist aber auch die Situation, in der Kunden bei einem Callcenter anrufen, um beispielsweise eine Frage zu einem erworbenen Produkt zu klären. Das

[137] Grentzenberg/Schreibauer/Schuppert, K&R 2009, 535 (537).
[138] Roßnagel/Jandt, MMR 2011, 86 (90).
[139] Plath/Frey, BB 2009, 1762 (1763).
[140] S. dazu Kapitel 3.2.1 „Verbot von Werbeanrufen ohne Einwilligung“.
[141] Hecker, K&R 2009, 601 (604); zum Transparenzgebot des Einwilligungsersuchens BGH v. 14.4.2011, CR 2011, 513 f.
[142] S. dazu Kapitel 5.3 „Verbot der Rufnummerunterdrückung“.
[143] von Wallenberg, BB 2009, 1768 (1773), geht sogar soweit, die zukünftige Outbound-Telefonie zu Werbezwecken aufgrund der rechtlichen Anforderungen für praktisch nicht mehr durchführbar zu erklären.
[144] von Wallenberg, BB 2009, 1768 (1773).

Callcenter kann nicht nur die Aufgabe haben, die Kunden bei der Problemlösung hinsichtlich ihrer Produkte zu unterstützen, sondern auch gleichzeitig die Funktion erfüllen, für andere Produkte zu werben.

Nachdem die Rechtfertigungsgrundlage aus § 28 Abs. 3 ff. BDSG zur Durchführung von Werbemaßnahmen allgemein dargestellt wurde, ist fraglich, inwieweit sie dazu zu dienen vermag, die Komponenten des Gesprächsmanagement-Systems zulässig einzusetzen. Diese Frage wird in Kapitel 3.1.1.4 „Zulässigkeit des Datenumgangs in den einzelnen Systemkomponenten“ untersucht.

3.1.1.1.2 Erlaubnis aus einer anderen Rechtsvorschrift

Ein zulässiger Umgang mit personenbezogenen Daten kann sich überdies aus einer anderen Rechtsvorschrift als aus dem Bundesdatenschutzgesetz ergeben. Als solche Vorschriften kommen zunächst fach- und bereichspezifische Normen des Bundes gemäß § 1 Abs. 3 Satz 1 BDSG in Frage, die die Regelungen des Bundesdatenschutzgesetzes verdrängen.[145] Diesbezügliche spezialgesetzliche Bundesvorschriften stellen etwa das Telekommunikationsgesetz, das Telemediengesetz und das Sozialgesetzbuch dar.[146]

Die in § 4 Abs. 1 BDSG als „andere Rechtsvorschrift“ bezeichneten Regelungen sind ferner dem Bundesrecht untergeordnete Normen, wie Landesgesetze, kommunales Recht, Tarifverträge und Betriebs- oder Dienstvereinbarungen. Liegen derartige Bestimmungen vor, die den Umgang mit personenbezogenen Daten regeln, ist das Bundesdatenschutzgesetz insoweit nachrangig. Voraussetzung ist, dass diese anderen Rechtsvorschriften den vorgesehenen Datenumgang eindeutig, das heißt zumindest unter Nennung der Datenart sowie des Zwecks, beschreiben.[147] Die alternative Rechtsnorm muss den Umgang mit personenbezogenen Daten regeln oder zwingend voraussetzen.[148]

Die spezielle Erlaubnisnorm kann negativ vom Schutzniveau des Bundesdatenschutzgesetzes abweichen.[149] Dies ist in bestimmten Fällen möglich, in denen ein überwiegendes Allgemeininteresse an der Abweichung vorliegt.[150] Dennoch steckt

[145] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 7; ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 4 Rn. 2.
[146] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 4 Rn. 16.
[147] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 7.
[148] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 4 Rn. 3.
[149] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 4 Rn. 3; *BAG* v. 27.5.1986, NJW 1987, 674.
[150] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 1 Rn. 172.

das allgemeine Persönlichkeitsrecht der Betroffenen die Grenze zur unzulässigen Datenverarbeitung ab.[151] Die Betriebs- oder Dienstvereinbarung nimmt als spezielle Erlaubnisnorm im Rahmen des Beschäftigtendatenschutzes eine bedeutende Rolle ein.[152] Eine solche Kollektivvereinbarung dient primär der Konkretisierung und Auslegung der abstrakten Vorschriften des Bundesdatenschutzgesetzes im Hinblick auf die jeweiligen betrieblichen Gegebenheiten.[153]

Die Zulässigkeitsvariante in Bezug auf den Umgang mit personenbezogenen Daten aufgrund einer anderen Rechtsvorschrift kann beispielsweise beim Einsatz des Gesprächsmanagement-Systems im Bereich der telefonischen Gesundheitsberatung Relevanz erlangen. Generell existiert nunmehr eine nicht mehr zu überblickende Anzahl vorrangiger Bestimmungen gemäß § 1 Abs. 3 Satz 1 BDSG.[154]

§ 1 Abs. 3 Satz 2 BDSG enthält darüber hinaus die Vorgabe, dass spezielle Berufs- und Amtsgeheimnisse sowie gesetzliche Geheimhaltungspflichten unberührt bleiben. Derartige spezifische Geheimhaltungsverpflichtungen verkörpern das Fundament für die Vertrauensbeziehung zwischen Bürgern und den zur Geheimhaltung Verpflichteten, wie etwa den Angehörigen besonderer Berufsstände. Die praktische Auswirkung der Vorschrift liegt darin, das größtmögliche Schutzniveau zu bieten: Es kommt zur gleichzeitigen Geltung der Vorschriften des Bundesdatenschutzgesetzes und des Geheimnisschutzes. Der durch das Bundesdatenschutzgesetz gewährleistete Schutzstandard stellt das Minimum an Schutz dar, der eingehalten werden muss. Geht der spezielle Geheimnisschutz über diesen Standard hinaus, bildet er selbst den zu beachtenden Mindeststandard.[155]

3.1.1.1.3 Erlaubnis aus einer Einwilligung

Die dritte Alternative für einen zulässigen Umgang mit den personenbezogenen Daten besteht in der Erlaubnis durch den Betroffenen. Eine Einwilligung ist eine vorherige Einverständniserklärung im Sinne des § 183 BGB.[156] Eine nachträgliche Zustimmung gemäß § 184 BGB kann die Rechtswidrigkeit der zwischenzeitlich

[151] *BAG* v. 26.8.2008, NZA 2008, 1187.
[152] Zur Regelung der Datenverarbeitungsbefugnisse mittels Kollektivvereinbarungen ausführlich Kapitel 4.1.1.2 „Erlaubnis aus einer anderen Rechtsvorschrift".
[153] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 4 Rn. 2.
[154] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 1 Rn. 161; *Garstka*, Informationelle Selbstbestimmung und Datenschutz, 55 (abrufbar unter: www.bpb.de/files/YRPN3Y.pdf).
[155] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 1 Rn. 175 ff.; *KG* v. 20.8.2010, NJW 2011, 324.
[156] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 15; *Zscherpe*, MMR 2004, 723 (724).

durchgeführten Datenverarbeitungsprozesse nicht heilen.[157] Der Hauptgrund dafür liegt darin, dass der Betroffene nicht vor vollendete Tatsachen gestellt werden soll, indem sich zunächst eine meist irreversible Verwendung seiner personenbezogenen Daten vollzieht, gegen die er sich nachträglich nicht mehr entscheiden kann.[158]

Damit eine Einwilligung Wirksamkeit erlangt, müssen gemäß § 4a BDSG verschiedene Voraussetzungen erfüllt sein. Zunächst benennt § 4a Abs. 1 BDSG den Aspekt der Freiwilligkeit, der insbesondere im Rahmen von Arbeitsverhältnissen[159] eine Schwierigkeit darstellen kann. Der Betroffene ist darüber hinaus auf die vorgesehenen Zwecke des Datenumgangs sowie unter Umständen auf die Konsequenzen einer verweigerten Einwilligung hinzuweisen. Grundsätzlich muss die Einwilligung schriftlich eingeholt werden; bei Vorliegen besonderer Umstände kann davon abgewichen werden. Ferner ist die Einwilligung besonders hervorzuheben, wenn sie zusammen mit anderen schriftlichen Erklärungen abgegeben werden soll. Soll sich die Erhebung, Verarbeitung oder Nutzung auf besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG erstrecken, muss sich die Einwilligung gemäß § 4a Abs. 3 BDSG ausdrücklich auf diese spezifischen Daten beziehen.[160]

Die Einwilligung hat auf freier Entscheidung zu beruhen. Die Freiwilligkeit als notwendiges Merkmal kommt bereits in der EG-Datenschutzrichtlinie[161] zum Ausdruck.[162] In Art. 2 lit. b EG-Datenschutzrichtlinie ist die Rede von einer „…Willensbekundung, die ohne Zwang…“ ergangen sein muss. Freiwilligkeit setzt voraus, dass kein Zwang bei der Entscheidung vorliegt. Dies ist dann gegeben, wenn die Einwilligung nicht unter Ausnutzen einer wirtschaftlichen Machtposition erzwungen wird.[163]

Der Kunde hat über die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung aufgeklärt zu werden. Des Weiteren ist er über potenzielle Empfänger der Daten und vorgesehene Datenübermittlungen zu informieren.[164] Die Einwilligungserklärung „Ich erteile hiermit die Einwilligung, dass meine Daten auch an andere

[157] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BDSG, § 4a Rn. 1; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 29.
[158] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 204 m. w. N.
[159] Zur Schwierigkeit der freiwilligen Einwilligung im Rahmen von Arbeitsverhältnissen ausführlich Kapitel 4.1.1.3 „Erlaubnis aus einer Einwilligung“.
[160] Zu den Voraussetzungen, unter denen sensitive personenbezogene Daten verarbeitet werden dürfen, s. Kapitel 3.1.1.3 „Besonderheit beim Umgang mit sensitiven personenbezogenen Daten“.
[161] Richtlinie 95/46/EG v. 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
[162] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 62.
[163] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 6.
[164] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 72; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 11a; *Beisenherz/Tinnefeld*, DuD 2011, 110 (111).

Unternehmen weitergegeben werden dürfen“ steht für ein klassisches Beispiel, bei dem ein rechtswirksames Einverständnis nicht erteilt ist.[165]

Das grundsätzliche Schriftformerfordernis führt bei einer Nichteinhaltung dazu, dass die Einwilligung gemäß §§ 125, 126 BGB nichtig ist und sämtliche sich anschließenden Datenverarbeitungsvorgänge unzulässig sind.[166] Besondere Umstände können jedoch trotz Abweichens vom grundsätzlichen Erfordernis der Schriftlichkeit die Datenverarbeitung rechtfertigen; von einem solchen Fall kann in der Regel ausgegangen werden, wenn eine besondere Eilbedürftigkeit vorliegt.[167] Abhängig davon, welche Rechtsbeziehung zwischen dem Callcenter und dem Gesprächspartner besteht, kann die schriftliche Einwilligung gegebenenfalls durch eine mündliche ersetzt werden.[168] Bei einer Vielzahl von Callcenter-Dienstleistungen hat vor dem Telefonat zwischen Callcenter und Gesprächspartner kein schriftlicher Kontakt und damit auch keine Möglichkeit für eine schriftliche Einwilligung bestanden.[169] In den meisten Fällen wird dies praktisch gar nicht möglich sein. Entscheidend in diesem Zusammenhang ist jedenfalls, dass die Einwilligung ausdrücklich ergeht. Keinesfalls reicht eine stillschweigende, konkludente oder gar mutmaßliche Erklärung aus.[170] Vielmehr ist es notwendig, dass der Gesprächspartner aktiv sein Einverständnis zur Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten signalisiert. Dieses Einverständnis muss durch ein eindeutiges Zeichen zum Ausdruck kommen, wie durch ein ausdrückliches „Ja“ oder durch das explizite Drücken einer Taste. Insofern kann eine telefonische Einwilligungserklärung allgemein nur in Form eines Opt-In als rechtsgemäß betrachtet werden.[171]

Unbestreitbar ist, dass auch im Bereich der Callcenter-Dienstleistungen ein massenhafter Umgang mit personenbezogenen Daten notwendig sein kann. Als problematisch erweist sich, wenn Ermächtigungen zur personenbezogenen Datenverarbeitung in Allgemeinen Geschäftsbedingungen (AGB) verankert sind. Lediglich der Hinweis auf Vorliegen derartiger AGB reicht für das wirksame Einbeziehen nicht aus.[172] Die Klauseln unterliegen der AGB-Kontrolle und können unwirksam sein.

[165] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 11a.
[166] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 13.
[167] *Hoeren*, Grundzüge des Internetrechts, 2. Aufl. 2002, 247; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 13.
[168] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 61 in Bezug auf telefonische Umfragen; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 13.
[169] *Voigt*, DuD 2008, 780 (782).
[170] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 13; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 44 ff.
[171] Zur Diskussion, ob die Einwilligung als Opt-In gestaltet sein muss, oder ob ein Opt-Out ausreicht, s. ausführlich *Voigt*, DuD 2008, 780 (782).
[172] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 41.

Eine Unwirksamkeit kann insbesondere bei Klauseln gegeben sein, die gegen die Gebote von Treu und Glauben gemäß § 307 Abs. 1 Satz 1 BGB verstoßen. Weitere unangemessene Benachteiligungen, die verhindern, dass AGB in den Vertrag mit einbezogen werden, können darin bestehen, dass die Klauseln nach § 307 Abs. 1 Satz 2 BGB nicht klar und verständlich sind. Ferner werden solche Regelungen gemäß § 305c Abs. 1 BGB nicht Vertragsbestandteil, die sich als überraschend und mehrdeutig darstellen.[173]

Obwohl nicht ausdrücklich in § 4a BDSG erwähnt, lässt sich eine wirksam erteilte Einwilligung für die Zukunft widerrufen. Die Wirkung eines diesbezüglichen Widerrufs entfaltet sich ex nunc, das heißt sämtliche bis zum Zeitpunkt des Widerspruchs vollzogenen Datenverarbeitungsvorgänge sind bis dahin von der Einwilligung gedeckt.[174] Gerade dieser Aspekt erweist sich als praktische Schwierigkeit im Hinblick auf den weiteren Umgang mit den personenbezogenen Daten von Kunden innerhalb des CRM-Systems: Erfolgt ein Widerspruch, dürfen mit den Daten keinesfalls zukünftige Verarbeitungsvorgänge – beispielsweise ein automatisiertes Verknüpfen von Daten oder in Bezug setzen mit anderen Daten – stattfinden. Vollkommen neue Informationen, die durch Anwendung von Data-Mining-Methoden auf diese Daten erst entstanden sind, werden in vielen Fällen gar nicht mehr als solche erkennbar sein.

Aus praktischer Sicht ist die Rechtfertigungsgrundlage der Einwilligung im Vergleich zu den Zulässigkeitsvarianten aus § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG nachrangig in Betracht zu ziehen. Die besondere Problematik liegt in der möglichen Verweigerung eines Einverständnisses durch den Betroffenen: Ergibt sich die Rechtfertigung zum Umgang mit den personenbezogenen Daten der Kunden bereits aus den gesetzlichen Erlaubnistatbeständen, und will der Datenverarbeiter dennoch auf das Mittel der Einwilligung zurückgreifen, so kann er sich bei deren Verweigerung im Nachhinein grundsätzlich nicht mehr auf § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG berufen. Daneben besteht die oben angeführte Problematik der Rücknahme einer Einwilligung, die dazu führen kann, dass die Rechtsgrundlage zum Umgang mit den Daten wegfällt.[175]

[173] *Weber et al.*, DuD 2003, 614 (618); in Bezug auf Telefonwerbung *BGH* v. 16.3.1999, RDV 1999, 163; *BGH* v. 27.1.2000, NJW 2000, 2677; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 8; *Bizer et al.*, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, 2006, 40 ff.; zur Gestaltung rechtskonformer Datenschutzklauseln *Heidemann-Peuser*, DuD 2002, 389 ff.

[174] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 4a Rn. 13.

[175] *Engelien-Schulz*, VR 2009, 366 (368); in Bezug auf widerrufene Einwilligungen innerhalb des Arbeitsverhältnisses *Gola*, RDV 2002, 109 (110).

Im Hinblick auf die Abgabe der datenschutzrechtlichen Einwilligung wird außerdem vertreten, dass das Kopplungsverbot – wie bei §§ 12 Abs. 3 TMG a. F. und 95 Abs. 5 TKG – den Aspekt der Freiwilligkeit stützen soll. Das Kopplungsverbot besagt, dass das Zustandekommen des Vertrags nicht von der Einwilligung in Verarbeitungsvorgänge, die personenbezogene Daten betreffen, abhängig gemacht werden darf. Wird eine diesbezügliche Einwilligung nicht abgegeben, reicht dies für den Ausschluss eines Vertragsverhältnisses nur insoweit aus, als die verantwortliche Stelle präzise darlegen kann, weshalb sie auf die konkret verlangten Daten oder Verarbeitungsprozesse angewiesen ist. Ein vorenthaltenes Einverständnis darf zu keiner Benachteiligung des Kunden führen.[176] Willigen Kunden in die für den Betrieb des Gesprächsmanagement-Systems notwendigen personenbezogenen Datenverarbeitungen nicht ein, muss das System in bestimmten Fällen bei den jeweiligen Kunden oder Gesprächen deaktiviert werden.

Zusammenfassend lässt sich festhalten, dass für die Beurteilung der Zulässigkeit des Umgangs mit Kundendaten entscheidend ist, welches rechtliche Verhältnis zwischen dem Callcenter oder dessen Auftraggeber und den Kunden vorliegt.

Da sich die Intensität der personenbezogenen Datenverarbeitungen bei den einzelnen Hauptkomponenten des Gesprächsmanagement-Systems stark voneinander unterscheidet, bedarf es einer komponentenspezifischen Betrachtung, inwieweit das informationelle Selbstbestimmungsrecht jeweils potenziell beeinträchtigt werden kann. Überdies ist stets das konkrete Tätigkeitsfeld des Callcenters mit zu berücksichtigen: So sind sensitive Daten an wesentlich strengere Verarbeitungsvoraussetzungen gebunden als „gewöhnliche“ personenbezogene Daten.

3.1.1.2 Zulässigkeitsalternativen im öffentlichen Bereich

Ebenso wie im nichtöffentlichen Bereich gibt es in der öffentlichen Verwaltung Bestrebungen, die internen Abläufe zu optimieren.[177] Für Callcenter, die durch öffentliche Stellen des Bundes betrieben werden und soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten grundsätzlich dieselben Zulässigkeitsvoraussetzungen für den Datenumgang aus § 4 Abs. 1 BDSG wie für nichtöffentliche Callcenter-Betriebe. Dies bedeutet, dass ein Datenumgang nur erfolgen darf, wenn eine gesetzliche Grundlage in Form einer bereichsspezifischen Regelung vorliegt oder im Bundesdatenschutzgesetz enthalten ist, oder darin ein-

[176] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 89 ff.
[177] S. zur Verwaltungsmodernisierung durch Mobile Government *Roßnagel/Knopp*, DÖV 2006, 982 ff.

gewilligt wurde.[178] Dies gilt analog für Callcenter-Betriebe der öffentlichen Landesverwaltung, für welche das Datenschutzgesetz des jeweiligen Landes maßgeblich ist. Rechtsvorschriften stellen im öffentlichen Bereich allgemein die bedeutendste Legitimationsgrundlage für den Umgang mit personenbezogenen Daten dar.

Die Befugnisse der öffentlichen Verwaltungsorgane beschränken sich auf die Wahrnehmung gesetzlich vorgeschriebener Aufgaben oder ihnen innerhalb ihrer Organisationsgewalt zugewiesener Funktionen. Aus dem Grundsatz der Gesetzmäßigkeit, an den die Verwaltung gebunden ist, resultiert die Verpflichtung, nur dann mit personenbezogenen Daten der Bürger umzugehen, wenn und soweit dies zur Aufgabenerfüllung geeignet und erforderlich ist.[179] Dies ergibt sich regelmäßig aus bereichsspezifischen Regelungen.[180]

Durch eine Einwilligung kann sich eine Verwaltungsstelle im Ausnahmefall grundsätzlich weiterreichende Verarbeitungsbefugnisse erteilen lassen, als sie im Gesetz vorgesehen sind; dies allerdings nur in sehr engen Grenzen. Der Datenumgang muss direkten Bezug zur Aufgabenerfüllung besitzen und dazu geeignet, das heißt mindestens nützlich, sein. Personenbezogene Daten der Bürger, die keinen Zusammenhang mit der gesetzlichen Aufgabe der Verwaltungsstelle aufweisen, dürfen trotz Einwilligung nicht verwendet werden.[181]

Dass sich Datenverarbeitungsvorgänge auch im öffentlichen Bereich durch Einwilligungen legitimieren lassen, zeigt sich zum einen am Wortlaut und zum anderen an der Systematik des Bundesdatenschutzgesetzes: Erstens enthält es keine ausdrückliche Untersagung dieser Rechtfertigungsgrundlage in Bezug auf öffentliche Stellen. Zweitens wurde die Möglichkeit der Abgabe einer Einwilligung in der Gesetzessystematik „vor die Klammer gezogen“ und kann somit sowohl von nichtöffentlichen als auch von öffentlichen Organisationen herangezogen werden. Insbesondere die Tatsache, dass in den Datenschutzgesetzen der Länder die Einwilligungsmöglichkeit ausdrücklich verankert ist, zeigt, dass auch im Bereich der öffentlichen Verwaltung datenschutzrechtliche Einwilligungen zur Anwendung gelangen können.[182]

---

[178] *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.7 Rn. 6; *Engelien-Schulz*, VR 2009, 73 (74).
[179] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 74; *Menzel*, DuD 2008, 400 ff.
[180] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 4a Rn. 12; *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 13 Rn. 2.
[181] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 74; *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.7 Rn. 39.
[182] So zutreffend *Engelien-Schulz*, VR 2009, 73 (76).

Beim Datenumgang im öffentlichen Bereich auf Bundesebene wird in Bezug auf dessen Zulässigkeit nach den Phasen der

- Datenerhebung,
- Datenspeicherung, -veränderung oder -nutzung,
- Datenübermittlung an öffentliche sowie nichtöffentliche Stellen

differenziert.

Nach § 13 Abs. 1 BDSG ist eine personenbezogene Datenerhebung zulässig, wenn sie zur Aufgabenerfüllung der öffentlichen Stelle erforderlich ist. Es dürfen nur solche Daten erhoben werden, ohne die die öffentliche Einrichtung ihre gesetzlichen Aufgaben nicht, nicht vollständig, nicht rechtmäßig oder nur mit unverhältnismäßigem Aufwand erledigen könnte.[183] Die Datenerhebung auf Vorrat – wie für den Betrieb des CRM-Systems notwendig – ist mit dem Erfordernis nach aktueller Erforderlichkeit der Daten zur Aufgabenerfüllung nur schwerlich in Einklang zu bringen.[184] Allerdings schließt allein der Umstand, dass bestimmte Aufgaben der öffentlichen Verwaltung bislang ohne die Callcenter-Dienstleistung erledigt werden konnten, die Erforderlichkeit dieser Leistung nicht aus. Diesbezüglich gilt es, den zusätzlichen Zweck der Bürgerfreundlichkeit zu berücksichtigen, vergleichbar mit dem Serviceangebot von Bürgerbüros.[185]

Zum einen muss zwar der Zugriff auf Grunddaten sichergestellt sein, damit adäquate Auskünfte zum Beispiel über Verwaltungsvorgänge überhaupt möglich sind. Zum anderen darf aber nicht auf sämtliche personenbezogenen Daten von Kunden zugegriffen werden können, wenn der Zweck der Callcenter-Dienstleistung beispielsweise lediglich in der einfachen Beratung, deren Durchführung mit wenigen personenbezogenen Daten möglich ist, besteht. Hier kommt auch der im Volkszählungsurteil[186] des *BVerfG* entwickelte Grundsatz der „informationellen Gewaltenteilung“ zum Tragen: Dieser sieht vor, innerhalb der Verwaltung ausreichende Barrieren einzurichten, die den unbegrenzten Datenumgang verhindern sollen. Dazu kommen Weitergabe- und Verwertungsverbote sowie technische und organisatorische Maßnahmen in Betracht.[187] Die öffentliche Verwaltung verkörpert keine In-

[183] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 13 Rn. 15; *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.7 Rn. 57.
[184] Simitis/*Sokol*, BDSG, 7. Aufl. 2011, § 13 Rn. 26.
[185] S. dazu etwa *o. V.*, Vom Bürgerbüro zum Internet (abrufbar unter: http://www.datenschutz.hessen.de/download.php?download_ID=140); zu den Vorzügen von Bürgerbüros s. *Kraemer/Kaufung*, VR 2000, 200 ff.; *Müller*, DÖD 2000, 16 ff.
[186] *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[187] *Laue*, Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung, 2010, 318.

formationseinheit, in der personenbezogene Daten zwischen verschiedenen Stellen nach Belieben ausgetauscht werden dürfen.[188]

Gerade für öffentliche Stellen bleibt zu fordern, dass sie sich nicht durch totale Informiertheit auszeichnen, sondern vielmehr ein ausgeglichenes Verhältnis zwischen Behalten und Vergessen gewährleisten.[189] Wurden personenbezogene Daten erhoben, ist regelmäßig zu überprüfen, ob die Daten weiterhin für die Aufgabenerfüllung der Stelle erforderlich sind; sollte man zum Ergebnis gelangen, dass dies nicht zutrifft, müssen die Daten gelöscht werden.[190]

Auch die personenbezogene Datenspeicherung, -veränderung oder -nutzung ist nach § 14 Abs. 1 Satz 1 BDSG erlaubt, wenn sie zur Aufgabenerfüllung des öffentlichen Callcenters als erforderlich gilt. Die personenbezogenen Daten müssen darüber hinaus für die Zwecke verwendet werden, für welche die Erhebung erfolgte. An dieser Stelle kommt der dem gesamten Datenschutzrecht immanente Zweckbindungsgrundsatz zum Ausdruck: Bereits vor Erhebung der personenbezogenen Daten haben die Zwecke hierzu grundsätzlich festzustehen. Damit keine verbotene Vorratsdatenspeicherung entsteht, ist die Zweckbestimmung vollständig am intendierten Datenumgang auszurichten. So kann die Speicherung der Daten für festgelegte – auch in der Zukunft liegende – Zwecke durchaus zulässig sein. Dazu müssen die gesetzlichen Voraussetzungen vorliegen.[191] Bestimmte Register, wie das Bundeszentral- oder Verkehrszentralregister, lassen sich exemplarisch als zulässige Vorratsdatenspeicherungen durch öffentliche Stellen ins Feld führen. Ihre Zulässigkeit ergibt sich aus bereichsspezifischen Regelungen.[192]

Effizientes Verwaltungshandeln vermag im Einzelfall zu erfordern, dass die strikte Zweckbindung nicht immer aufrechterhalten werden kann. Deshalb ist mit § 14 Abs. 2 BDSG ein umfangreicher Ausnahmekatalog gegeben, der das Speichern, Verändern oder Nutzen der Daten in bestimmten Fällen auch für andere Zwecke für zulässig erklärt. Die in § 14 Abs. 1 BDSG festgeschriebene Erforderlichkeit erstreckt sich in jedem Fall auch auf erlaubte Zweckänderungen.[193] Im Kontext der vorgesehenen Anwendungsfelder des Gesprächsmanagement-Systems kommen regelmäßig nur die Ausnahmen aus § 14 Abs. 1 Nr. 1 und Nr. 2 BDSG in Betracht.

[188] *o. V.*, Datenschutzgerechtes eGovernment, 14 f. (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/egovern/egovern.pdf).
[189] *Bull*, ZRP 1975, 7 (11 f.).
[190] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 13 Rn. 17.
[191] *Jürgens*, DSB 4/2000, 8; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 14 Rn. 7 ff.
[192] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 14 Rn. 6.
[193] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 14 Rn. 12.

Die Ausnahme aus Nr. 1 betrifft den Fall, dass eine Norm eine Zweckänderung vorsieht oder zwingend voraussetzt. Die erste Alternative liegt vor, wenn die Vorschrift die Änderung des Zwecks ausdrücklich anordnet oder zulässt;[194] die zweite kann bei Rechtsnormen gegeben sein, die im Hinblick auf den Datenumgang keine ausdrückliche Aussage enthalten und insofern nicht dem Kriterium der Normenklarheit genügen; dies ist oftmals bei älteren Rechtsvorschriften der Fall.[195] Von der Ausnahme aus Nr. 1 werden in erster Linie bereichsspezifische Vorschriften erfasst.

Besonderes Gewicht fällt der Legitimation aus einer Einwilligung gemäß § 14 Abs. 2 Nr. 2 BDSG zu: Eine Zweckänderung ist zulässig, wenn der Kunde diesbezüglich eingewilligt hat. Zur Ausdehnung der hoheitlichen Befugnisse kann die Einwilligung jedoch nicht dienen.[196] Im Vergleich zur allgemeinen Einwilligung aus §§ 4 Abs. 1, 4a BDSG besitzt diese Spezialregelung keinen eigenständigen normativen Gehalt.[197] Es gelten die bereits dargestellten Grundsätze zur Einwilligung bei öffentlichen Stellen.

Datenübermittlungen an öffentliche oder nichtöffentliche Stellen sind für den Betrieb des Gesprächsmanagement-Systems nicht vorgesehen, da ausgelagerte Dienstleistungen im Wege der Auftragsdatenverarbeitung erbracht werden.

Die Datenschutzgesetze der Länder enthalten dem Dargestellten entsprechende Regelungen;[198] insofern kann von deren expliziter Erörterung abgesehen werden.

Insbesondere bei den Merkmalen Erforderlichkeit und Zweckbindung sind im Hinblick auf den Umgang mit personenbezogenen Daten bei öffentlichen Stellen strenge Maßstäbe anzulegen.[199] Im Hinblick auf Callcenter-Dienstleistungen ist das Merkmal der Erforderlichkeit unter Berücksichtigung der Aufgabe des bürgerfreundlichen Umgangs zu bestimmen. Wie sich diese strikte Vorgabe auf die Zulässigkeit des Betriebs des Gesprächsmanagement-Systems bei öffentlichen Stellen auswirkt, wird in Kapitel 3.1.1.4 „Zulässigkeit des Datenumgangs in den einzelnen Systemkomponenten“ aufgezeigt.

[194] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 14 Rn. 12 f.
[195] Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 14 Rn. 56; *D/K/W/W*, BDSG, 3. Aufl. 2010, § 14 Rn. 13.
[196] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 14 Rn. 14.
[197] Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 14 Rn. 57.
[198] So etwa in §§ 13 - 19 LDSG.
[199] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 14 Rn. 9 ff.

3.1.1.3 Besonderheit beim Umgang mit sensitiven personenbezogenen Daten

Das Datenschutzrecht durchdringt praktisch sämtliche Lebensbereiche, da ihm eine Querschnittsfunktion zukommt. Aufgrund der bestehenden Unterschiedlichkeit der Lebenssachverhalte sind spezifische rechtliche Vorkehrungen notwendig, die ein höheres Schutzniveau gewährleisten als das allgemeine Datenschutzrecht.[200] Es existieren zahlreiche Berufs- und Geschäftsgeheimnispflichten, die für Callcenter-Betriebe relevant werden können, wenn Callcenter-Dienstleistungen geheim zu haltende Informationen betreffen.[201] Das Gesprächsmanagement-System soll auch in Anwendungsszenarien zum Einsatz gelangen, bei denen sensitive personenbezogene Daten der Kunden betroffen sind, wie im Bereich der Krankheitsprävention.

Um bezeichnete Daten handelt es sich gemäß § 3 Abs. 9 BDSG bei Angaben über rassische und ethnische Herkunft, über politische, religiöse und philosophische Ansichten sowie über Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Die Charakteristika dieser Daten bergen ein besonderes Risiko für die informationelle Selbstbestimmung der Betroffenen in sich. Sie sollen daher im Grundsatz unzugänglich sein. Art. 8 Abs. 1 der EG-Datenschutzrichtlinie[202] enthält ein grundsätzliches Verbot des Umgangs mit solchen Daten, für das in den nachfolgenden Absätzen Ausnahmen formuliert werden; es ist insofern auf den Verwendungszusammenhang abzustellen.[203]

Allgemein dürfen nichtöffentliche Callcenter besonders schützenswerte personenbezogene Daten grundsätzlich nur unter den Voraussetzungen der §§ 28 Abs. 6 - 9 und 29 Abs. 5 BDSG erheben, verarbeiten, nutzen und übermitteln. Die genannten Vorschriften enthalten Ausnahmetatbestände, wann diese Vorgänge zulässig durchführbar sind.[204]

Der Befugnis zum Umgang mit besonderen personenbezogenen Daten aus § 28 Abs. 6 Nr. 3 BDSG dürfte im Zusammenhang mit Callcenter-Dienstleistungen gro-

[200] *Miedbrodt*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.9 Rn. 1.
[201] Zum Umgang mit Gesundheitsdaten durch Versicherungsunternehmen *Neuhaus/Kloth*, NJW 2009, 1707 ff.; zum anwaltlichen Berufsgeheimnis *Spielmann*, AnwBl 2010, 373 ff.
[202] Richtlinie 95/46/EG v. 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
[203] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 86; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BDSG, § 28 Rn. 10; *Gola*, RDV 2001, 125; *Franzen*, RDV 2003, 1 (3); *Lambrich/Cahlik*, RDV 2002, 287 (289); *Iraschko-Luscher/Kiekenbeck*, NZA 2009, 1239; zum Einwilligungserfordernis von Patienten bei der Übergabe von Arztpraxen an Nachfolger *BGH* v. 11.12.1991, NJW 1992, 737; *Roßnagel*, NJW 1989, 2303 ff.; *Körner-Damman*, NJW 1992, 1543 ff.
[204] *Gola*, RDV 2001, 125 f.

ße praktische Relevanz zukommen. Sie betrifft die Verwendung von sensitiven Daten im Rahmen von Vertragsverhältnissen und vertragsähnlichen Vertrauensverhältnissen.[205] Hiernach ist der Umgang mit diesen Daten gestattet, wenn es zur Geltendmachung, Verteidigung oder Ausübung rechtlicher Ansprüche notwendig ist und keine schutzwürdigen Interessen der Betroffenen an seinem Ausschluss überwiegen.

§ 28 Abs. 7 BDSG regelt die Erhebung, Verarbeitung oder Nutzung sensitiver personenbezogener Daten im Zusammenhang mit Organisationen, deren Tätigkeitsfeld sich beispielsweise auf die Gesundheitsvorsorge, medizinische Diagnostik und Verwaltung von Gesundheitsdienstleistungen erstreckt. Solche Stellen sind von ihrem Geschäftszweck her gezwungen, mit spezifischen sensitiven Daten umzugehen. Die Verwendung der Gesundheitsdaten darf durch Stellen erfolgen, die aufgrund ihrer Schweigepflichten aus § 203 StGB zum vertraulichen Umgang mit diesen Daten verpflichtet sind.[206]

Angehörige bestimmter Berufsgruppen und Amtsträger unterliegen Geheimhaltungsverpflichtungen, die neben den Vorschriften des Bundesdatenschutzgesetzes gemäß § 1 Abs. 3 Satz 2 BDSG anzuwenden sind.[207] Somit ist sichergestellt, dass stets die Vorschrift, die das höhere Schutzniveau der konkurrierenden Regelungen gewährleistet, Vorrang erhält.[208] Als Berufsgruppen, die den Geheimnispflichten aus § 203 Abs. 1 Satz 1 StGB unterfallen, lassen sich exemplarisch anführen:

- Ärzte und Angehörige von Heilberufen,
- Psychologen,
- Rechtsanwälte,
- Sozialarbeiter und
- Angehörige einer privaten Unfall-, Lebens- oder Krankenversicherung.

Sollen Tätigkeiten, die den Berufsgeheimnispflichten nach § 203 Abs. 1 Satz 1 StGB unterliegen, im Wege des Outsourcings auf externe Dienstleistungsunternehmen übertragen werden, so ist dies straffrei unter der Bedingung möglich, dass der Auftragnehmer als „Gehilfe“ im Sinne des § 203 Abs. 3 Satz 2 StGB eingeordnet werden kann. Ein solcher Fall könnte etwa bei einer Auslagerung von Beratungs-

[205] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 77 f.
[206] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 80; *Kilian*, NJW 1992, 2313 (2317); s. zum Komplex Gesundheits- und Sozialdatenschutz ausführlich *Bake/Blobel/Münch* (Hrsg.), Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, 3. Aufl. 2009.
[207] *Miedbrodt*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.9 Rn. 2; *Rasmussen*, NZS 1998, 67 (69).
[208] *Schirmer*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 7.12 Rn. 26.

leistungen im Gesundheitswesen auf ein externes Callcenter gegeben sein. Die Callcenter-Mitarbeiter kämen dabei zwangsläufig mit Informationen in Kontakt, die ein Berufsgeheimnis darstellen.[209] Im medizinischen Kontext sind dies etwa Angaben zur Krankheit und Diagnose, durchgeführte Therapie sowie Prognose über den Heilungsverlauf.[210] Ein berufsmäßig tätiger Gehilfe gilt nicht als Dritter, gegenüber dem das Geheimnis nicht offenbart werden darf. Das Berufsgeheimnis bezieht den Gehilfen in den Kreis der Schweigepflichtigen mit ein, somit handelt es sich um einen befugten Mitwisser. Damit das beauftragte Callcenter die Stellung des Gehilfen einnehmen kann, ist es notwendig, dass das auslagernde Unternehmen als primär Schweigepflichtiger die Herrschaft über die zur Verfügung gestellten Daten behält, diese Herrschaft ausüben kann und diese tatsächlich auch ausübt. Eine gesetzliche Regelung, wann eine derartige Steuerungsmacht vorliegt, existiert nicht; ihre Bestimmung kann anhand der Kriterien für das Vorliegen einer Auftragsdatenverarbeitung gemäß § 11 BDSG erfolgen.[211] Aus Gründen der Vollständigkeit wird darauf hingewiesen, dass bei einer Datenübermittlung die spezifische Zweckbindung der Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, aus § 39 BDSG zu beachten ist.

Weitere gesetzliche Geheimhaltungsverpflichtungen ergeben sich beispielsweise aus

- § 18 Abs. 1 BNotO für Notare,
- § 43a Abs. 2 BRAO für Rechtsanwälte,
- § 57 Abs. 1 StBerG für Steuerberater,
- § 43 Abs. 1 Satz 1 WiPrO für Wirtschaftsprüfer,
- §§ 30 AO, 5 Abs. 1 MRRG für Amtsträger.[212]

Eine besondere Stellung nehmen gemäß § 28 Abs. 9 BDSG Organisationen ein, die eine politische, philosophische, religiöse oder gewerkschaftliche Ausrichtung haben und keine erwerbswirtschaftlichen Ziele verfolgen. Sie dürfen sensitive Daten ihrer Mitglieder und regelmäßig mit der Stelle in Kontakt stehender Personen in dem Umfang verwenden, wie es für die Aufgabenerfüllung der Organisation notwendig ist.[213]

[209] *Heghmanns/Niehaus*, NStZ 2008, 57.
[210] *Langkeit*, NStZ 1994, 6.
[211] *Heghmanns/Niehaus*, NStZ 2008, 57 ff.
[212] *Miedbrodt*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.9 Rn. 4 f.
[213] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 28 Rn. 20.

§ 13 Abs. 2 Nr. 1 - 9 BDSG enthält einen Katalog von Ausnahmetatbeständen, wann öffentliche Stellen besondere Arten von personenbezogenen Daten erheben dürfen.[214] Die normierten Ausnahmemöglichkeiten sind eng auszulegen, um das erhöhte Schutzniveau dieser Daten nicht zu unterlaufen.[215] Ausnahmen können zum Beispiel in

- einer Rechtsvorschrift,
- lebenswichtigen Interessen,
- der Gefahrenabwehr und
- der Gesundheitsversorgung

bestehen.

Soll eine vom Erhebungszweck abweichende Speicherung, Veränderung oder Nutzung sensitiver personenbezogener Daten erfolgen, ist dies unter den Voraussetzungen des § 14 Abs. 5 BDSG zulässig. Eine öffentliche Einrichtung, die bereits zur Erhebung besonderer Arten personenbezogener Daten berechtigt ist, soll – bis auf zwei Ausnahmen – unter denselben Bedingungen den zweckändernden Umgang mit den Daten pflegen dürfen. Die Ausnahmen betreffen die wissenschaftliche Forschung und die Gesundheitsversorgung.[216]

Die Datenschutzgesetze der Länder enthalten teilweise vom Bundesdatenschutzgesetz erheblich abweichende Vorschriften im Hinblick auf den Umgang mit besonderen Arten personenbezogener Daten: So ist dieser Umgang etwa in Hessen neben einer dazu ermächtigenden Rechtsvorschrift nur dann erlaubt, wenn er im Interesse des Betroffenen liegt und der Landesdatenschutzbeauftragte im Vorfeld hierzu angehört wurde.[217] Aufgrund der Vielgestaltigkeit der einzelnen landesrechtlichen Regelungen hinsichtlich des Umgangs mit sensitiven personenbezogenen Daten wird auf eine Darstellung im Einzelnen verzichtet.

Neben den gesetzlichen Erlaubnistatbeständen kann – sowohl gegenüber nichtöffentlichen Stellen gemäß § 28 Abs. 6 BDSG als auch gegenüber öffentlichen Organisationen gemäß § 13 Abs. 2 Nr. 2 BDSG – eine Einwilligung zum zulässigen Umgang mit besonderen Arten personenbezogener Daten führen. § 4a Abs. 3 BDSG regelt die Anforderungen an diese Einwilligung. Zu den ohnehin im Rahmen einer datenschutzrechtlichen Einwilligung bestehenden Anforderungen tritt diesbe-

[214] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 13 Rn. 13.
[215] Simitis/*Sokol*, BDSG, 7. Aufl. 2011, § 13 Rn. 34.
[216] Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 14 Rn. 119 ff.
[217] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 13 Rn. 25; s. § 7 Abs. 4 HDSG.

züglich ein weiteres Kriterium hinzu: Das Einverständnis muss sich ausdrücklich auf die verwendeten sensitiven Daten beziehen. Überdies wird in Bezug auf diese besonderen Arten von Daten im Regelfall noch eher das Schriftformerfordernis zum Tragen kommen, als dies bei „herkömmlichen" personenbezogenen Daten der Fall ist.[218] Jedenfalls wird ein konkludentes oder stillschweigendes Einverständnis zum Umgang mit sensitiven personenbezogenen Daten nicht ausreichen.[219]

3.1.1.4 Zulässigkeit des Datenumgangs in den einzelnen Systemkomponenten

Das Gesprächsmanagement-System besteht aus mehreren Komponenten, die in ihrem Zusammenspiel die gleichzeitige Suche in mehreren Informationsquellen und Rückkopplung der gefundenen Ergebnisse an das Frontend-System der Callcenter-Arbeitsplätze ermöglichen. Grundsätzlich ist auch denkbar, bestimmte Systembestandteile wegzulassen. So könnte etwa auf die Anbindung der Kundendatenbank verzichtet werden; in diesem Fall würden sich die ausgelösten Suchvorgänge auf die anderen zur Verfügung stehenden Datenquellen beschränken.

Da bei der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten von Kunden, bezogen auf die verschiedenen Systembestandteile, unterschiedlich hohe Zulässigkeitsvoraussetzungen zu erfüllen sind, werden diese nachfolgend komponentenspezifisch dargestellt. Der Grund liegt darin, dass die Tiefe des Eingriffs in das Persönlichkeitsrecht der Kunden je nach Verarbeitungsvorgang und den daraus (potenziell) resultierenden neuen Daten variiert. Um beurteilen zu können, welche Zulässigkeitsvoraussetzungen vorliegen müssen, ist der gesamte Datenverarbeitungsprozess des Gesprächsmanagement-Systems zu zerlegen und eine detaillierte Betrachtung der einzelnen Systemkomponenten vorzunehmen.

Abschließend wird eine Lösung dargestellt, wie sich das vollständige Gesprächsmanagement-System im Hinblick auf den Umgang mit den Kundendaten datenschutzrechtlich zulässig betreiben lässt.

[218] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 57; *Gola*, RDV 2001, 125 (126); Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 88.
[219] *Iraschko-Luscher/Kiekenbeck*, NZA 2009, 1239; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 88.

3.1.1.4.1 Frontend-System

Unter der Bezeichnung „Frontend-System“ wird im Folgenden die den Callcenter-Agenten an ihren Arbeitsplätzen zur Verfügung stehende Hard- und Software verstanden. Diese umfasst das Computersystem, mit dem der Mitarbeiter insbesondere seine Telefonate organisiert, Termine koordiniert und Vermerke zu einzelnen Telefongesprächen eintragen kann. Über das Frontend-System lassen sich Kunden gezielt anrufen oder Anrufe der Kunden entgegennehmen; es verkörpert eine Verschmelzung von Computer und Telefon (CTI). Der Telefonapparat dient nur noch zur Übermittlung der Sprache; oftmals wird er durch ein Headset ersetzt.[220] Darüber hinaus ist im Frontend-System ein Webservice integriert, der es den Callcenter-Agenten über manuelle Eingaben von Suchbegriffen ermöglicht, im World Wide Web nach Problemlösungsansätzen zu suchen.

Die durch das Frontend-System ausgelösten Datenverarbeitungsvorgänge in den angeschlossenen Datenbanken (CRM-System) sowie externen Wissensquellen sind nicht in die datenschutzrechtliche Betrachtung des Frontend-Systems mit einbezogen, da diese einer selbstständigen Betrachtung zu unterziehen sind.[221] Dasselbe gilt für Auswertungsergebnisse, wie die der Verhaltenserkennung, die lediglich am Frontend-System dargestellt werden, deren Berechnung jedoch in anderen – fakultativ zu- oder abschaltbaren – Datenverarbeitungsprozessen erfolgt.

Nachfolgende Abbildung zeigt stellvertretend für sämtliche am Frontend-System der Agenten verfügbaren Funktionen eine einzelne Anwendung zum Management der Kundenkontakte:

[220] *o. V.*, CTI - Computer Telephony Integration (abrufbar unter: http://www.elektronik-kompendium.de/sites/kom/0603051.htm).
[221] Ausführlich in den Kapiteln 3.1.1.4.4 „CRM-System: Kundendatenbank und Archivdatenbank“ und 3.1.1.4.5 „Weitere Informationsquellen“.

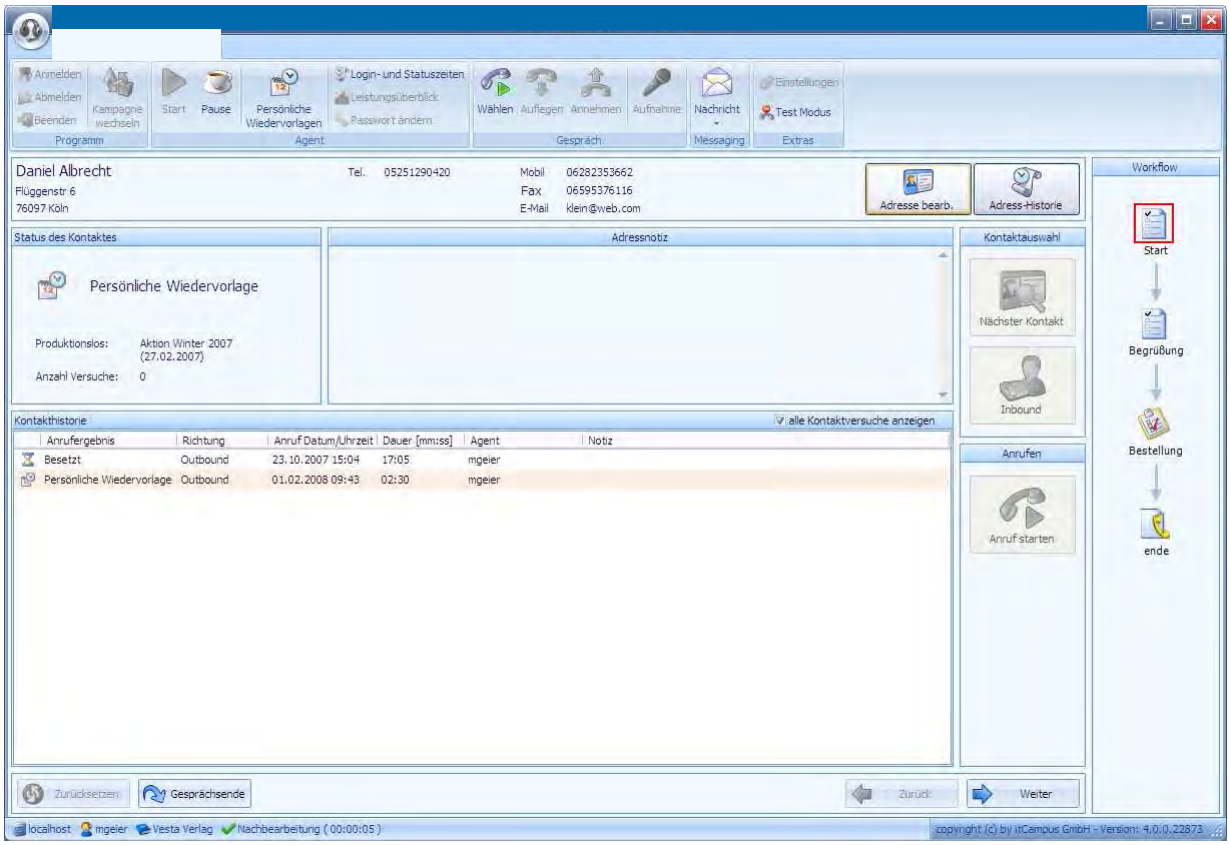

Abb. 2: Frontend-System: Kontaktmanagement.
Quelle: itCampus Software- und Systemhaus GmbH.

Fraglich ist, unter welchen Zulässigkeitsvoraussetzungen die Funktionen des Frontend-Systems, die einen Umgang mit personenbezogenen Daten der Kunden einschließen, genutzt werden dürfen. Neben einer Einwilligung der Kunden oder dem Vorliegen bereichsspezifischer Erlaubnistatbestände erlangt im Hinblick auf privatrechtliche Callcenter-Betriebe insbesondere der § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 sowie Abs. 3 BDSG Relevanz.

Aus beiden erstgenannten Erlaubnisnormen könnte sich der Einsatz des Frontend-Systems grundsätzlich legitimieren lassen. Entscheidend für die Zulässigkeit ist jeweils, dass der Umgang mit den personenbezogenen Daten der Kunden für die vorgesehenen Zwecke erforderlich ist. Darüber hinaus darf für den Fall, dass sich der Datenumgang auf die Wahrung berechtigter Interessen von nichtöffentlichen Callcenter-Betrieben stützen soll (Nr. 2), zusätzlich kein Grund zur Annahme eines überwiegenden schutzwürdigen Interesses der Kunden vorliegen.

Im Falle der Nr. 1 hat der Zweck des Datenumgangs im Zusammenhang mit der Abwicklung eines Schuldverhältnisses gemäß § 311 BGB zu stehen; der Umgang mit personenbezogenen Daten darf insoweit erfolgen, als er hierzu erforderlich ist.

Vollkommen abhängig vom jeweiligen Einsatzgebiet des Gesprächsmanagement-Systems können dabei mehr oder weniger umfangreich personenbezogene Daten als erforderlich einzustufen sein. Die Erforderlichkeit muss einzelfallabhängig bestimmt werden. Ist es beispielsweise im Rahmen eines Servicevertrags mit Kunden notwendig, bestimmte personenbezogene Daten innerhalb des Vertragsverhältnisses ständig und fortlaufend aktualisiert im Callcenter-Betrieb für die dortigen Mitarbeiter am Frontend-System abrufbar zu halten, so gilt das Kriterium der Erforderlichkeit als erfüllt. Eine solche Situation liegt vor, wenn sich eine sinnvolle Problemlösung erst mit Kenntnis etwa der detaillierten Produktdaten und der beim jeweiligen Kunden bereits aufgetretenen Störungen inklusive Zeitangabe realisieren lässt.

Gibt es hingegen die Möglichkeit, die vorgesehenen Zwecke auch ohne personenbezogene Daten zu erreichen, so ist eine solche Datenverarbeitung keinesfalls erforderlich. Ein Beispiel dafür kann eine telefonische Beratung darstellen, bei der keine Notwendigkeit besteht, Daten über die (potenziellen) Kunden zu erheben.

Im Ergebnis vermag die Zulässigkeitsvariante aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG unter den genannten Voraussetzungen den Betrieb des Frontend-Systems für die vorgesehenen Einsatzszenarien des Gesprächsmanagement-Systems zu legitimieren.

Ferner kommt in der Regel für die Fälle, in denen kein (potenzielles) Schuldverhältnis mit Kunden besteht, die Erlaubnis aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Die Datenverwendung im Frontend-System muss zur Wahrung berechtigter Interessen des Callcenters erforderlich sein. Das Kriterium des „berechtigten Interesses“ stellt keine schwer überwindbare Hürde dar: Es genügt, unter rationalen Überlegungen zum Schluss zu gelangen, dass ein begründbares Bedürfnis vorliegt. So können beispielsweise Warenhersteller das berechtigte Interesse besitzen, Daten über die Personen zu speichern, die ihre Güter erwerben, um bei potenziellen Rückrufaktionen die Käufer zeitnah kontaktieren zu können.[222] Erforderlichkeit des Datenumgangs ist allerdings nur dann gegeben, wenn keine objektiv zumutbare Alternative existiert. Konkret bedeutet dies, dass die geforderte Erforderlichkeit nicht vorliegt, wenn das Informationsziel über andere Mittel und Wege erreicht werden kann.[223] Als weiterer Vorbehalt darf kein Grund zur Annahme bestehen, dass ein überwiegendes schutzwürdiges Interesse der Betroffenen gegeben ist. Es hat also eine Interessenabwägung zu erfolgen, bei der das informationelle Selbstbestimmungsrecht der Betroffenen den berechtigten Interessen des Callcenters gegenüber-

[222] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 113.
[223] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rn. 108.

zustellen ist. Keinesfalls dürfen erhebliche und offensichtliche Umstände erkennbar sein, die eine Beeinträchtigung nahe legen.[224]

Unter den abstrakt formulierten Bedingungen kann – kurzgefasst – auch § 28 Abs. 1 Satz 1 Nr. 2 BDSG dazu dienen, das Frontend-System im Callcenter zulässig, unter Einbezug personenbezogener Kundendaten zu betreiben.

Das Frontend-System darf darüber hinaus unter Einbezug von Listendaten für Zwecke der Eigenwerbung gemäß § 28 Abs. 3 Satz 2 Nr. 1 BDSG grundsätzlich einwilligungsfrei eingesetzt werden, wenn die Beziehung zum (potenziellen) Kunden auf einem Schuldverhältnis gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG beruht oder diese Daten aus bestimmten allgemein zugänglichen Verzeichnissen erhoben worden sind. In einem solchen Fall ist nach § 28 Abs. 3 Satz 3 BDSG auch die Verwendung weiterer Kundendaten, die allerdings im Rahmen von § 28 Abs. 1 Satz 1 Nr. 1 BDSG – etwa bei Vertragsschluss – zulässig erhoben worden sein müssen, erlaubt. Somit darf beispielsweise die Telefonnummer des (potenziellen) Kunden zu den Listendaten hinzugespeichert und für Werbezwecke für eigene Angebote verwendet werden.

Die Hinzuspeicherung von Daten, die aus oben genannten allgemein einsehbaren Verzeichnissen stammen, ist demgegenüber nicht zulässig. Der Betroffene muss nicht davon ausgehen, dass öffentlich zugängliche Informationen über seine Person mit den Listendaten zusammengeführt werden, um damit Werbemaßnahmen durchzuführen.[225] Hier überwiegen die schutzwürdigen Interessen der Kunden ohne jeden Zweifel.

Nur die gesetzliche Legitimation aus § 28 Abs. 3 Satz 2 Nr. 1 BDSG erlaubt es dem Callcenter aus der Perspektive des Datenschutzes, dem Callcenter-Mitarbeiter die angereicherten Listendaten am Frontend-System anzuzeigen und diese zur Durchführung von Werbemaßnahmen gezielt einzusetzen.

Die in § 28 Abs. 3 Satz 2 BDSG enthaltenen Listendaten, die ohne Einwilligung für Werbezwecke verarbeitet oder genutzt werden dürfen, beschränken sich auf wenige Angaben, die jedenfalls nicht die Telefonnummer einbeziehen. Der Einsatz des Frontend-Systems darf sich demzufolge aufgrund der weiteren gesetzlichen Rechtfertigungsgrundlagen in der Praxis nur derart gestalten, dass die (potenziellen) Kunden von sich aus beim Callcenter anrufen und dadurch ihr Interesse an einer werbli-

[224] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 28 Rn. 52.
[225] Vollkommen zutreffend *Roßnagel/Jandt*, MMR 2011, 86 (89).

chen Ansprache bekunden. Am Frontend-System dürfen den Callcenter-Mitarbeitern keine weiteren personenbezogenen Informationen als die Listendaten angezeigt werden. Die Anzeige der Rufnummer des jeweiligen Kunden wäre bereits unzulässig. Ein anderer Einsatz des Frontend-Systems auf Basis der alternativen gesetzlichen Rechtfertigungstatbestände für Werbemaßnahmen ist datenschutzrechtlich nicht zulässig.

Was öffentliche Stellen des Bundes betrifft, die selbst Callcenter betreiben oder durch Callcenter telefonische Leistungen im Auftrag erbringen lassen, so ist die datenschutzrechtliche Zulässigkeit des Einsatzes des Frontend-Systems, sofern personenbezogene Daten der Kunden betroffen sind, insbesondere an bereichsspezifischen Vorschriften und im Übrigen an den §§ 13 - 14 BDSG zu beurteilen.

Der allgemeine Rechtfertigungsgrund für die Erhebung personenbezogener Kundendaten findet sich in § 13 Abs. 1 BDSG. Sie ist zulässig, wenn die Kenntnis dieser Daten zur Aufgabenerfüllung der Stelle erforderlich ist. Ferner muss eine örtliche, sachliche und verbandsmäßige Zuständigkeit der öffentlichen Stelle gegeben sein und die Datenerhebung muss sich rechtmäßig vollziehen.[226]

§ 14 BDSG regelt die Zulässigkeit der Speicherung, Veränderung oder Nutzung personenbezogener Daten bei öffentlichen Verwaltungseinrichtungen. Die genannten Vorgänge sind nach § 14 Abs. 1 Satz 1 BDSG erlaubt, wenn die Erfüllung der Aufgaben der öffentlichen Stelle dies erfordert und sie grundsätzlich für die Zwecke erfolgen, für die die Datenerhebung vorausging. Im Bereich der öffentlichen Verwaltung sind die möglichen Zweckfestlegungen eng an die jeweilige Aufgabe der Verwaltungsstelle geknüpft.[227]

Bei öffentlichen Stellen werden hohe Anforderungen an das Merkmal Erforderlichkeit gestellt. Ihnen kann grundsätzlich nur die Menge an Daten zugebilligt werden, auf die sie zur Aufgabenerfüllung angewiesen sind.[228] Im Zusammenhang mit Callcenter-Dienstleistungen von Behörden muss der Aspekt der Bürgerfreundlichkeit bei der Erforderlichkeitsbestimmung Berücksichtigung finden. Die durch Callcenter erbrachten Dienste dienen hauptsächlich zur Erfüllung der Primäraufgaben der öffentlichen Stellen und bieten darüber hinaus ein hohes Effektivierungspotenzial im Hinblick auf die behördeninternen Prozesse und die Bürgerorientierung. Zu nennen sind etwa die Beschleunigung der Verwaltungsabläufe und die Ausweitung der Erreichbarkeit der Behörde.

[226] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 13 Rn. 7 ff.
[227] *Laue*, Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung, 2010, 316.
[228] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 13 Rn. 15.

Falls Kunden beispielsweise Formulare oder Bescheinigungen mittels des Callcenter-Services bestellen können, sind zum Versand zumindest deren Namen und Anschriften erforderlich.[229] Wenn keine Erforderlichkeit zur Aufgabenerfüllung der Stelle besteht, darf nach Abschluss des Versandvorgangs keine weitere Speicherung der personenbezogenen Daten erfolgen; die Daten sind zu löschen.

Eine zulässige längerfristige Speicherung ist demgegenüber in Fällen denkbar, die zum Beispiel die Kenntnis der Kontaktdaten zur Klärung eines Sachverhalts voraussetzen, oder wenn die Daten im Zusammenhang mit einem nicht abgeschlossenen Antragsverfahren stehen. Erstreckt sich der Aufgabenbereich des Callcenters auf die Auskunftserteilung gegenüber Kunden in Bezug auf derartige Vorgänge oder Verwaltungsprozesse, können auch weitergehende personenbezogene Daten als erforderlich einzustufen sein.[230] Am Frontend-System im Callcenter dürfen diese Daten abrufbar sein und den zuständigen Mitarbeitern zur Verrichtung ihrer Arbeitsaufgabe zur Verfügung stehen.

Es sind somit – in Abhängigkeit davon, welche telefonische Serviceleistung das öffentliche Callcenter bereitstellt – mehr oder weniger umfangreich personenbezogene Daten der Kunden erforderlich. Handelt es sich dabei beispielsweise um

- Informationen über notwendige Formulare und einzuhaltende Fristen,
- Auskünfte über den zuständigen Mitarbeiter oder
- die Entgegennahme von Anregungen durch Kunden,

kann die Dienstleistung des öffentlichen Callcenters vollkommen ohne Kenntnis personenbezogener Daten der Kunden realisiert werden.[231]

Von öffentlichen Landeseinrichtungen betriebene Callcenter haben sich an denselben Grundsätzen wie öffentliche Stellen des Bundes zu orientieren, da die Landesdatenschutzgesetze vergleichbare Vorschriften enthalten.

[229] *o. V.*, Vom Bürgerbüro zum Internet, 11 (abrufbar unter: http://www.datenschutz.hessen.de/download.php?download_ID=140).
[230] *o. V.*, Vom Bürgerbüro zum Internet, 11 (abrufbar unter: http://www.datenschutz.hessen.de/download.php?download_ID=140); zum konfligierenden Verhältnis zwischen informationeller Selbstbestimmung und Informationsfreiheit *Roßnagel*, MMR 2007, 16 ff.
[231] *o. V.*, Vom Bürgerbüro zum Internet, 11 (abrufbar unter: http://www.datenschutz.hessen.de/download.php?download_ID=140).

3.1.1.4.2 Telefonanlage

Der eingesetzten Telefonanlage kommt die zentrale Aufgabe der Vermittlung ein- und ausgehender Telefonate zu. Was die im Callcenter ankommenden Anrufe anbelangt, so übernimmt die integrierte ACD-Funktion die Zuordnung der Anrufe zum zuständigen Callcenter-Mitarbeiter. Mit der Bereitstellung verschiedener Nummernkreise können gleichzeitig unterschiedliche Aufgabenbereiche durch das Callcenter bearbeitet werden: Während zum Beispiel ein Teil der Mitarbeiter den Kundenservice für ein bestimmtes Produkt bereitstellt, kümmert sich ein anderer um Fragen im Gesundheitsbereich.

Falls sich zu einem bestimmten Zeitpunkt sämtliche zuständigen Callcenter-Agenten in einem Gespräch befinden und weitere Anrufe hinzukommen, lassen sich diese in eine Warteschleife stellen. Die Einreihung des jeweiligen Anrufs in die Warteschleife kann grundsätzlich nach verschiedenen Kriterien erfolgen. So ist es denkbar, den jeweiligen Kunden anhand der Telefonnummer des ankommenden Anrufs zu identifizieren und diesen aufgrund der Kategorie, zu der er zugeordnet ist (zum Beispiel Stammkunde mit hoher Priorität), in eine bestimmte Position zu stellen.

Die Telefonanlage erhebt und speichert die äußeren Daten der Telekommunikationsvorgänge. Als derartige Informationen lassen sich exemplarisch

- Anschlussnummern der Gesprächspartner,
- Angaben zu den Wartezeiten der Anrufenden,
- Anzahl der Anrufe, die innerhalb der Wartezeit von Kunden beendet wurden,
- Zeitpunkt und Dauer der einzelnen Gespräche und
- Anzahl der durchgeführten Telefonate in einer bestimmten Zeitspanne

ins Feld führen.[232]

Die Telefondatenerfassung, die in der Telefonanlage automatisch abläuft, stellt grundsätzlich einen Umgang mit personenbezogenen Daten der Kunden – gleichwohl mit denen der Callcenter-Mitarbeiter – dar. Eine Identifizierungsmöglichkeit besteht regelmäßig anhand der Anschlussnummern.

Falls die genannten Datenverarbeitungsprozesse in der Telefonanlage nur zum technischen Vorgang des Vermittelns ein- und ausgehender Gespräche dienen, und ein

[232] *Kettlitz*, „Hier Amt, was beliebt?“, 2008, 55.

Auslesen der darin gespeicherten personenbezogenen und -beziehbaren Daten nicht möglich ist, kann sie ohne datenschutzrechtliche Einschränkungen betrieben werden. Die Speicherung von nur verkürzten Anschlussnummern im Hinblick auf Kunden machte eine eindeutige Identifizierbarkeit unmöglich.

Eine solche Zugriffsmöglichkeit auf die personenbezogenen Rahmendaten der Kommunikation und Auswertungsmöglichkeit derselben werden jedoch regelmäßig gegeben sein. Im Übrigen lässt sich eine Vielzahl dieser Informationen auch über das Frontend-System einsehen, da die Informationen eine wichtige Grundlage für das Kundenmanagement bilden. Entscheidend für die Zulässigkeit – analog zum Umgang mit personenbezogenen Kundendaten im Frontend-System – ist deren Erforderlichkeit für festgelegte Zwecke. In Bezug auf nichtöffentliche Callcenter-Betriebe können diese insbesondere im Zusammenhang mit einem Schuldverhältnis gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG, in der Wahrung berechtigter Interessen gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG und in der Werbung gemäß § 28 Abs. 3 BDSG bestehen.

Besitzen die äußeren Daten der Telekommunikation Relevanz für die Begründung, Durchführung oder Beendigung von Schuldverhältnissen mit Kunden, so ist deren Erhebung, Verarbeitung oder Nutzung für diese Zwecke grundsätzlich erlaubt. Werden zur Erbringung einer telefonischen Dienstleistung beispielsweise die Kommunikationsrahmendaten durch die Telefonanlage erhoben und in einem Datensatz, der über das Frontend-System abrufbar ist oder in diesem abgelegt wird, gespeichert, ist dies unter Einhaltung des Erforderlichkeitsgrundsatzes zulässig. Eine solche Situation kann vorliegen, wenn eine detaillierte Anrufhistorie der Kunden zur Erfüllung der Serviceleistung durch das Callcenter benötigt wird.

Der Umgang mit den Kommunikationsdaten in der Telefonanlage, und gegebenenfalls deren Übertragung in das Frontend-System, wird sich jedoch in der Regel auf Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig vollziehen lassen. Es existieren zahlreiche berechtigte Interessen des Callcenter-Betreibers, die als erforderlich qualifiziert werden können. Zu nennen sind etwa

- Erstellung kundenindividueller Statistiken,
- Bildung einer Datengrundlage zur Skalierung des Gesprächsmanagement-Systems,
- Bildung einer Datenbasis zur Personaleinsatzplanung im Callcenter-Betrieb und
- Protokollierung zur potenziellen Aufdeckung von Fehlern.

In den Fällen, in denen die Bildung der Datengrundlage auch mit anonymen Daten möglich ist, sollte diese datenschutzfördernde Alternative genutzt werden. Bei den drei letztgenannten Datenarten ist dies grundsätzlich denkbar.

Offensichtlich überwiegende schutzwürdige Interessen der Kunden sind im Hinblick auf die genannten Zweckbestimmungen nicht erkennbar. Der Umgang mit den Kommunikationsrahmendaten ist dazu mithin grundsätzlich erlaubt.

Ausnahmen stellen jedoch zum Beispiel die telefonische Suchtberatung, die Beratung von Schwangeren, Familien und Kindern sowie die Telefonseelsorge dar, bei denen Kunden regelmäßig davon ausgehen werden, dass deren Inanspruchnahme anonym erfolgt. Selbst wenn dabei keine personenbezogenen Daten der Kunden im Frontend-System gespeichert würden, darf ein Umgang mit solchen Daten, wie den ungekürzten Telefonnummern der Kunden, in der Telefonanlage nicht erfolgen. Die Anonymität könnte nicht gewahrt werden, da Rückschlüsse auf die Anschlussinhaber gezogen werden könnten. Technische Vorkehrungen müssen daher sicherstellen, dass die gesamte Dienstleistung derart genutzt werden kann, dass keine Rückschlüsse auf betroffene Kunden möglich sind. In diesem Beispiel überwiegen ohne jeden Zweifel die schutzwürdigen Interessen der Kunden am Ausschluss des Umgangs mit ihren personenbezogenen Daten.

Darüber hinaus existiert die Rechtfertigungsgrundlage aus § 28 Abs. 3 BDSG im Hinblick auf Werbemaßnahmen: Ausschließlich unter der Voraussetzung, dass keine weitergehenden Daten als die, die dem Callcenter bereits aufgrund eines Schuldverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG bekannt sind, zur Ansteuerung der Telefonanlage verarbeitet und genutzt werden, ist ihre Nutzung zu Werbezwecken ohne diesbezügliche Einwilligung erlaubt. Durch Maßnahmen des Systemdatenschutzes muss sichergestellt sein, dass die Erhebung weiterer personenbezogener Daten in der Anlage unterbunden wird, da die Nutzungs- und Verarbeitungserlaubnis aus § 28 Abs. 3 Satz 2 Nr. 1 BDSG keine Rechtfertigung für die Datenerhebung darstellt.

Die Nutzung der Telefonanlage bei der Durchführung von Werbemaßnahmen ist auf Grundlage der übrigen gesetzlichen Erlaubnistatbestände nur insoweit zulässig, wie keine weiteren als lediglich die Listendaten tangiert werden. So muss etwa durch die Speicherung der verkürzten Telefonnummer von anrufenden Kunden sichergestellt sein, dass hinsichtlich des Verbindungsaufbaus keine personenbezogene Datenerhebung stattfindet.

Für Callcenter-Betriebe von Bundes- oder Landeseinrichtungen ist die Zulässigkeit des Umgangs mit personenbezogenen Daten der Kommunikationsverbindungen primär anhand bereichsspezifischer Bestimmungen festzustellen. Die §§ 13 - 14 BDSG oder deren landesrechtliche Entsprechungen gilt es zu beachten, sofern keine bereichsspezifischen Regelungen bestehen.

Wenn der Datenumgang mit den äußeren Umständen der Kundenkommunikation für öffentliche Callcenter dafür erforderlich ist, dass sie ihre gesetzlich zugewiesenen Aufgaben erfüllen können oder sie zu höherer Bürgerfreundlichkeit beitragen, wird er als zulässig einzustufen sein. Etwa im Rahmen von Verwaltungsprozessen besteht oftmals die Notwendigkeit zu wissen, zu welchen Zeitpunkten Kontakt mit Kunden bestanden hat. Die Feststellung solcher Daten lässt sich mittels Telefonanlage durchführen.

3.1.1.4.3 Sprach- und Emotionserkennung

Eine bedeutende Funktion des Gesprächsmanagement-Systems stellt die Spracherkennung dar, welche eine automatisierte Datenerhebung in Bezug auf die Gesprächsinhalte realisiert. Dabei werden sowohl die auf dem Kunden- als auch dem Agentenkanal gesprochenen Wörter der weitergehenden Datenverarbeitung zugänglich gemacht. Erkannte Wörter und Phrasen führen zur Auslösung von Suchvorgängen in den innerhalb des Gesprächsmanagement-Systems integrierten und freigegebenen Informationsquellen.

Zur Erschließung wenig strukturierter und unstrukturierter Dateien in den angeschlossenen Datenbanken kommen Methoden des Text-Minings zum Einsatz. Da sich Textdateien in natürlicher Sprache nicht zur automatisierten Bearbeitung durch Computer eignen, ist eine Technik erforderlich, die deren Analyse und eine Wissensextraktion erlaubt; diese besteht im Text-Mining. Mit Hilfe des Text-Minings lassen sich neue, zuvor unbekannte Informationen aus Textdateien erschließen.[233]

Um den Callcenter-Agenten während ihrer Beratungsgespräche in Echtzeit gesprächsrelevante Informationen zur Verfügung stellen zu können, werden Methoden des Information Retrieval eingesetzt. Der Zeichenkettenvergleich (sogenanntes Keyword-Matching) ist eine diesbezügliche Technik, bei der ein Vergleich erkannter Schlüsselwörter mit den in den Dokumenten enthaltenen Termen stattfindet. Das Gesprächsmanagement-System soll ein darüber hinausgehendes Information Ret-

[233] *Siegmund*, in: Witte/Mülle (Hrsg.), Text Mining, 2006, 41 (42 f.).

rieval bieten, das die Semantik mit einschließt.[234] Anhand der semantischen Analyse des Gesprächsverlaufs kann das Gesprächsmanagement-System im Idealfall den Gesprächsgegenstand erkennen und damit die Suche nach maßgeblichen Informationen signifikant verbessern.

Vor dem Einsatz des Gesprächsmanagement-Systems im jeweiligen Anwendungsszenario ist es notwendig, der Spracherkennung im Vorfeld das domänenspezifische Vokabular „beizubringen“. Je anwendungsbezogener der Wortschatz ist, desto präzisere Ergebnisse lassen sich erzielen.

Nachfolgende Abbildung veranschaulicht beispielhaft Ergebnisse der Worterkennung:

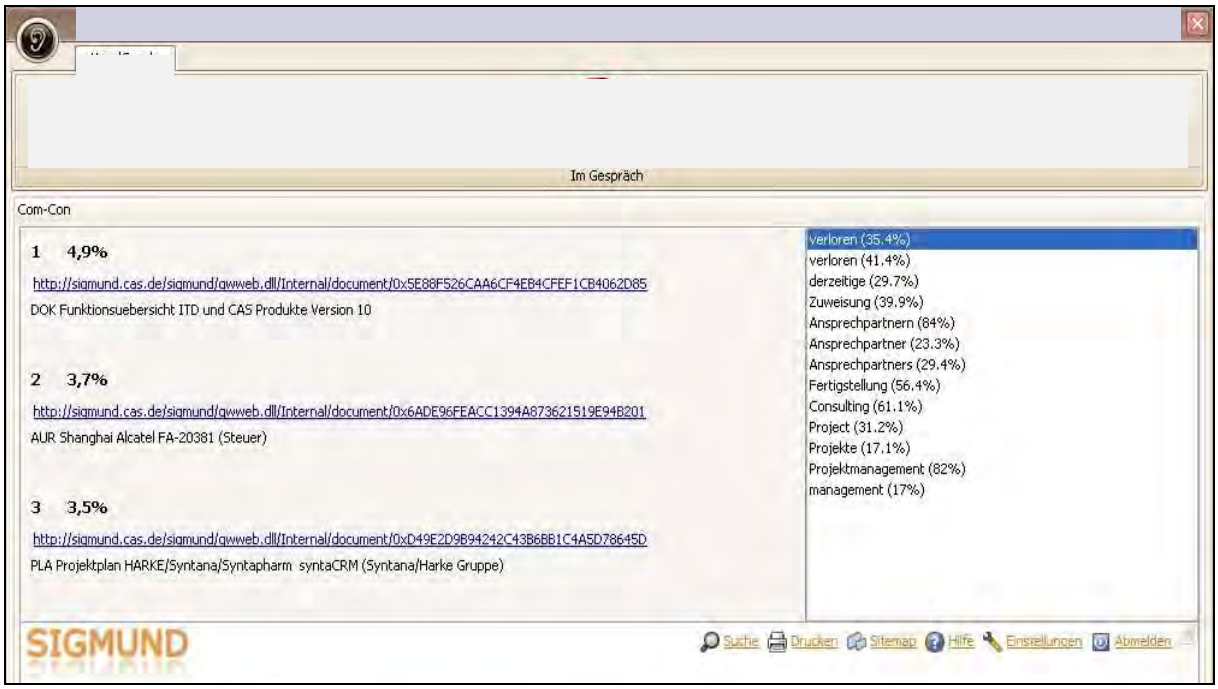

Abb. 3: Spracherkennung.
Quelle: itCampus Software- und Systemhaus GmbH.

Auf der linken Seite des abgebildeten Bildschirmausschnitts ist eine Liste der zurückgelieferten Suchergebnisse in Form von Web-Links mit den zugehörigen Relevanzwerten dargestellt. Je höher dieser Wert, desto wahrscheinlicher ist es, dass der angegebene Link zu den gefragten Informationen führt und damit zur Problemlösung beiträgt. Rechts im Bildschirmausschnitt werden die vom Spracherkennungsmodul erkannten Wörter angezeigt, die einen Suchprozess auslösen.

[234] *o. V.*, Vorhabensbeschreibung des Forschungsprojekts SIGMUND, 2008, 7.

Es erfolgt keine kundenspezifische Speicherung der Ergebnisliste oder deren Zuordnung zum Kundenprofil in der Kundendatenbank. Zur Optimierung des Suchprozesses im Gesprächsmanagement-System können jedoch Web-Links aus der Ergebnisliste – beispielsweise diejenigen, die unmittelbar zur Problemlösung führten – als solche gekennzeichnet gespeichert werden.

Neben der Spracherkennung, die das zentrale Element des Gesprächsmanagement-Systems ausmacht, existiert eine Funktion, mit der sich im weitesten Sinne die Emotionalität des aktuellen Gesprächs ablesen lässt. Der von der Verhaltenserkennungsfunktion ermittelte Wert, auch als „Stress-Level“ bezeichnet, kann sich grundsätzlich aus mehreren sogenannten Gesprächsqualitätsfaktoren zusammensetzen. So vermag er beispielsweise die Kriterien Gesprächsorientierung, Stimmklang, Sprechgeschwindigkeit, Pausenverhalten und Sprechspannung zu berücksichtigen.

Ein solcher Indikator zur Anzeige der Emotionalität könnte etwa folgendermaßen aussehen:

Abb. 4: Stress-Level-Indikator.
Quelle: Der Verfasser.

Je weiter sich der Anzeigepfeil im roten – und damit negativen – Bereich befindet, desto angespannter ist die Atmosphäre im laufenden Gespräch.

Erweitern lässt sich die emotionsinduzierte Rückmeldefunktion etwa dahingehend, dass den Mitarbeitern bei erkannten Extremsituationen ein situationsadäquater Gesprächsleitfaden am Frontend-System präsentiert wird, der ihnen eine angemessene Reaktionsweise vorschlägt. Wenn das Gesprächsmanagement-System etwa ein Gespräch als Streitgespräch qualifiziert, könnte es dem Callcenter-Mitarbeiter verschiedene Deeskalationsstrategien zur Verfügung stellen.

Die datenschutzrechtliche Zulässigkeit der Sprach- und der Emotionserkennung in Bezug auf nichtöffentliche Callcenter lässt sich anhand des § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 sowie Abs. 3 BDSG beurteilen. Beide Funktionen dienen der Unterstützung der Callcenter-Agenten im Gespräch und damit mindestens mittelbar der Be-

gründung, Durchführung oder Beendigung eines Schuldverhältnisses, falls ein solches gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG vorliegt.

Die von der Spracherkennungskomponente ausgelöste Suche hat den Zweck, die Mitarbeiter im Callcenter im passenden Moment mit relevantem Wissen zu versorgen. Sie erhalten damit die effiziente Möglichkeit, Anliegen der Kunden, zum Beispiel technische Problemlösungen, kompetent zu erledigen. Ohne diese zentrale Funktion des Gesprächsmanagement-Systems wäre es in vielen Fällen gar nicht möglich, auf ad hoc im Callcenter eingehende Fragestellungen der Kunden zu reagieren. Der Vorzug des Gesprächsmanagement-Systems besteht insbesondere in der automatisierten Erschließung unstrukturierten Wissens und zeitnaher Präsentation der Suchergebnisse. Andernfalls müssten relativ aufwändig manuelle Suchvorgänge in den zur Verfügung stehenden Datenbanken und in weiteren Wissensquellen durch die Callcenter-Mitarbeiter selbst betrieben werden. Eine Lösungsfindung während der laufenden Gespräche mit Kunden wäre im Normalfall überhaupt nicht möglich; insofern ist die Erforderlichkeit im Hinblick auf die Spracherkennung gegeben.

Die Funktion Emotionserkennung dient weniger der Optimierung der inhaltlichen Komponente der Telefonkommunikation als vielmehr derjenigen der Beziehungskomponente. Mit ihrer Hilfe soll eine angenehme und entspannte Gesprächsatmosphäre hergestellt und aufrechterhalten werden. Darüber hinaus kommt die Anzeige situationsadäquater Gesprächsleitfäden in Betracht. Zwar wird im Normalfall jeder ausgebildete Callcenter-Mitarbeiter selbst einschätzen können, wann sich ein Streit im Gespräch anzubahnen droht, dennoch kann die automatisierte Rückmeldung gerade dann eine große Hilfe darstellen, wenn keine Extremsituation vorliegt. Der Callcenter-Mitarbeiter hat ständig im Blick, welche emotionale Tendenz das Telefongespräch annimmt und kann darauf entsprechend reagieren. Dies gilt umso mehr, wenn die emotionsinduzierte Rückmeldung zur Präsentation situationsgerechter Gesprächsleitfäden am Frontend-System führt. Auch die Systemfunktion Emotionserkennung ist für die Erfüllung der genannten Zwecke erforderlich.

Falls kein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis zwischen dem Callcenter und (potenziellen) Kunden gegeben ist, kann der Einsatz der Sprach- und der Emotionserkennung aufgrund berechtigter Interessen des Callcenters gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein. Dabei darf – einschränkend – kein Grund zur Annahme vorliegen, dass schutzwürdige Interessen der Gesprächspartner überwiegen. Berechtigte Interessen aufseiten des Callcenters liegen zahlreich vor. Exemplarisch lassen sich die Verbesserung der Kundenorientierung

und die signifikante Erhöhung der Problemlösungsquote benennen. Dem stehen die schutzwürdigen Interessen der Gesprächspartner gegenüber, die insbesondere im Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG bestehen. Zwar werden die Gesprächsinhalte der Telefonate von den beiden Systemkomponenten erhoben und das Gespräch – zumindest phasenweise – automatisiert bewertet, dennoch ist das schutzwürdige Interesse der Gesprächspartner nicht überwiegend: Es gilt zu berücksichtigen, dass eine Speicherung erkannter Schlüsselwörter, ausgelöster Suchvorgänge, gefundener Suchergebnisse und der Ergebnisse der Verhaltenserkennung nicht erfolgt. Diese Daten stehen lediglich den Callcenter-Mitarbeitern für die jeweils stattfindenden Gespräche zur Verfügung. Insoweit ist der persönlichkeitsrechtliche Eingriff beider Funktionen – der Sprach- und der Emotionserkennung – auf ein Minimum reduziert.

Was die gesetzlichen Rechtfertigungsgrundlagen aus § 28 Abs. 3 BDSG zur Durchführung von Werbekampagnen anbelangt, so können diese die Verwendung der beiden Systemkomponenten Sprach- und Emotionserkennung im Normalfall nicht rechtfertigen. Die Vorschrift enthält keine Befugnis zur Erhebung von personenbezogenen Daten zu Zwecken der Werbung. Selbst die Erlaubnis aus § 28 Abs. 3 Satz 3 BDSG, auch weitere Daten zu den Listendaten hinzuspeichern zu dürfen, stellt keine eigene Erhebungsbefugnis dar.[235] Da beide Funktionen grundsätzlich in großem Umfang personenbezogene Daten erheben, darf deren Einsatz für Werbezwecke ohne entsprechende Einwilligung nicht erfolgen.

Eine Ausnahmesituation ist allerdings denkbar: Diese kann vorliegen, wenn die anrufenden (potenziellen) Kunden dem Callcenter gegenüber vollkommen anonym sind. Die im Gesprächsmanagement-System zur Anwendung gelangende Emotionserkennung kann zwar die Information verarbeiten, dass zum Beispiel gewisse „Werte“ im Stimmklang mit bestimmten Emotionen korrelieren. Dennoch sind derartige Informationen nicht per se personenbezogen, da in dem genannten Ausnahmefall kein Bezug zu einer konkreten Person gegeben ist.[236]

Callcenter der öffentlichen Verwaltung müssen sich demgegenüber an strengere Maßstäbe halten. § 13 Abs. 1 BDSG regelt die Zulässigkeitsvoraussetzungen für die Datenerhebung. Nur was grundsätzlich zwingend zur Erfüllung der gesetzlich zugewiesenen Aufgaben der Stelle notwendig ist, kann bei öffentlichen Stellen als erforderlich gelten. Diesbezüglich ist eine enge Auslegung des Rechtsbegriffs „Erforderlichkeit“ geboten.

[235] BT-Drs. 16/12011, 28.
[236] *Zoebisch*, DuD 2011, 394 (395).

Die Spracherkennung, als zentrale Funktion des Gesprächsmanagement-Systems, ermöglicht eine zeitgerechte Suche nach Problemlösungen. Sie gilt bei komplexen Fragestellungen als wesentliche Hilfestellung für die Arbeit der Callcenter-Agenten. Fraglich ist, inwieweit diese Systemkomponente tatsächlich benötigt wird, damit die verantwortliche Stelle ihrer Aufgabe nachkommen kann. Besteht die Aufgabe eines Callcenters der öffentlichen Verwaltung zum Beispiel lediglich in der Auskunft über Öffnungszeiten und Zuständigkeiten der Stelle, so ist die Funktion für diese nicht notwendig. Insoweit kann nicht konstatiert werden, dass diese Funktion generell für die Aufgabenerfüllung der öffentlichen Stelle als unabdingbar gilt: Die Beurteilung, ob die Erforderlichkeit der Spracherkennung im Hinblick auf die Zuständigkeit der öffentlichen Stelle gegeben ist, muss einzelfallabhängig erfolgen. Notwendigkeit kann insbesondere dann gegeben sein, wenn komplexe Fragestellungen unter Zeitdruck erkannt oder schwierige Auskünfte erteilt werden müssen.

Eindeutiger ist die Frage zu beantworten, ob die Emotionserkennung zur Aufgabenerfüllung der öffentlichen Stelle erforderlich ist: Die unbedingte Notwendigkeit hierzu besteht nicht. Auch ohne die Kenntnis der jeweils vorliegenden Emotionalität der Telefongespräche wird das Callcenter der öffentlichen Verwaltung seiner gesetzlichen Verantwortung nachkommen können, obgleich der Einsatz der Emotionserkennung zur Verbesserung der Serviceorientierung führte.

Für den Fall, dass sich der Einsatz der Spracherkennungskomponente in öffentlichen Callcenter-Betrieben nicht durch gesetzliche Erlaubnistatbestände rechtfertigen lässt, kann auf eine Einwilligung der Kunden zurückgegriffen werden; auch im Hinblick auf die Emotionserkennung vermag eine Einwilligung als Rechtfertigungsgrund zu dienen. Zwar können sich öffentliche Stellen selbst mit dem Einverständnis der Kunden grundsätzlich keine weitergehenden Datenverarbeitungsbefugnisse erteilen lassen als ihnen bereits aufgrund ihrer gesetzlich zugewiesenen Aufgaben zustehen. In diesem Fall geht es jedoch nicht um eine Ausweitung von Datenverarbeitungsbefugnissen, die eine Kompetenzüberschreitung der öffentlichen Stelle bedeuteten, sondern um die Erlaubnis, mit Daten umgehen zu dürfen, die im unmittelbaren Zusammenhang mit ihrer Aufgabenerfüllung stehen und diese im Normalfall wesentlich erleichtern. Die Datenerhebung durch die Sprach- und Emotionserkennung sowie die Verarbeitung dieser Informationen können mit dem Einverständnis der Kunden grundsätzlich zulässig durchgeführt werden.

3.1.1.4.4 CRM-System: Kundendatenbank und Archivdatenbank

Das Customer Relationship Management (CRM) versteht sich als ganzheitlicher Ansatz zur Unternehmensführung, der sämtliche kundenbezogenen Prozesse in den Bereichen Forschung und Entwicklung, Beschaffung, Produktion, Marketing sowie Vertrieb integriert. Vorrangiges Ziel ist der Aufbau und die Erhaltung nachhaltiger Geschäftsbeziehungen mit Kunden.[237] Die Einsatzmöglichkeiten von CRM sind jedoch nicht auf das produzierende Gewerbe beschränkt, sondern erstrecken sich ebenso auf den Dienstleistungssektor und grundsätzlich auch auf den Bereich der öffentlichen Verwaltung.[238]

Ganz allgemein dienen CRM-Systeme der systematischen Sammlung von Kundendaten, um diese miteinander zu verknüpfen und auszuwerten.[239] Die Intention des Betriebs eines CRM-Systems besteht in der Fokussierung sämtlicher Abläufe auf Kunden.[240]

Die Kundendatenbank[241], die den bedeutendsten Bestandteil des CRM-Systems im Gesprächsmanagement-System darstellt, sowie die Archivdatenbank realisieren das Konzept des Data-Warehouse.[242] Darunter ist allgemein die Speicherung kundenbezogener Informationen in einer zentralen Datenbank zu verstehen, welche es ermöglicht, die Daten jederzeit verfügbar und nach Belieben und für unterschiedlichste Zwecke abrufbar zu halten; dieses Prinzip verwirklicht ein Lagerhaus für digitale Daten.[243] Eine Beschreibung der im Data-Warehouse enthaltenen Daten erfolgt mittels Metadaten, die gewissermaßen eine Art Inhaltsverzeichnis bilden und zur Steuerung des gesamten informationstechnischen Ablaufs dienen.[244]

---

[237] *Volle*, Datenschutz als Drittwirkungsproblem, 2007, 13; *Taeger*, K&R 2003, 220; *Boehme-Neßler*, K&R 2002, 217 (218).
[238] Zur Diskussion der Notwendigkeit von CRM in öffentlichen Verwaltungen *Bauer/Grether*, in: Hippner/Wilde (Hrsg.), Management von CRM-Projekten, 2004, 347 ff.; *Schmitt*, CRM-Systeme in der öffentlichen Verwaltung, 2003, 51 ff.
[239] *von Lewinski*, RDV 2003, 122 (123).
[240] *Volle*, Datenschutz als Drittwirkungsproblem, 2007, 14.
[241] Zu den datenschutzrechtlichen Aspekten des internationalen Kundendatentransfers ausführlich *Scheja*, Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank, 2006.
[242] In der Literatur, so beispielsweise bei *Schulz/Waldenspuhl/Hermerschmidt*, Data Warehouse und Data Mining im öffentlichen Bereich, 2002, 4 (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf), wird häufig eine Trennung zwischen einem operativen Datenbanksystem und einem strategischen Data-Warehouse-System, welches die Daten langfristig für Auswertungszwecke vorhält, vollzogen. Diese technische Separierung ist im Rahmen der vorliegenden Betrachtung irrelevant, da die langfristige Speicherung von Kundendaten innerhalb des CRM-Systems das Konzept des Data-Warehousings verwirklicht.
[243] *Möller*, DuD 1998, 555 (556); *Baeriswyl*, RDV 2000, 6.
[244] *Frosch-Wilke*, DuD 2003, 597.

Die Auswertung der vorhandenen Datenbasis kann anhand von vordefinierten Abfragen oder von Methoden des Data-Minings erfolgen. Letztere erlauben es, große Datenbestände automatisiert mittels Algorithmen auf Zusammenhänge hin zu analysieren. Dabei sollen ohne Anwendung von Data-Mining nicht zu erkennende Korrelationen aufgedeckt und somit neue Wissenszusammenhänge erschlossen werden.[245] Unterscheiden lassen sich beispielsweise die Klassifikation und Segmentierung von Daten sowie die Bildung von Assoziationen.[246]

Durch die konsequente Speicherung und Auswertung der vorliegenden Kundendaten können Kundenprofile erstellt werden. Damit ist es möglich, aus einer Masse von wenig aussagekräftigen Informationen präzise Aussagen über das Kundenverhalten abzuleiten. Über die Zusammenführung kundenbezogener Einzelinformationen hinaus lassen sich weitergehende Informationen gewinnen, mit denen das Kundenprofil fortwährend vervollständigt werden kann. Somit sind letztendlich Prognosen über das zukünftige Verhalten der Kunden erstellbar.[247]

Zusätzlich zu den zum Beispiel im Rahmen einer Verkaufsabwicklung notwendigen Daten können auch sensitive Daten hinzugespeichert werden, sodass sich ein noch präziseres Profil der Kunden ergibt. Derartige Profile können zu einer massiven Verletzung des informationellen Selbstbestimmungsrechts führen, wenn die Informationen die individuelle Persönlichkeitsstruktur abbilden.[248] So ist es denkbar, dass sich persönliche Präferenzen, Bedürfnisse sowie Kauf- und Zahlungsverhalten von Kunden direkt ablesen lassen.[249] Bereits im Jahre 1969 hat das *BVerfG* in seinem Beschluss zur Verfassungsmäßigkeit des Mikrozensus festgestellt, dass es mit der Menschenwürde nicht zu vereinbaren sei, „...wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist“.[250]

[245] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 28 f.; *Hahn*, DuD 2003, 605 (607); *Jürgens*, DSB 4/2000, 8.
[246] *Büllesbach*, CR 2000, 11 (12); *Frosch-Wilke*, DuD 2003, 597 (602); zu den verschiedenen Methoden und Algorithmen des Data Mining ausführlich etwa *Runkler*, Data Mining, 2010.
[247] *Hladjk*, Online-Profiling und Datenschutz, 2007, 37; *Bull*, NJW 2006, 1617 (1620); *Bizer et al.*, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, 2006, 31; zur Profilbildung im Internet *Weber*, DuD 2003, 625 ff.
[248] *Bizer et al.*, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, 2006, 31; zur Zulässigkeit des Zukaufs branchenspezifischer Fachdatenbanken mit Personenbezug *Moos*, MMR 2006, 718 ff.
[249] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 35.
[250] *BVerfG* v. 16.7.1969, NJW 1969, 1707.

Öffentliche Stellen dürfen keine umfassenden Persönlichkeitsprofile der Bürger erstellen. Privatwirtschaftliche Unternehmen können hierzu bis zu einem gewissen Grad auf die Einwilligung ihrer Kunden zurückgreifen.[251] Allgemein lässt sich festhalten, dass solange kein gesetzliches Verbot die Profilerstellung untersagt, grundsätzlich darin eingewilligt werden kann.[252]

3.1.1.4.4.1 Besondere Problematik des Data-Warehousings und Data-Minings

Aus der Fähigkeit des Callcenters, die Interaktion mit Kunden individuell zu gestalten, kann der entscheidende Wettbewerbsvorteil resultieren. Wenn es gelingt, die richtigen Kunden zum richtigen Zeitpunkt mit den richtigen Werbemaßnahmen anzusprechen, vermag dies die eigene Marktposition zu sichern und auszubauen. Das optimale Resultat der Data-Mining-Methoden besteht darin, Kunden mit dem maßgeschneiderten Angebot zu begegnen.[253]

Eine grundlegende datenschutzrechtliche Forderung, die in der Zweckbindung der erhobenen Daten besteht, gilt im Zusammenhang mit dem Aufbau und der Nutzung einer Kundendatenbank als bedroht: Die in einem Data-Warehouse-System gespeicherten Daten können auf Vorrat und für unbestimmte Zwecke aufgenommen werden. Das *BVerfG* hat in dem für das Datenschutzrecht wegweisenden Volkszählungsurteil[254] festgestellt, dass die Sammlung personenbezogener Daten auf Vorrat, zu unbestimmten oder noch nicht bestimmbaren Zwecken, nicht mit dem Recht auf informationelle Selbstbestimmung zu vereinbaren sei.[255] Daraus folgt die Unzulässigkeit, Datendepots aufzubauen, um diese mit erst später festzulegenden Zwecken auszuwerten.[256]

Die Zielrichtung des Data-Warehousings besteht oftmals darin, operative Daten zweckneutral zu speichern, um anschließend – auch nach Jahren der Speicherung – mittels Data-Mining-Methoden neue Muster, Strukturen und Zusammenhänge aufzudecken sowie Trends vorherzusagen. Grundlage für solche Auswertungsvorgänge

[251] *Schaar*, DuD 2001, 383.
[252] *Schaar*, DuD 2001, 383 (385); *Hladjk*, Online-Profiling und Datenschutz, 2007, 123.
[253] *Link/Gary*, Grundlagen und rechtliche Aspekte von Kundendatenbanken (abrufbar unter: http://www.marketing-boerse.de/fachartikel/details/grundlagen-und-rechtliche-aspekte-von-kundendatenbanken/14366); *Jacob/Jost*, DuD 2003, 621; *Wittig*, RDV 2000, 59.
[254] *BVerfG* v. 15.12.1983, NJW 1984, 419 ff.
[255] *BVerfG* v. 15.12.1983, NJW 1984, 419 (422), *Petri/Kieper*, DuD 2003, 609; *Roßnagel*, MMR 2003, 693 f.
[256] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 73; *Roßnagel*, NZV 2006, 281 (285).

bilden bekannte Verhaltensschemata der Kunden aus der Vergangenheit.[257] Methoden des Data-Minings ermöglichen es, Analysen des Datenbestands durchzuführen – die meist zweckungebunden erfolgen. Zum Zeitpunkt der Datenerhebung stehen oftmals weder die Zwecke der Speicherung noch der Auswertung der personenbezogenen Daten fest.[258] Datenschutzrechtlich unproblematisch sind hingegen die Speicherung und Auswertung lediglich anonymer Daten, die keine personenbezogene Profilbildung erlauben.

Insbesondere zwei Aspekte im Zusammenhang mit dem Aufbau und Betrieb eines Data-Warehouse und der automatisierten Auswertung des Datenpools mittels Data-Mining-Methoden stellen die Objektivität der gewonnenen Ergebnisse in Frage und somit eine Bedrohung für das informationelle Selbstbestimmungsrecht der betroffenen Kunden dar; namentlich sind dies Kontextverlust und Scheinobjektivität.

Der Kontextverlust entsteht durch die verkürzte, formalisierte Speicherung von aus ihrem Zusammenhang gelöster konkreter Sachverhalte und kann zu falschen Annahmen führen, auf deren Grundlage sich die anschließende Datenauswertung vollzieht.[259] Die Problematik des Kontextverlusts verschärft sich mit fortwährender Aufbewahrung der Daten. Im Zeitverlauf verlieren die Daten in der Regel zunehmend an Aussagekraft im Hinblick auf die Vorhersage zukünftigen Verhaltens.

Eine weitere, damit eng verbundene Schwierigkeit ergibt sich aus der vermeintlichen Objektivität von Computern. Im Allgemeinen besteht eine Richtigkeitsvermutung für automatisiert verarbeitete Daten, weil diese Daten im Verarbeitungsprozess keinen subjektiven Beeinträchtigungen unterliegen.[260] Erfolgt durch eine fehlerhafte Datenauswertung eine falsche Zuordnung von Kunden zu einer bestimmten Kategorie, etwa zu einer der säumigen Schuldner, kann dies geradezu eine Stigmatisierung der betroffenen Personen verursachen.

Als problematisch erweist sich für Betroffene darüber hinaus die Tatsache, dass im Rahmen des Data-Warehousings und Data-Minings die über sie gespeicherten Da-

[257] *Büllesbach*, CR 2000, 11 (12); *Grosskreutz/Lemmen/Rüping*, Informatik Spektrum 2010, 380; *Petri/Kieper*, DuD 2003, 609; *Schumann*, DuD 2010, 709; *Gola/Reif*, in: *Gesellschaft für Datenschutz und Datensicherheit e. V./Zentralverband der deutschen Werbewirtschaft e. V.* (Hrsg.), Kundendatenschutz, 3. Aufl. 2011, Rn. 649; *Weichert*, RDV 2003, 113 (119); *Hahn*, DuD 2003, 605 (608).
[258] *Hladjk*, Online-Profiling und Datenschutz, 2007, 139 f.
[259] *Wittig*, RDV 2000, 59 (62); *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 2 Rn. 34; *Elschner*, Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2004, 18.
[260] *Koeppen*, Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz, 2007, 35 f.; *Elschner*, Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2004, 19 f.; *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 23.

ten derart vielseitig nutzbar sind, dass sie nicht mehr ansatzweise überschauen können, zu welchen Erkenntnissen sie führen.[261]

Die grundsätzlich verbotene Datenspeicherung auf Vorrat ist jedenfalls bei nichtöffentlichen Callcentern weniger bedenklich als bei solchen der öffentlichen Verwaltung. Öffentliche Stellen nehmen regelmäßig gesetzlich feststehende Aufgaben wahr, während sich privatwirtschaftliche Unternehmen an die Marktsituation anpassen müssen.[262]

An dem dargestellten Spannungsverhältnis zwischen dem datenschutzrechtlichen Zweckbindungsgrundsatz und der praktisch notwendigen zweckoffenen Erhebung, Speicherung oder Auswertung der personenbezogenen Daten von Kunden wird deutlich, dass sich die Auflösung dieses Konflikts keineswegs trivial gestaltet. Die Legitimation zur Aufnahme von „einfachen" Kundendaten, wie Name und Adresse, in ein Data-Warehouse ist weniger kritisch als Angaben über finanzielle Verhältnisse oder sogar besonders schutzwürdige personenbezogene Daten gemäß § 3 Abs. 9 BDSG; an den Umgang mit Letzteren sind generell hohe Anforderungen gestellt.

Problematisch ist die Anhäufung von Daten und deren Verknüpfung, sodass vollkommen neue Daten entstehen, die höhere Sensitivität aufweisen können. So kann ein für sich genommen belangloses Datum durch Anreicherungen dazu führen, dass es eine höhere datenschutzrechtliche Relevanz erlangt.[263] § 3a BDSG enthält zwei zentrale Grundsätze des Datenschutzrechts, namentlich die der Datenvermeidung und der Datensparsamkeit.[264] In § 3a Satz 1 BDSG ist die Forderung enthalten, dass die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten möglichst datensparsam erfolgen soll. Darüber hinaus hat sich die Auswahl und Gestaltung der Datenverarbeitungssysteme an dem Ziel zu orientieren, dass diese möglichst wenig personenbezogene Daten benötigen. Es handelt sich also primär um eine Vorgabe zur datenschutzkonformen Technikgestaltung und stellt ein Element des Systemdatenschutzes dar.[265] Die Prinzipien der Datenvermeidung und der Datensparsamkeit sollen dem Vorsorgegedanken im Datenschutz Rechnung tragen.[266] Entstehen erst gar keine personenbezogenen Daten, so ist auch deren Missbrauch nicht möglich.[267]

[261] *Bull*, NJW 2006, 1617 (1621).
[262] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 29 Rn. 62.
[263] *Bull*, NJW 2006, 1617 (1618).
[264] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 62.
[265] *Roßnagel*, ZRP 1997, 26 (29); *Hladjk*, Online-Profiling und Datenschutz, 2007, 135 ff.; *Bull*, NJW 2006, 1617 (1619).
[266] *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation, Recht und öffentliche Kommunikation, 2011, 41 (44).
[267] *Roßnagel/Scholz*, MMR 2000, 721 f.

Auch hier wird der bestehende Konflikt zwischen den Zwecken des CRM-Systems und dem Datenschutzrecht evident.

Da Data-Warehousing und Data-Mining in der Regel Sekundärnutzungen der erhobenen personenbezogenen Daten darstellen, sind sie nur zulässig, wenn eine Vereinbarkeit mit den primären Erhebungszwecken noch gegeben ist. Der Primärzweck muss in diesem Fall derartige Verarbeitungsvorgänge mit einschließen.[268]

Fraglich ist, auf welcher Rechtsgrundlage sich Data-Warehousing und Data-Mining im Rahmen des Gesprächsmanagement-Systems legitimieren lassen. § 28 BDSG verkörpert in Bezug auf nichtöffentliche Callcenter die einschlägige Vorschrift, wenn die strategische Informationsgewinnung etwa zur Stärkung der Kundenbeziehung für das Callcenter selbst oder für die nichtöffentliche Stelle, die das Callcenter beauftragt hat, erfolgt.[269]

Der Datenumgang ist gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG erlaubt, wenn er für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem (potenziellen) Kunden erforderlich ist. Erfasst sind damit vertragliche und vorvertragliche Rechtsbeziehungen.[270] Zulässigkeit des Datenumgangs liegt also vor, soweit er dazu notwendig ist, das von den Vertragsparteien miteinander vereinbarte Ziel zu erreichen.[271] Dieses besteht beispielsweise bei einem Versandhandelsunternehmen und seinen Kunden darin, dass zum einen die bestellte Ware geliefert und zum anderen der Kaufpreis erstattet wird. Der Versandhändler darf zur Abwicklung des gesamten Bestellvorgangs mit sämtlichen dafür erforderlichen personenbezogenen Daten der Kunden, etwa mit ihrer Anschrift und gegebenenfalls mit ihrer Bankverbindung, umgehen. Die zum Zweck der Vertragsabwicklung gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhobenen und gespeicherten personenbezogenen Daten dürfen jedoch nicht zum Aufbau eines Data-Warehouse und zur Durchführung von Data-Mining verwendet werden, wenn dies nicht beispielsweise mittels Aggregierung der Daten anonymisiert oder zumindest pseudonymisiert geschieht.[272] Diese Prozesse sind für die Vertragserfüllung objektiv nicht erforderlich. § 28 Abs. 1 Satz 1 Nr. 1 BDSG kann nur dann als Rechtfertigungsgrundlage für den Aufbau eines Data-Warehouse und die Durchführung von Data-Mining mit personenbezogenen Daten dienen, wenn gerade

[268] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 75.
[269] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 82 ff.
[270] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 12 f.
[271] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 86; *Körffer*, DuD 2004, 267 (268).
[272] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 11.

dies der Gegenstand des Vertrags darstellt, oder der Vertragszweck ausdrücklich um diese Vorgänge erweitert wurde.[273] Eine langfristige Speicherung von Kundendaten auf Grundlage des § 28 Abs. 1 Satz 1 Nr. 1 BDSG kann im Rahmen von Dauerschuldverhältnissen erlaubt sein.[274]

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG lässt den Datenumgang zu, soweit er zur Wahrung berechtigter Interessen des Callcenters oder des Unternehmens, für welches das Callcenter agiert, erforderlich ist. Einschränkend dürfen aber schutzwürdige Interessen der Kunden am Ausschluss des Datenumgangs nicht überwiegen. Der Interessenkonflikt ist im Rahmen einer gegenseitigen Interessenabwägung unter Betrachtung des konkreten Verarbeitungsprozesses aufzulösen. Der Aufbau und Betrieb eines Data-Warehouse, dessen personenbezogener Datenbestand mittels Data-Mining-Methoden im Hinblick auf das Kundenverhalten analysiert werden soll, kann sich jedenfalls nicht auf die datenschutzrechtliche Erlaubnisnorm aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG stützen.[275] Die schutzwürdigen Interessen der Kunden überwiegen, da dieser Eingriff zu tiefgehend wäre.

§ 28 Abs. 3 Satz 3 BDSG erlaubt zum Zwecke der Werbung für eigene Angebote die Zuspeicherung von weiteren Daten zu den Listendaten über (potenzielle) Kunden, falls diese weitergehenden Daten zulässig im Rahmen der Begründung, Durchführung oder Beendigung eines Schuldverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben wurden. Die Vorschrift des § 28 Abs. 3 Satz 3 BDSG stellt jedoch keine eigene Befugnis zur Datenerhebung dar, sondern erlaubt dem Callcenter nur, einen bereits vorliegenden – und zulässig erhobenen und gespeicherten – Datenbestand für Zwecke der Eigenwerbung zu selektieren. Dies soll die gezielte Ansprache von (potenziellen) Kunden ermöglichen.[276] Die gegebenenfalls daraus gewonnenen Informationen dürfen vom Callcenter beispielsweise dazu genutzt werden, neben der Primäraufgabe Erledigung des Beschwerdemanagements, Bestandskunden auf weitere Produkte aufmerksam zu machen. Aufgrund existierender schutzwürdiger Interessen der (potenziellen) Kunden, die insbesondere in der Vermeidung eines vollumfänglichen Käuferprofils bestehen, legitimiert die Vorschrift allerdings keine unbegrenzte Speicherung personenbezogener Daten in einem Data-Warehouse und Anwendung extensiver Data-Mining-Methoden.

[273] *Büllesbach*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 7.1 Rn. 34; *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 87; *Petri/Kieper*, DuD 2003, 609 (611); *Möncke*, DuD 1998, 561 (566).
[274] *Büllesbach*, CR 2000, 11 (13).
[275] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 11; *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 90 ff.
[276] BT-Drs. 16/12011, 28.

Die anderen Erlaubnistatstände aus § 28 Abs. 3 BDSG gestatten es nicht, mehr Daten als ausschließlich die Listendaten aus § 28 Abs. 3 Satz 2 BDSG zu verarbeiten oder zu nutzen. Insofern kann auf Grundlage dieser wenigen Informationen kein Data-Warehouse und Data-Mining betrieben werden. Einzig die Ordnung der Listendaten nach bestimmten Kriterien ist aufgrund der gesetzlichen Rechtfertigung zulässig. So dürfen beispielsweise diejenigen Personen in einer Listenansicht zusammengestellt werden, die älter als 18 Jahre sind.

Die gesetzlichen Erlaubnistatbestände aus § 28 BDSG lassen tendenziell kein personenbezogenes Data-Warehousing und Data-Mining zu, sodass diese Vorgänge in vielen Fällen nur bei Vorliegen einer Einwilligung durch Kunden zulässig durchführbar sein werden.[277] Es ist stets einzelfallabhängig vor dem Hintergrund des jeweiligen Anwendungskontexts des Gesprächsmanagement-Systems sowie des potenziellen Ausmaßes der personenbezogenen Datenverarbeitungsvorgänge zu ermitteln, ob sich der Datenumgang im CRM-System noch durch gesetzliche Erlaubnistatbestände rechtfertigen lässt, oder ob eine diesbezügliche Einwilligung des Kunden notwendig ist.

Das Einverständnis des Kunden mit den Datenverarbeitungsprozessen kann nur dann als vollwertiges Substitut zu den gesetzlichen Erlaubnistatbeständen aus § 28 BDSG gewertet werden, wenn eine hinreichende Bestimmtheit vorliegt sowie eine rechtzeitige und umfassende Information über den vorgesehenen Datenumgang erfolgte.[278] Je multifunktionaler die angewandte Data-Mining-Methode ausgestaltet ist, und je mehr Zusammenhänge der einzelnen personenbezogenen Daten potenziell aufgedeckt werden können, desto höhere Anforderungen sind an eine wirksame Einwilligung durch Kunden zu stellen.[279] Jedenfalls ist eine „Vorratseinwilligung“, die im Grunde genommen pauschal den Datenumgang für unbestimmte Zwecke erlauben soll, unzulässig.[280] Eine datenschutzrechtliche Einwilligung, die sich auf die Speicherung personenbezogener Kundendaten im Data-Warehouse sowie auf die Auswertung dieses Datenbestands nach verschiedenen Kriterien bezieht, muss eine umfassende Darlegung sämtlicher relevanter Tatsachen enthalten.[281]

[277] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 116; *Gola/Reif*, in: *Gesellschaft für Datenschutz und Datensicherheit e. V./Zentralverband der deutschen Werbewirtschaft e. V.* (Hrsg.), Kundendatenschutz, 3. Aufl. 2011, Rn. 651.
[278] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 119.
[279] *Petri/Kieper*, DuD 2003, 609 (610); *Gola/Reif*, in: *Gesellschaft für Datenschutz und Datensicherheit e. V./ Zentralverband der deutschen Werbewirtschaft e. V.* (Hrsg.), Kundendatenschutz, 3. Aufl. 2011, Rn. 652; *Weichert*, DuD 2003, 161 (165).
[280] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 4a Rn. 29.
[281] *Podlech/Pfeifer*, RDV 1998, 139 (146).

Besteht für den vorgesehenen Datenumgang innerhalb des CRM-Systems die Notwendigkeit einer Einwilligung, ist Folgendes zu beachten: Die Zulässigkeit von personenbezogenem Data-Warehousing und Data-Mining hängt maßgeblich vom Grad der Präzisierung ihrer Zweckbestimmung ab. Vollkommen abhängig von der „Enge und Weite" der angegebenen Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten wird die Grenze zur rechtfertigungsbedürftigen Zweckänderung früher oder später erreicht.[282] So kann beispielsweise die sehr pauschale Formulierung „…zur Durchführung von Marketingzwecken…" in der Einwilligungserklärung nicht für umfangreiche Data-Warehouse- und Data-Mining-Prozesse ausreichen.[283] Ist etwa eine Klassifizierung der Kunden nach verschiedenen Merkmalen angestrebt, muss jeder Kunde im Rahmen der Einwilligung insbesondere wissen,

- auf Grundlage welcher Informationen dies geschieht,
- welche Kriterien zur Aufnahme der Daten herangezogen werden,
- welche Bewertungskriterien mit welcher Gewichtung relevant sind und
- welche Auswirkungen die Kategorisierung konkret haben kann.[284]

Den Kunden muss die Tragweite ihrer Einwilligung bewusst sein; dazu ist es unumgänglich, dass das Einwilligungsersuchen elementare Angaben zu den vorgesehenen Verarbeitungsschritten und Auswertungsmethoden im CRM-System enthält.[285]

Der Idealfall – aus datenschutzrechtlicher Sicht – besteht in einem vollkommen anonymen Data-Warehouse, bei dem überhaupt keine Rückschlüsse auf Personen möglich sind. Allgemein sollte bereits in der Planungsphase – vor dem Prozess der Implementierung – eines CRM-Systems im Unternehmen dahingehend eine Prüfung stattfinden, ob es unter Verzicht auf personenbezogene Daten betrieben werden kann. Dies wäre unter anderem denkbar, wenn keine Wiedererkennung der Personen notwendig ist, wenn lediglich statistische Informationen gewonnen werden sollen, oder wenn die Analyse von Gruppenverhalten im Fokus des Interesses steht.[286] Ein konkretes Beispiel hierzu stellt ein „Sorgentelefon" dar, bei dem Ratsu-

[282] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 76; *Hladjk*, Online-Profiling und Datenschutz, 2007, 140.
[283] *Jacob/Jost*, DuD 2003, 621 (622).
[284] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 123.
[285] *Petri/Kieper*, DuD 2003, 609 (610); *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 76.
[286] Mit grundsätzlich derselben Forderung *Büllesbach*, CR 2000, 11 (17); *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 140.

chende Unterstützung in einer schwierigen Lebenssituation suchen können.[287] Um einerseits die Anonymität der Anrufer zu wahren, andererseits die im Gespräch anfallenden Daten trotzdem einem Data-Warehouse und späteren Auswertungen durch Data-Mining zugänglich zu machen, könnte jeder Anruf eine fortlaufende Nummer im System erhalten, unter welcher die im Gespräch angefallenen Informationen abgespeichert werden.

Der Einsatz eines Data-Warehouse in der öffentlichen Verwaltung könnte ebenso wie bei Organisationen im nichtöffentlichen Bereich zu erheblichen Effizienzvorteilen führen. Es könnten beispielsweise sämtliche Verwaltungsvorgänge einem bestimmten Kunden oder einem bestimmten Bearbeiter zugeordnet gespeichert werden. Die zentralisierte Speicherung vermag zu einer einfachen und schnellen Auffindbarkeit relevanter Vorgänge beizutragen. Unter dem Stichwort „Verwaltungsmodernisierung“ gilt es als naheliegend, sämtliche Daten, die von unterschiedlichen Organisationseinheiten einer Behörde erhoben, verarbeitet und gespeichert wurden, in einem Data-Warehouse zusammenzufassen und sie mit Methoden des Data-Minings auf Effektivierungspotenziale hin zu untersuchen.[288]

Die Erhebung personenbezogener Daten durch öffentliche Stellen ist gemäß § 13 Abs. 1 BDSG zulässig, wenn diese Daten für ihre Aufgabenerfüllung erforderlich sind. Im Hinblick auf den Betrieb eines Data-Warehouse bedeutet dies, dass gerade dieser zum Aufgabengebiet der öffentlichen Stelle zu zählen hat. Zumindest jedoch muss das Data-Warehouse zur Erfüllung einer der Organisation zugewiesenen Aufgabe erforderlich sein. Es existieren keine gesetzlichen Regelungen, die den Betrieb von Data-Warehouse-Systemen für öffentliche Einrichtungen vorschreiben. Nützlich können die potenziell zu speichernden Daten zwar durchaus sein, das Kriterium der Erforderlichkeit der Speicherung ist – abgesehen von unter Umständen bestehenden besonderen bereichsspezifischen Erlaubnistatbeständen – nicht erfüllt.[289]

Im Zusammenhang mit öffentlichen Stellen ist der Rechtsbegriff der Erforderlichkeit eng auszulegen: Generell sind öffentlichen Einrichtungen nur insoweit Daten zuzubilligen, wie es zur gesetzlich festgelegten Aufgabenwahrnehmung notwendig ist.[290] Die Daten müssen zur Aufgabenerfüllung „conditio sine qua non“ sein, das

[287] Derartige Statistiken sind beispielsweise abrufbar unter: http://www.elterntelefon.org/de/Nummer-gegen-Kummer/Presse/Zahlen-und-Fakten__381/.
[288] *Schulz/Waldenspuhl/Hermerschmidt*, Data Warehouse und Data Mining im öffentlichen Bereich, 2002, 4 ff. (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf).
[289] *Schulz/Waldenspuhl/Hermerschmidt*, Data Warehouse und Data Mining im öffentlichen Bereich, 2002, 10 (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf).
[290] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 13 Rn. 15.

heißt alleinig ihre Geeignetheit und Zweckmäßigkeit reichen dafür keinesfalls aus.[291]

Aus dem dargestellten Erforderlichkeitsgrundsatz resultiert das Verbot der Vorratsdatenhaltung für potenzielle zukünftige Aufgaben: Wenn zum Zeitpunkt der Datenerhebung ungewiss ist, ob überhaupt solche Aufgaben entstehen werden, zu deren Erfüllung die in Rede stehenden Daten notwendig sind, dann können die Daten nicht erforderlich sein.[292] Im Ergebnis lässt sich eine Datenerhebung zum Aufbau und Betrieb eines Data-Warehouse, in welchem die Daten langfristig gespeichert und ausgewertet werden sollen, nicht durch allgemeines Datenschutzrecht legitimieren.

§ 14 BDSG regelt die Datenspeicherung, -veränderung oder -nutzung. Gemäß § 14 Abs. 1 Satz 1 BDSG sind diese Vorgänge erlaubt, wenn sie zur Erfüllung der im Zuständigkeitsbereich der öffentlichen Stelle liegenden Aufgaben erforderlich sind und ferner die Zwecke verfolgt werden, zu denen die Datenerhebung erfolgte. Für das Vorliegen einer Datenerhebung ist es gemäß § 3 Abs. 3 BDSG notwendig, dass Daten über den Betroffenen beschafft werden; hierzu muss eine zielorientierte Vorgehensweise gegeben sein.[293] Falls die Daten ohne Erhebung der öffentlichen Stelle zur Kenntnis gelangt sind, dürfen sie nach § 14 Abs. 1 Satz 2 BDSG nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert wurden. Dieser seltene Fall ist dann gegeben, wenn ein Bürger einer Behörde unverlangt personenbezogene Daten, beispielsweise mittels einer Initiativbewerbung, bereitstellt und ist für die weitere Betrachtung nicht relevant.

Da sich bereits die Datenerhebung nicht durch eine Rechtfertigungsgrundlage aus dem Bundesdatenschutzgesetz legitimieren lässt, gilt dies ebenso für die Speicherung, Veränderung oder Nutzung der Daten in einem Data-Warehouse. Mangels Erforderlichkeit dieser Vorgänge für den Zweck der Aufgabenwahrnehmung der öffentlichen Stelle dürfen solche Vorgänge auf Grundlage des § 14 Abs. 1 Satz 1 BDSG nicht vollzogen werden.

Im Verwaltungsvollzug lässt sich der Zweckbindungsgrundsatz nicht immer stringent wahren. § 14 Abs. 2 BDSG enthält daher einen umfassenden Ausnahmekatalog, wann Zweckänderungen abweichend vom Erhebungszweck zulässig sind. Die

[291] *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.7 Rn. 58.
[292] *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.7 Rn. 62.
[293] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 24; *Hoss*, Callcenter: Mitarbeiterkontrollen auf dem datenschutzrechtlichen Prüfstand, 2010 (abrufbar unter: http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-010050732848/3/HossCallcenter.pdf).

Daten dürfen bei Vorliegen der Voraussetzungen zu einem anderen Zweck verarbeitet oder genutzt werden, als zu dem sie erhoben wurden. Da jede Zweckänderung einen eigenständigen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen darstellt, ist die Eingriffsrechtfertigung eng auszulegen.[294]

§ 14 Abs. 2 Nr. 1 BDSG lässt das Speichern, Verändern oder Nutzen personenbezogener Daten für andere Zwecke als den eigentlichen Erhebungszweck zu, wenn dies eine Rechtsvorschrift vorsieht oder zwingend voraussetzt. Eine Rechtsvorschrift, die der öffentlichen Verwaltung ausdrücklich den Betrieb eines Data-Warehouse inklusive die Durchführung von Data-Mining zubilligt oder sogar zwingend vorschreibt, existiert außerhalb des Polizeirechts und außerhalb des Bereichs der Strafverfolgung nicht. Darüber hinaus vermag gemäß § 14 Abs. 2 Nr. 2 BDSG die Einwilligung des Betroffenen eine Zweckänderung zulässig herbeizuführen. Da eine Einwilligung gemäß § 4 Abs. 1 BDSG ohnehin den Umgang mit personenbezogenen Daten rechtfertigen kann, ist die ausdrückliche Aufnahme dieser Möglichkeit in den Katalog der Zweckänderungen im Grunde genommen überflüssig.[295] Die Einwilligung als Rechtfertigungsgrundlage im Zusammenhang mit Data-Warehousing und Data-Mining in der öffentlichen Verwaltung wird untenstehend gesondert beleuchtet. § 14 Abs. 2 Nr. 3 BDSG kann eine Zweckänderung erlauben, wenn sie offensichtlich im Interesse des Betroffenen liegt und kein Grund zur Annahme existiert, dass der Betroffene in Kenntnis des anderen Zwecks seine Zustimmung verweigern würde. Es ist zwar nicht ausgeschlossen, dass generelle Vorteile – beispielsweise die Beschleunigung der Verfahrensabläufe – aus einem personenbezogenen Data-Warehouse und dessen Auswertung resultieren können. Dennoch wird der betroffene Bürger keine konkreten Vorteile für sich selbst daraus erlangen, dass gerade seine persönlichen Daten gespeichert und analysiert werden. Im Übrigen ist die persönlichkeitsrechtliche Beeinträchtigung als hoch einzustufen, sodass klar überwiegende Vorteile nicht gegeben sein können. Auch die weiteren Ausnahmetatbestände des § 14 Abs. 2 Nr. 4 - 9 BDSG greifen problembezogen nicht.[296]

Aus der Betrachtung der denkbaren Zweckänderungen gemäß § 14 Abs. 2 Nr. 1 und Nr. 3 - 9 BDSG folgt also, dass sich der Aufbau und Betrieb eines Data-Warehouse

[294] *Schulz/Waldenspuhl/Hermerschmidt*, Data Warehouse und Data Mining im öffentlichen Bereich, 2002, 12 (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf).
[295] So auch *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 14 Rn. 16.
[296] *Schulz/Waldenspuhl/Hermerschmidt*, Data Warehouse und Data Mining im öffentlichen Bereich, 2002, 12 f. (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf).

sowie die Durchführung von Data-Mining durch öffentliche Stellen grundsätzlich nicht durch die Zweckänderungen legitimieren lassen.[297]

Da die bislang untersuchten Vorschriften des allgemeinen Datenschutzrechts keine Rechtfertigung zum Data-Warehousing und Data-Mining mit personenbezogenen Daten in Bezug auf öffentliche Stellen enthalten, ist die Frage nach der Zulässigkeit einer diesbezüglichen datenschutzrechtlichen Einwilligung zu stellen.[298] Eine rechtswirksame Einwilligung des Betroffenen gemäß § 4a BDSG vermag auch zur Legitimation von personenbezogenen Datenverarbeitungsvorgängen bei öffentlichen Organisationen zu führen; sie kann ausnahmsweise dann in Betracht kommen, wenn der Datenumgang direkten Bezug zur Erfüllung der gesetzlich zugewiesenen Aufgabe der Stelle aufweist und mindestens dazu geeignet ist. Aufgrund der Tatsache, dass es generell jedoch nicht zum Aufgabengebiet von öffentlichen Stellen gehört, Data-Warehousing und Data-Mining mit personenbezogenen Daten der Bürger zu betreiben, führte eine diesbezügliche Einwilligung zur Ausdehnung der hoheitlichen Befugnisse der Stelle und wäre damit unzulässig.[299]

Im Hinblick auf personenbezogenes Data-Warehousing und Data-Mining bei öffentlichen Stellen lässt sich allgemein festhalten, dass diese Vorgänge ohne weitere Einschränkung nicht erlaubt sind.

3.1.1.4.4.2 Automatisierte Einzelentscheidung

Im Zusammenhang mit dem Kundendatenbank-System und den eingesetzten Auswertungsmethoden ist die Frage aufzuwerfen, ob die daraus gewonnenen Ergebnisse nicht eine automatisierte Einzelentscheidung im Sinne des § 6a BDSG darstellen. Nach der Vorschrift dürfen Entscheidungen, die für den Betroffenen rechtliche Folgen nach sich ziehen oder ihn erheblich beeinträchtigen, grundsätzlich nicht ausschließlich auf Grundlage einer automatisierten Verarbeitung personenbezogener Daten ergehen, welche der Bewertung von Persönlichkeitsmerkmalen dient. Dies ist insbesondere dann der Fall, wenn eine inhaltliche Bewertung des Sachverhalts

[297] Mit demselben Ergebnis *Schulz/Waldenspuhl/Hermerschmidt*, Data Warehouse und Data Mining im öffentlichen Bereich, 2002, 12 f. (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf).
[298] *Engelien-Schulz*, VR 2009, 73 (75); *Globig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.7 Rn. 37 ff.
[299] *Engelien-Schulz*, VR 2009, 73 (75); *Schulz/Waldenspuhl/Hermerschmidt*, Data Warehouse und Data Mining im öffentlichen Bereich, 2002, 14 (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf); *Menzel*, DuD 2008, 400 ff.

durch eine natürliche Person und eine darauf beruhende Entscheidung nicht stattfand.

Allgemein bezweckt die Vorschrift zu verhindern, dass man sich auf automatisierte Verfahren verlässt, die mit mehr oder weniger pauschalen Informationen arbeiten und der Vielfalt der Lebensverhältnisse nicht gerecht werden können. Menschen dürfen nicht von Computern getroffenen Entscheidungen ausgeliefert sein.[300]

Ausnahmen von dem grundsätzlichen Verbot liegen gemäß § 6a Abs. 2 Nr. 1 und Nr. 2 BDSG vor, wenn einerseits die Entscheidung im Zusammenhang mit einem Vertrags- oder einem sonstigen Rechtsverhältnis getroffen wird und dem Begehren des Betroffenen entspricht. Andererseits ist ein Abweichen möglich, wenn geeignete Maßnahmen implementiert wurden, die der Wahrung der berechtigten Interessen des Betroffenen dienen und dieser über das Vorliegen einer automatisierten Einzelentscheidung informiert wird. Darüber hinaus sind ihm auf sein Verlangen hin sämtliche entscheidungsrelevanten Gründe offenzulegen und zu erklären.

§ 6a BDSG gilt für nichtöffentliche und öffentliche Callcenter von Bundeseinrichtungen gleichermaßen. Auch in den Landesdatenschutzgesetzen sind entsprechende Vorschriften enthalten, wobei einige Bundesländer Ausnahmen von dem Grundsatz zulassen.[301]

Vollzieht sich der Einsatz von Data-Mining-Methoden mit dem Zweck, vollständig automatisiert über Kreditvergaben zu entscheiden, so handelt es sich um Verfahren gemäß § 6a BDSG.[302] Die weiteren Voraussetzungen des § 6a Abs. 1 BDSG sind erfüllt, wenn die Erkenntnisse, die aus der automatisierten Auswertung von Persönlichkeitsmerkmalen resultieren, direkt zur Entscheidungsfindung führen. Stellen diese Erkenntnisse nur Grundlage für weitere Schritte im Entscheidungsfindungsprozess dar und die endgültige Entscheidung wird von einem Menschen getroffen, liegt keine automatisierte Einzelentscheidung im Sinne der Vorschrift vor.[303] Dasselbe gilt, wenn neben einem automatisiert errechneten Ergebnis weitere Faktoren in die Entscheidung mit einbezogen werden.[304]

[300] *Roßnagel*, NJW 2009, 2716 (2719); *Bull*, NJW 2006, 1617 (1622); ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 6a Rn. 1; *Piltz/Holländer*, ZRP 2008, 143 (145).
[301] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 6a Rn. 20.
[302] *Bull*, NJW 2006, 1617 (1622).
[303] *Möller/Florax*, NJW 2003, 2724 (2725); *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 6a Rn. 5.
[304] *Abel*, RDV 2006, 108 (112).

Wird etwa ein Kunde aufgrund der zu seiner Person errechneten Bewertung in Bezug auf seine Bonität einer bestimmten Gruppe zugeordnet, was wiederum über den Zugang zu bestimmten Angeboten entscheidet, kann darin bereits eine erhebliche Beeinträchtigung des Kunden liegen.[305] Eine eindeutig beeinträchtigende Folge im Sinne der Vorschrift ist beispielsweise darin zu sehen, dass die automatisierte Auswertung zu einer Einschränkung der möglichen Zahlungsweise eines Kunden auf Vorkasse oder Nachnahme führt.[306] Im Bereich der öffentlichen Verwaltung liegt eine Entscheidung mit rechtlichen Konsequenzen vor, wenn ein Verwaltungsakt ergeht.[307] Fällt demgegenüber im Rahmen einer breit gestreuten Werbeaktivität die Entscheidung zu Gunsten der Zusendung eines Werbeprospekts an einen bestimmten Kunden, so ist die geforderte rechtliche oder erheblich beeinträchtigende Folge nicht gegeben.[308] Es ist stets im Einzelfall zu prüfen, ob mit dem Ergebnis aus dem eingesetzten Verfahren der automatisierten Einzelentscheidung die Schwelle zur rechtlichen Folge oder erheblichen Beeinträchtigung überschritten werden kann.

Das bedeutendste automatisierte Verarbeitungsverfahren besteht im Scoring gemäß § 28b BDSG. Beim Scoring werden Kunden anhand verschiedenster Kriterien unter Zuhilfenahme mathematisch-statistischer Verfahren nach ihrer wirtschaftlichen Leistungsfähigkeit bewertet und bekommen auf Grundlage des ermittelten Ergebnisses vertragliche Konditionen angeboten.[309] Dabei gelangen Analyseverfahren zum Einsatz, die die Wahrscheinlichkeit des zukünftigen Verhaltens von Kunden vorhersagen. Meist gelangt Scoring im Zusammenhang mit der Entscheidung über Kreditvergaben zur Anwendung. Durch Auswertung des bisherigen Verhaltens vergleichbarer Personengruppen lässt sich prognostizieren, wie bestimmte Kunden den Kredit voraussichtlich bedienen.[310]

Banken gehen mit dem Verbot aus § 6a BSDG in der Praxis derart um, dass ein Kreditgesuch nicht ausschließlich aufgrund eines schlechten Scores des Kreditbewerbers Ablehnung findet; im Falle einer schlechten Bewertung wird das Gesuch noch einmal durch einen Bankmitarbeiter überprüft.[311]

---

[305] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 129; zur Zulässigkeit der Übermittlung von Kundendaten mit Angaben zur Bonität an Wirtschaftsauskunfteien *Taeger*, BB 2007, 785 ff.
[306] *Taeger*, in: Schubert/Reusch/Jesse (Hrsg.), Informatik bewegt, 2002, 537 (539); *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 6a Rn. 10.
[307] *Möller/Florax*, MMR 2002, 806 (809).
[308] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 6a Rn. 10.
[309] *Piltz/Holländer*, ZRP 2008, 143; *Wäßle/Heinemann*, CR 2010, 410 f.
[310] *Möller/Florax*, MMR 2002, 806 f.; a. A. *Wuermeling*, NJW 2002, 3508 ff., der gegen das Scoring-Verfahren der SCHUFA keine datenschutzrechtlichen Bedenken hat.
[311] *Klein*, BKR 2003, 488 (489).

Wenn ein Verfahren der automatisierten Einzelentscheidung zur Anwendung kommt, steht den Kunden gemäß § 6a Abs. 3 BDSG ein erweitertes Auskunftsrecht – über §§ 34 und 19 BDSG hinaus – zu, das sich auf den logischen Aufbau der automatisierten Datenverarbeitung bezieht. Im Rahmen dieses Auskunftsrechts sollen die grundlegenden Funktionsprinzipien dargelegt werden.[312]

Zusammenfassend lässt sich konstatieren, dass die Frage, ob eine automatisierte Einzelentscheidung nach § 6a BDSG im Rahmen des Data-Minings vorliegt, nur unter einzelfallabhängiger Betrachtung des konkreten Verfahrens beantwortet werden kann. Sollte das Verfahren die Voraussetzungen des § 6a Abs. 1 BDSG erfüllen, müssen entweder die Ausnahmen gemäß Abs. 2 gegeben sein, oder die Ergebnisse müssen – analog dem aufgezeigten Vorgehen von Banken – vor endgültiger Entscheidungsfindung nochmals durch einen Sachbearbeiter geprüft werden.

3.1.1.4.5 Weitere Informationsquellen

Über Suchvorgänge in internen Informationsquellen hinaus sollen Suchvorgänge in externen Datenbanken, wie Wikipedia, und anderen über das Internet frei verfügbaren Ressourcen realisiert werden. Durch Einbeziehung der in kollaborativer Arbeit entstandenen Wissensquellen lässt sich die Qualität der Suchergebnisse optimieren. Diese Suchprozesse werden automatisiert durch die Spracherkennung oder durch manuelle Texteingaben am Frontend-System der Callcenter-Agenten ausgelöst.

Die Anbindung externer Wissensquellen an das Gesprächsmanagement-System und die dortige Datenverarbeitung ist aus Sicht des Datenschutzes grundsätzlich unproblematisch. Es werden keine Suchvorgänge in externen Datenbanken innerhalb der Gesprächsphasen ausgelöst, in denen personenbezogene Daten – beispielsweise solche zur Nutzeridentifizierung – abgefragt werden müssen. Die an die externen Wissensquellen gesandten Suchanfragen enthalten keine weitergehenden Informationen, die eine Aufdeckung der dahinterstehenden Person zuließen. Die Anfragen bestehen lediglich aus den im Telefongespräch erkannten Schlüsselwörtern.

Texteingaben über das Freitextfeld am Frontend-System sind datenschutzrechtlich genauso einzustufen, wie wenn der Callcenter-Agent mittels herkömmlichem Internetbrowser während des Gesprächs mit Kunden in frei zugänglichen Internetressourcen nach weitergehenden Informationen sucht. Personenbezogene Daten der

[312] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 6a Rn. 18 f.; *Petri*, DuD 2003, 631 (635); *Beckhusen*, BKR 2005, 335 (343 f.); zum datenschutzrechtlichen Auskunftsanspruch beim Scoring ausführlich *Heinemann/Wäßle*, MMR 2010, 600 ff.

Kunden sind nicht betroffen, da sich Suchvorgänge in der Regel lediglich auf technische Informationen beziehen und der Abhilfe bei Problemen mit einem Produkt dienen sollen. Anders wäre die Situation zu beurteilen, wenn explizit Personensuchmaschinen oder soziale Netzwerke in die Suche mit eingeschlossen würden.

3.1.1.4.6 Bewertung des gesamten Systems

Im Hinblick auf den Einsatz des gesamten Gesprächsmanagement-Systems, unter Einbeziehung sämtlicher Systemkomponenten, lässt sich konstatieren, dass für die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Kundendaten in erster Linie die Rechtsbeziehung zwischen dem Callcenter oder seinem Auftraggeber und den Kunden ausschlaggebend ist.[313]

Wie in obenstehenden Ausführungen dargelegt wurde, lässt sich der Betrieb nahezu aller Systemkomponenten grundsätzlich auf die allgemeinen gesetzlichen Erlaubnistatbestände stützen, das heißt unter anderem auf ein bestehendes oder potenzielles Schuldverhältnis gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG oder auf berechtigte Interessen des Callcenter-Betreibers aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Eine Ausnahme kann jedoch die CRM-Datenbank darstellen, die sich als größte Schwierigkeit in Bezug auf den Datenschutz erweist: Das fortlaufend aktualisierte Festhalten der Kundendaten in der Kundendatenbank verwirklicht eine Vorratsdatenspeicherung. In Abhängigkeit davon, welche Daten wie lange und zu welchen konkreten Zwecken dort gespeichert sein sollen, sind unterschiedlich hohe Zulässigkeitsvoraussetzungen zu erfüllen. Liegt beispielsweise ein Dauerschuldverhältnis vor, so dürfen personenbezogene Daten, die für die voraussichtliche Dauer des Vertragsverhältnisses erforderlich sind, gespeichert bleiben. In bestimmten Fällen, wenn zum Beispiel gesetzliche Aufbewahrungsfristen einzuhalten sind, kann eine über das Vertragsverhältnis hinausgehende Speicherung der Daten zulässig sein.

Insbesondere ist die eingesetzte Methode zur Auswertung der gespeicherten Daten von hoher Relevanz: Je extensiver das angewandte Data-Mining – bei dem vollkommen unklar sein kann, welche Informationen potenziell überhaupt gewonnen werden können – desto höher sind die Anforderungen an die rechtliche Legitimation dieser Vorgänge. Die Zweckbindung der Daten ist bei der Anwendung derartiger Methoden massiv gefährdet. Vordefinierte und „profane“ Abfragen hingegen bedeuten im Regelfall weniger intensive Eingriffe in das Persönlichkeitsrecht der be-

[313] So auch *Gola*, Datenschutz im Call Center, 2. Aufl. 2006, 101.

troffenen Kunden. Zu Letzteren kann beispielsweise die Kenngröße Umsatz pro Kunde gezählt werden.

Primär aufgrund der dargestellten Schwierigkeiten im Zusammenhang mit Data-Warehousing und Data-Mining kann es sich für nichtöffentliche Callcenter als notwendig erweisen, sich eine diesbezügliche Einwilligung der Kunden erteilen zu lassen. Einzelfallabhängig – vor dem Hintergrund des jeweiligen Anwendungskontexts des Gesprächsmanagement-Systems – muss geprüft werden, ob der intendierte Datenumgang noch von den gesetzlichen Erlaubnistatbeständen gedeckt ist. Andernfalls ist der Rückgriff auf die datenschutzrechtliche Einwilligung der Kunden unumgänglich, wenn personenbezogene – und nicht anonyme – Daten betroffen sind.

Neben den Rechtfertigungsgrundlagen aus § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG kommt eine Rechtfertigung im Hinblick auf Werbezwecke aus § 28 Abs. 3 BDSG in Betracht: Soll das Gesprächsmanagement-System mit sämtlichen Systemkomponenten für Werbezwecke im Callcenter zur Anwendung gelangen, ist nach § 28 Abs. 3 Satz 1 BDSG die datenschutzrechtliche Einwilligung der (potenziellen) Kunden praktisch zwingend erforderlich. Lediglich einzelne Systemkomponenten, wie das Frontend-System, dürfen in bestimmten Fällen einwilligungsfrei eingesetzt werden.

Die Einwilligung gemäß § 28 Abs. 3 Satz 1 BDSG muss überdies um die Phase der Datenerhebung für Zwecke der Werbung erweitert werden, da das Gesprächsmanagement-System durch die Sprach- und Emotionserkennung im Normalbetrieb kontinuierlich personenbezogene Daten gemäß § 3 Abs. 3 BDSG zielgerichtet beschafft. Der personenbezogene Datenumgang im Gesprächsmanagement-System lässt sich – sofern die volle Funktionalität des Systems genutzt werden soll – nicht mehr auf eine gesetzliche Rechtfertigungsgrundlage aus § 28 Abs. 3 BDSG stützen. Im Ergebnis bedeutet dies für das Callcenter, dass es sich selbst für die Fälle, in denen ihm der Datenumgang im Gesprächsmanagement-System etwa für Zwecke der Durchführung eines Vertragsverhältnisses grundsätzlich erlaubt ist, die Einwilligung in den Datenumgang für Werbezwecke erteilen lassen muss. Hier liegt eine Zweckänderung vor, die nach den Grundsätzen des Datenschutzrechts stets einer eigenen Legitimation bedarf.

Da ohnehin ein wettbewerbsrechtliches Erfordernis zur Einholung einer Einwilligung in die Durchführung von Werbeanrufen besteht, sollte im Zusammenhang mit dieser Einverständniserklärung gleichzeitig eine datenschutzrechtliche Einwilligung

zum Datenumgang im Gesprächsmanagement-System eingeholt werden, falls die vorgesehene Werbekampagne in Form der Outbound-Telefonie stattfinden soll.[314]

Was Callcenter der öffentlichen Verwaltung anbelangt, bestehen allgemein schärfere Zulässigkeitsvoraussetzungen für den Einsatz des Gesprächsmanagement-Systems als bei nichtöffentlichen Callcentern. Der Grund liegt darin, dass bei öffentlichen Stellen ein sehr begrenzter Spielraum bezüglich der Auslegung des Rechtsbegriffs „Erforderlichkeit" vorhanden ist. Allerdings muss eine spezielle Erforderlichkeit für den Aspekt der Bürgerfreundlichkeit berücksichtigt werden. Jedenfalls können – im Gegensatz zu nichtöffentlichen Callcentern – berechtigte Interessen der öffentlichen Stelle keinen personenbezogenen Datenumgang legitimieren.

Grundsätzlich ist der Datenumgang, unter Beachtung des Erforderlichkeitsgrundsatzes, im Frontend-System und in der Telefonanlage gemäß §§ 13 Abs. 1 und 14 Abs. 1, 2 BDSG erlaubt. Schwieriger ist die Beurteilung der Zulässigkeit im Hinblick auf die Spracherkennungskomponente. Hier gilt es im Einzelfall zu prüfen, ob das Einverständnis der Kunden herangezogen werden kann. Die Emotionserkennung wird sich in der Regel nur auf Grundlage einer Einwilligung zulässig einsetzen lassen.

Für öffentliche Stellen gilt das Kriterium der Erforderlichkeit als besonders hohe Hürde in Bezug auf das CRM-System. Hier ist stets einzelfallabhängig zu prüfen, ob und inwieweit die Datenerhebung, -verarbeitung oder -nutzung zur Ausführung der der öffentlichen Stelle gesetzlich zugewiesenen Aufgabe erforderlich ist. Dabei muss auch die Speicherungsdauer der personenbezogenen Daten Berücksichtigung finden. Eine generelle Angabe zur Zulässigkeit ist nicht möglich. Sicher hingegen ist jedenfalls, dass umfangreiche Datenansammlungen im Data-Warehouse in der öffentlichen Verwaltung nicht zu deren Aufgabenerfüllung erforderlich sein können. Erst recht muss dies für Methoden des Data-Minings gelten. Selbst die diesbezügliche Einwilligung der Kunden vermag die Rechtswidrigkeit nicht zu heilen. Je nach gesetzlich übertragener Aufgabe der öffentlichen Stelle kann zu deren Durchführung der Umgang mit mehr oder weniger umfangreichen personenbezogenen Daten erforderlich sein; der Umgang mit den Daten ist auf das Maß zu reduzieren, welches zur Aufgabenerfüllung notwendig ist. Im äußersten Fall muss das CRM-System mit anonymen Daten betrieben oder vollständig auf seine Anbindung verzichtet werden.

[314] Es gelten die bereits in Kapitel 3.1.1.1.3 „Erlaubnis aus einer Einwilligung" aufgezeigten Grundsätze zu den inhaltlichen Anforderungen der Einwilligung.

3.1.2 Informationspflichten

3.1.2.1 Allgemeine Informationspflichten

Erfolgt eine Datenerhebung beim Betroffenen selbst, obliegen nichtöffentlichen und öffentlichen Stellen gemäß § 4 Abs. 3 BDSG ganz allgemein bestimmte Aufklärungspflichten, die der Herstellung von Transparenz und eines effektiven Rechtsschutzes dienen sollen.[315] Nach diesen Pflichten ist der Betroffene, dessen personenbezogene Daten erhoben werden, von der verantwortlichen Stelle über die

- Identität der verantwortlichen Stelle,
- Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung sowie
- Kategorien von Empfängern, soweit einzelfallabhängig nicht mit einer Datenübermittlung gerechnet werden muss,

aufzuklären. Die Aufklärungspflichten bestehen allerdings nicht mehr, wenn der Betroffene bereits anderweitig Kenntnis von den Informationen erlangt hat. Dass er über die notwendigen Angaben im Bilde ist, die Informationspflicht somit entfällt, ist von der verantwortlichen Stelle nachzuweisen. Nach allgemeiner Lebenserfahrung muss in gewissen Fällen mit einer Weitergabe der Daten gerechnet werden; liegt eine solche Konstellation vor, entfällt eine diesbezügliche Aufklärungspflicht.[316]

Angaben zur Identität der datenverarbeitenden Stelle haben in jedem Fall Name und Anschrift der nichtöffentlichen oder öffentlichen Organisation zu umfassen. Im Rahmen der Aufklärung über die Zweckbestimmung des Datenumgangs ist auf sämtliche zum Zeitpunkt der Datenerhebung verfolgten Zwecke hinzuweisen.[317] Liegt eine Auftragsdatenverarbeitung gemäß § 11 BDSG vor, die eine Datenübermittlung an den Auftragnehmer beinhaltet, muss auch darüber aufgeklärt werden.[318] Die Hinweispflicht kommt folglich nicht nur dann zum Tragen, wenn eine Übermittlung von Daten an Dritte erfolgt. Auch über systeminterne Datenflüsse, die die Organisationsgrenzen verlassen, hat der Kunde informiert zu werden.[319] Dies ist im Rahmen des Gesprächsmanagement-Systems etwa dann gegeben, wenn sich eine Komponente – beispielsweise die CRM-Datenbank – bei einem spezialisierten

[315] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BDSG, § 4 Rn. 9; ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 4 Rn. 5.
[316] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 34 ff.
[317] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 30 ff.
[318] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 4 Rn. 19.
[319] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 33 ff.

Dienstleister befindet, weil dieser ein hohes Maß an Datensicherheit garantieren kann.

Falls eine datenschutzrechtliche Einwilligung gemäß § 4a Abs. 1 BDSG zur Legitimation der vorgesehenen Datenverarbeitungsvorgänge innerhalb des Gesprächsmanagement-Systems erforderlich ist – also besonders bei der Durchführung von extensivem Data-Mining –, sind die in § 4 Abs. 3 BDSG geforderten Angaben das Minimum, was dem Betroffenen im Rahmen einer informierten Einwilligung mitzuteilen ist.[320]

Mit Blick auf den Kunden bedeutet dies unter Umständen, dass zu Beginn des Telefonats zum Beispiel eine Bandansage über die Datenverarbeitungsvorgänge aufklären muss; eine schriftliche Unterrichtung ist regelmäßig nicht notwendig.[321] Aus einer solchen Ansage hat insbesondere hervorzugehen, bei wem und wofür die Daten verwendet werden. Ist das Callcenter im Rahmen einer Auftragsdatenverarbeitung (§ 11 BDSG) für ein Unternehmen eingesetzt, muss in der Regel auch der Name des auftraggebenden Unternehmens – neben dem des Auftragnehmers – bekanntgegeben werden.

Die nachträgliche Information des Betroffenen ist in § 33 Abs. 1 BDSG geregelt: Wenn beispielsweise erstmals personenbezogene Daten ohne das Wissen des Betroffenen für eigene Zwecke gespeichert werden, ist der Betroffene über den Speicherungsprozess zu benachrichtigen. Abs. 2 enthält Regelungen, wann eine Benachrichtigung ausnahmsweise entbehrlich ist. Der großzügig angelegte Ausnahmekatalog lässt erkennen, dass die nachträgliche Benachrichtigungspflicht in den wenigsten Fällen ausgelöst wird. Als konkretes Beispiel, wann die nachträgliche Informationspflicht zum Tragen kommt, lässt sich die Speicherung von Daten bei Auskunfteien ins Feld führen.[322] Analog zu § 33 BDSG regelt § 19a BDSG die Benachrichtigungspflicht für öffentliche Einrichtungen.

In Bezug auf den Betrieb des Gesprächsmanagement-Systems haben die beiden Vorschriften zur nachträglichen Information der Kunden regelmäßig keine Relevanz, da den Kunden der Umgang mit ihren personenbezogenen Daten durch die bereits aufgezeigten Aufklärungspflichten bekannt sein muss. Wird der Aufklärungspflicht im Rahmen des § 4 Abs. 3 BDSG adäquat nachgekommen, das heißt für den Betroffenen ist insbesondere erkennbar, welche Verarbeitungsvorgänge zu

[320] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 40.
[321] S. dazu Kapitel 3.1.1.1.3 „Erlaubnis aus einer Einwilligung“.
[322] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 33 Rn. 27.

welchen Zwecken aktuell und potenziell vorgesehen sind, besteht etwa bei der Erweiterung der Datensätze im CRM-System keine Benachrichtigungspflicht.[323]

3.1.2.2 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Seit 1. September 2009[324] existiert mit § 42a BDSG eine besondere Informationspflicht für nichtöffentliche Unternehmen und öffentliche Wettbewerbsunternehmen, die die unrechtmäßige Übermittlung personenbezogener Daten und deren Kenntniserlangung durch Dritte betrifft. Der Neuregelung kommt große praktische Bedeutung zu, da nahezu jedes Unternehmen von ihr betroffen sein kann.[325]

Organisationen, bei denen beispielsweise Datenlecks dazu führen, dass Dritte illegal an bestimmte personenbezogene Daten gelangen, haben in der Regel bereits allein wegen des drohenden Imageverlusts großes Interesse daran, die „Datenpanne" zu verheimlichen oder sogar zu verschleiern. Der Zweck der Regelung des § 42a BDSG besteht darin, den Betroffenen derartiger Datenverluste frühzeitig darüber in Kenntnis zu setzen, damit er die Möglichkeit hat, weitergehende Schäden zu verhindern und seine Betroffenenrechte wahrzunehmen.[326]

Der Verstoß gegen diese besondere Informationspflicht stellt eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 7 BDSG dar, die gemäß § 43 Abs. 3 Satz 1 BDSG mit einem Bußgeld in Höhe von bis zu 300.000 Euro sanktioniert werden kann.

Nach der Vorschrift des § 42a BDSG sind die Betroffenen sowie die Aufsichtsbehörde in bestimmten Fällen zu informieren, wenn eine unrechtmäßige Übermittlung oder anderweitig unrechtmäßige Kenntniserlangung durch Dritte in Bezug auf festgelegte Datenkategorien stattgefunden hat. Um bezeichnete Datenarten handelt es sich bei

- sensitiven personenbezogenen Daten gemäß § 3 Abs. 9 BDSG,
- den einem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- personenbezogenen Daten im Zusammenhang mit strafbaren Handlungen oder Ordnungswidrigkeiten sowie einem diesbezüglichen Verdacht,
- personenbezogenen Daten zu Kreditkarten- und Bankkonten.

[323] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 33 Rn. 16.
[324] BT-Drs. 16/13657 und BT-Drs. 16/12011.
[325] *Duisberg/Picot*, CR 2009, 823 (825).
[326] *Hornung*, NJW 2010, 1841.

Überdies müssen schwerwiegende Beeinträchtigungen schutzwürdiger Interessen oder Rechte der Betroffenen zu befürchten sein, damit die Informationspflicht ausgelöst wird. Diesbezügliche Beeinträchtigungen können sowohl materieller Art, zum Beispiel aufgrund des Bekanntwerdens von Kontodaten, als auch immaterieller Natur, etwa wegen einer massiven Persönlichkeitsrechtsverletzung, sein.[327]

Die Vorschrift schreibt fest, dass die Daten „bei" der verantwortlichen Stelle gespeichert sein müssen, damit die Stelle von dieser Informationspflicht überhaupt betroffen sein kann. Dies wirkt sich auf Auftragsdatenverarbeitungsverhältnisse aus: Da der Auftraggeber im Außenverhältnis Verantwortlicher der Datenverarbeitungsprozesse bleibt, wird er selbst von der Unterrichtungspflicht erfasst.[328] § 11 Abs. 4 BDSG, welcher die Pflichten des Auftragnehmers aufführt, enthält keine dahingehende Aussage, dass die Informationspflicht für Auftragsdatenverarbeiter gilt.[329] Lagert beispielsweise ein Handelsunternehmen seinen telefonischen Service auf ein rechtlich selbstständiges Callcenter aus, so muss die auslagernde Organisation – im Falle eines entsprechenden Datenverlusts – der diesbezüglichen Informationspflicht nachkommen. Damit der Auftraggeber überhaupt seine Informationspflicht erfüllen kann, muss ihn der Auftragsdatenverarbeiter über Datenverluste in Kenntnis setzen.[330] Deshalb ist im Rahmen der Auftragsgestaltung darauf zu achten, dass der Auftragsdatenverarbeiter vertraglich verpflichtet wird, sämtliche Datenverluste dem Auftraggeber unverzüglich anzuzeigen und diesen bei gegebenenfalls entstehenden Benachrichtigungsverpflichtungen zu unterstützen.[331]

Die Meldung über den Datenverlust gegenüber dem Betroffenen hat unverzüglich zu geschehen, nachdem angemessene Datensicherungsmaßnahmen eingeleitet worden oder nicht unverzüglich erfolgt sind und keine Gefährdung der Strafverfolgung mehr besteht; es darf kein schuldhaftes Zögern vorliegen.[332] Ferner muss keine absolute Gewissheit darüber bestehen, dass genannte personenbezogene Daten tatsächlich zur Kenntnis Dritter gelangt sind, Anhaltspunkte dafür sind bereits ausreichend. Irrelevant ist darüber hinaus das Wissen um die Person des Dritten: Das Bewusstsein, dass die Daten unrechtmäßig an irgendjemanden gelangt sind, genügt.[333] Die zuständige Aufsichtsbehörde ist demgegenüber ohne Einschränkung unvermittelt zu informieren; sie ist zur Verschwiegenheit verpflichtet.[334]

[327] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 42a Rn. 4; *Wanagas*, DStR 2010, 1908 (1910).
[328] *Hornung*, NJW 2010, 1841 (1842).
[329] *Gabel*, BB 2009, 2045 (2046).
[330] *Gabel*, BB 2009, 2045 (2046).
[331] *Duisberg/Picot*, CR 2009, 823 (825).
[332] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 42a Rn. 2.
[333] *Wanagas*, DStR 2010, 1908 (1910).
[334] *Gabel*, BB 2009, 2045 (2048); *Wanagas*, DStR 2010, 1908 (1910).

Satz 3 und 4 des § 42a BDSG enthalten inhaltliche Anforderungen an die Information, die den Betroffenen und der Aufsichtsbehörde erteilt werden muss. In Bezug auf den Betroffenen sind die Art der unrechtmäßigen Kenntniserlangung sowie empfohlene Maßnahmen zur Eindämmung potenzieller negativer Folgen mitzuteilen. Die Benachrichtigung der Aufsichtsbehörde muss überdies eine Darlegung möglicher nachteiliger Konsequenzen aufgrund der unrechtmäßigen Kenntniserlangung und der diesbezüglich eingeleiteten Maßnahmen der verantwortlichen Stelle umfassen. Diese Informationen kann das Kontrollorgan bei der Durchführung sich eventuell anschließender Prüfungen der verantwortlichen Stelle heranziehen.[335]

Falls die Benachrichtigung sämtlicher einzelnen Betroffenen einen unverhältnismäßigen Aufwand bedeutete, kann sie gemäß § 42a Satz 5 BDSG öffentlich, insbesondere mittels Zeitungsanzeigen, erfolgen.

Dem Entstehen des Dilemmas, sich entweder selbst zu bezichtigen oder andernfalls eine Ordnungswidrigkeit aufgrund des Nichtnachkommens der Informationspflicht zu begehen, wurde durch § 42a Satz 6 BDSG Abhilfe geschaffen: Die Verwendung der erteilten Benachrichtigung im Rahmen eines Straf- oder Ordnungswidrigkeitenverfahrens gegen den Informationspflichtigen oder einen Angehörigen nach § 52 Abs. 1 StPO kommt nur unter Zustimmung des Benachrichtigungspflichtigen in Betracht. Dieses Verwendungsverbot erstreckt sich allerdings nicht auf Zivilverfahren, die beispielsweise Schadenersatzzahlungen zum Gegenstand haben.[336]

3.1.3 Rechte der Kunden

Durch die Novellen des Bundesdatenschutzgesetzes[337] erfuhren die Rechte der Betroffenen – problembezogen der Kunden – eine weitergehende Stärkung. Welche konkreten Ansprüche Kunden haben, ist nachfolgend dargestellt. In den landesgesetzlichen Bestimmungen zum Datenschutz finden sich dieselben Rechte – lediglich mit im Detail geringfügigen Abweichungen – wieder, sodass auf deren Darstellung verzichtet werden kann.

[335] *Hornung*, NJW 2010, 1841 (1843).
[336] *Wanagas*, DStR 2010, 1908 (1910); *Hornung*, NJW 2010, 1841 (1843); *Gabel*, BB 2009, 2045 (2049).
[337] BDSG-Novelle I, Fassung der BT-Drs. 16/10529 und 16/10581 mit den Änderungen der BT-Drs.
16/13219, trat am 1.4.2010 in Kraft; BDSG-Novelle II, Fassung der BT-Drs. 16/12011 mit den Änderungen der BT-Drs. 16/13657, trat weitestgehend am 1.9.2009 in Kraft mit Übergangsregelungen in § 47 (§ 34 Abs. 1a, Abs. 5 und § 43 Abs. 1 Nr. 8a BDSG neuer Fassung trat am 1.4.2010 in Kraft).

Die in den §§ 34 und 35 BDSG in Bezug auf nichtöffentliche Unternehmen sowie im Hinblick auf die öffentliche Verwaltung in den §§ 19 und 20 BDSG verankerten Rechte auf Auskunft, Berichtigung, Löschung und Sperrung sind unabdingbar, das heißt sie können gemäß § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft, beispielsweise einen Vertrag, ausgeschlossen oder beschränkt werden. Die Unabdingbarkeit dieser Rechte ist auch weitgehend in den Landesdatenschutzgesetzen verankert.[338] Genannte Ansprüche sind gegenüber der verantwortlichen Stelle gemäß § 3 Abs. 7 BDSG geltend zu machen. Wird das Callcenter im Rahmen einer Auftragsdatenverarbeitung betrieben, müssen sich Kunden an den Auftraggeber wenden, um ihre Rechte durchzusetzen.

3.1.3.1 Recht auf Auskunft

Was das Recht des Betroffenen auf Auskunft[339] über die zu seiner Person gespeicherten Daten anbelangt, so wurde die Vorschrift des § 34 BDSG vollkommen abgeändert und insbesondere an die Spezifika des Scorings angepasst.[340]

Das Callcenter ist auf Ersuchen des Kunden verpflichtet, Auskunft über

- die zu seiner Person gespeicherten Daten,
- potenzielle Empfänger und Empfängerkategorien der Daten und
- den Speicherungszweck

zu erteilen.[341] Gemäß § 34 Abs. 6 BDSG ist sie unter normalen Umständen auf Verlangen des Kunden in Textform durchzuführen. § 34 Abs. 8 Satz 1 BDSG bestimmt, dass die Auskunft grundsätzlich für den Kunden kostenfrei zu erfolgen hat. Für bestimmte Fälle, für die auch keine Benachrichtigungspflicht aus § 33 Abs. 2 BDSG besteht, ist die Information des Kunden gemäß § 34 Abs. 7 BDSG freiwillig.

Die datenschutzrechtliche Auskunft muss grundsätzlich vollständig sein und sich auf sämtliche gespeicherten Daten beziehen. Was jedoch vorliegende Kundendaten im Data-Warehouse – die unter Umständen erst durch Hinzuspeicherung und Verknüpfung weiterer Informationen entstehen – betrifft, so sind diesbezüglich weniger

[338] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 6 Rn. 9; beispielsweise im bayerischen Datenschutzgesetz ist die Unabdingbarkeit der Betroffenenrechte nicht ausdrücklich manifestiert.
[339] Zur praktischen Wirksamkeit des Auskunftsanspruchs aus § 34 Abs. 1 BDSG ausführlich *Hoss*, RDV 2011, 6 ff.
[340] *Roßnagel*, NJW 2009, 2716 (2719).
[341] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 34 Rn. 1.

die einzelnen Details als vielmehr die Funktionsprinzipien und Auswertungsmöglichkeiten der eventuell eingesetzten Data-Mining-Methoden relevant.[342]

Eine festgelegte Frist für den Zeitpunkt der Auskunft, nachdem eine diesbezügliche Anfrage bei der verantwortlichen Stelle eingegangen ist, existiert nicht. Daher ist auf eine im allgemeinen Geschäftsverkehr übliche Frist abzustellen, die im Regelfall zwei Wochen beträgt. Ist absehbar, dass diese Zeitspanne nicht eingehalten werden kann, empfiehlt es sich dringend, dem Antragsteller einen Zwischenbericht zum Bearbeitungsstand zu geben. Dieses Vorgehen soll in erster Linie dazu dienen, die Einschaltung der Aufsichtsbehörde zu verhindern.[343]

Damit keine Unberechtigten an personenbezogene Informationen Dritter gelangen, muss sich das Callcenter über die Identität des Auskunftsersuchenden vergewissern. Bei einem persönlichen Erscheinen des Kunden ist die Vorlage eines Ausweisdokuments zu verlangen. Mit der Abfrage eines Passworts lässt sich etwa beim telefonischen Kontakt sicherstellen, dass es sich tatsächlich um die Person handelt, die sie vorgibt zu sein.[344]

Der Auskunftsanspruch gegenüber öffentlichen Bundeseinrichtungen, problembezogen öffentlichen Callcenter-Betrieben, ist in § 19 BDSG reglementiert und im Wesentlichen deckungsgleich mit dem gegenüber privaten Callcentern.

3.1.3.2 Recht auf Berichtigung

Die Berichtigung unrichtiger personenbezogener Daten bei nichtöffentlichen Stellen ist durch § 35 Abs. 1 Satz 1 BDSG vorgeschrieben. Nunmehr enthält Satz 2 des § 35 Abs. 1 BDSG die Verpflichtung, geschätzte Daten als solche in deutlicher Weise zu kennzeichnen.

Als notwendig erweist sich der Berichtigungsanspruch deshalb, weil die Speicherung unrichtiger personenbezogener Daten das informationelle Selbstbestimmungsrecht des Betroffenen massiv verletzen kann.[345]

[342] *Hoss*, RDV 2011, 6 (9); *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 172.
[343] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 34 Rn. 16; *Hoss*, RDV 2011, 6.
[344] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 34 Rn. 6 f; *Hoss*, RDV 2011, 6.
[345] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 110.

Der Begriff „unrichtig“ umfasst sämtliche Fälle, in denen personenbezogene Daten gespeichert werden, die mit der Realität nicht übereinstimmen; dies bedeutet konkret, dass sowohl falsche (beispielsweise ein nicht zutreffendes Geburtsdatum) als auch unvollständige Angaben darunter zu subsumieren sind.[346] Die verantwortliche Stelle muss entsprechende Daten richtigstellen, und zwar unabhängig davon, ob Betroffene dies begehren. Unter „Berichtigung“ ist zu verstehen, dass die Daten in Einklang mit der Realität gebracht werden.[347]

Die Notwendigkeit zur Kennzeichnung geschätzter Daten ist in der Vorschrift des § 20 Abs. 1 BDSG, der den Berichtigungsanspruch gegenüber öffentlichen Stellen regelt, nicht enthalten. Der Berichtigungsanspruch selbst trägt denselben Wortlaut wie der aus § 35 Abs. 1 BDSG.

3.1.3.3 Recht auf Löschung

Gemäß § 3 Abs. 4 Satz 2 Nr. 5 BDSG ist unter dem Vorgang der Löschung das Unkenntlichmachen gespeicherter personenbezogener Daten zu verstehen. Unter „Unkenntlichmachen“ sind Vorgänge zu fassen, die gewährleisten, dass irreversibel keinerlei Informationen mehr aus Daten gewonnen werden können.[348]

§ 35 Abs. 2 BDSG enthält Löschungsansprüche der Kunden gegenüber privatrechtlichen Callcentern. Die personenbezogenen Daten können nach Satz 1 grundsätzlich jederzeit gelöscht werden. Ausgenommen von dieser Option sind Daten, für die gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten gelten, sowie Daten, deren Löschung voraussichtlich zu einer Beeinträchtigung der schutzwürdigen Belange von Betroffenen führt.

In § 35 Abs. 2 Satz 2 BDSG finden sich die Löschungspflichten der verantwortlichen Stelle. Personenbezogene Daten sind im Zusammenhang mit dem Gesprächsmanagement-System insbesondere zu löschen, falls einer der enumerativ aufgezählten Sachverhalte vorliegt:

- Die Daten sind unzulässig gespeichert. Dies ist besonders dann der Fall, wenn keine entsprechende Rechtsgrundlage oder Einwilligung des Betroffenen existiert, oder wenn eine diesbezügliche Einwilligung im Nachhinein

[346] *Wedde*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.4 Rn. 55 ff.
[347] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 35 Rn. 9 ff.
[348] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 40; Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 3 Rn. 174.

widerrufen wurde. Umgekehrt führt jedoch eine nachträgliche Einwilligung – im Sinne einer Genehmigung – dazu, dass die anfänglich unzulässig gespeicherten Daten nicht mehr der Löschungspflicht unterliegen.[349]

- Besonders schützenswerte Daten sind betroffen, deren Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann. Umfasst werden Angaben zur rassischen oder ethnischen Herkunft, politischen Einstellung, religiösen oder philosophischen Überzeugung, Gesundheit, Gewerkschaftszugehörigkeit, zum Sexualleben, zu strafbaren Handlungen sowie Ordnungswidrigkeiten. Datenverarbeiter dürfen nicht mit auf Vermutungen basierenden Daten umgehen, die ein erhebliches Diskriminierungsrisiko des Betroffenen beinhalten.[350]
- Die Kenntnis der personenbezogenen Daten ist zur Erfüllung des Zwecks, wofür sie erhoben wurden, nicht mehr erforderlich, falls die Daten für eigene Geschäftszwecke verarbeitet werden. Ob ihre Kenntnis weiterhin erforderlich ist, lässt sich anhand der Vorschrift des § 28 BDSG bestimmen.[351] Die Berechtigung, Daten weiterhin zu speichern, obwohl sie zur ursprünglichen Zweckerreichung nicht mehr erforderlich sind, kann sich aus der potenziellen Abwehr von Haftungsansprüchen ergeben. Dies muss einzelfallabhängig festgestellt werden und gilt allenfalls dann, wenn derartige Ansprüche höchstwahrscheinlich zu erwarten sind.[352]

Öffentlich-rechtliche Callcenter-Betriebe müssen die im Gesprächsmanagement-System gespeicherten personenbezogenen Daten demgegenüber löschen, wenn sie

- unzulässig gespeichert oder
- zur Aufgabenerfüllung nicht mehr erforderlich sind.

Eine verbotene Speicherung kann sich aufgrund einer fehlenden Rechtsgrundlage oder einer nicht ausreichenden Legitimation aus einer Einwilligung ergeben. Ferner erstreckt sich die Löschungspflicht auf personenbezogene Daten, die in Zukunft für die Aufgabenerfüllung der öffentlichen Stelle keine praktische Bedeutung mehr besitzen werden.[353]

[349] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 35 Rn. 11; Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 35 Rn. 26.
[350] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 35 Rn. 27 ff.
[351] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 35 Rn. 35.
[352] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 35 Rn. 13a; Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 35 Rn. 38.
[353] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 20 Rn. 10 f.; zum Konflikt zwischen Aktenvollständigkeit und Datenschutz *Riegel*, NJW 1984, 2194 f.

3.1.3.4 Recht auf Sperrung

Der Begriff des Sperrens beinhaltet nach § 3 Abs. 4 Satz 2 Nr. 4 BDSG die Kennzeichnung gespeicherter personenbezogener Daten, um deren weitere Verarbeitung oder Nutzung zu beschränken.

Gemäß § 35 Abs. 3 BDSG sind die Daten in privatrechtlichen Callcentern zu sperren – anstatt zu löschen –, soweit nach

- Nr. 1 in bestimmten Fällen gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen der Löschung entgegenstehen oder
- Nr. 2 eine Beeinträchtigung schutzwürdiger Interessen zu befürchten ist oder
- Nr. 3 eine Löschung aufgrund der besonderen Art der Speicherung nicht oder nur mit einem unverhältnismäßigen Aufwand zu bewerkstelligen wäre.[354]

Wenn personenbezogene Daten für eigene Zwecke verarbeitet werden, ihre weitere Speicherung zur Zweckerfüllung jedoch nicht mehr notwendig ist, sind sie für den Fall zu sperren, dass bestimmte Archivierungspflichten bestehen. Wann schutzwürdige Interessen überwiegen, lässt sich pauschal nicht ausmachen; es ist vielmehr eine einzelfallabhängige Prüfung erforderlich, ob aus der Löschung für den Betroffenen erhebliche Nachteile resultieren. Um betriebswirtschaftlich unverhältnismäßige Kosten zu verhindern, soll in gewissen Fällen eine Sperrung der Daten ausreichen. Die Vorschrift ist allerdings sehr eng, zu Gunsten der Löschungspflicht auszulegen.[355]

Auch für den Fall, dass der Betroffene die Richtigkeit der Daten bestreitet, muss eine Sperrung gemäß § 35 Abs. 4 BDSG vorgenommen werden, wenn weder die Richtigkeit noch die Unrichtigkeit ermittelt werden kann. Dazu ist es erforderlich, dass der betroffene Kunde die Richtigkeit bestreitet und sich nach Ausschöpfung der Beweismittel nicht ermitteln lässt, wer Recht hat. Daten sind ferner auch dann zu sperren, wenn sich Angaben einer bestimmten Person nicht eindeutig zurechnen lassen, diese Informationen – auf die Person bezogen – also unter Umständen falsch sind.[356] Werden Daten gesperrt, darf eine Übermittlung dieser Tatsache gemäß Abs. 4a nicht erfolgen.

[354] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 110.
[355] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 35 Rn. 48 ff.
[356] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 35 Rn. 51 f.

Die Rechtsfolge der Sperrung ergibt sich aus §§ 3 Abs. 4 Satz 2 Nr. 4 und 35 Abs. 8 BDSG: Sie besteht generell in der Einschränkung weiterer Nutzungen oder Verarbeitungen der Daten. Nur in bestimmten Ausnahmefällen oder bei Vorliegen einer Einwilligung können die Daten übermittelt oder genutzt werden.[357]

Der Löschungsanspruch hinsichtlich personenbezogener Daten gegenüber öffentlichen Callcenter-Betrieben findet sich in § 20 Abs. 3 BDSG und entspricht nahezu der Vorschrift des § 35 Abs. 3 BDSG. Der einzige Unterschied liegt in der Sperrpflicht in Bezug auf sämtliche personenbezogenen Daten, für die Aufbewahrungsfristen existieren – und nicht nur bezüglich derjenigen, die zu eigenen Zwecken verarbeitet werden und deren Kenntnis für die Zweckerreichung der Speicherung nicht mehr notwendig ist.

Für den sogenannten Non-liquet-Fall, den § 20 Abs. 4 BDSG für öffentliche Stellen regelt, gelten die Ausführungen zu § 35 Abs. 4 BDSG analog. Was die Rechtsfolge der Sperrung anbelangt, so ist der Ausnahmetatbestand des § 20 Abs. 7 BDSG im Wortlaut identisch mit dem des § 35 Abs. 8 BDSG.[358]

3.1.3.5 Recht auf Widerspruch

Ein weiteres Einwirkungsrecht des Betroffenen besteht im Widerspruchsrecht. Soweit der Betroffene der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten widerspricht und darüber hinaus ein überwiegendes Interesse am Ausschluss dieser Vorgänge darlegen kann, darf nach § 35 Abs. 5 BDSG ein Umgang mit den Daten nicht erfolgen. Bei einer bestehenden gesetzlichen Verpflichtung der Stelle zur Erhebung, Verarbeitung oder Nutzung der Daten kann ausnahmsweise kein Widerspruch eingelegt werden.

Will der Betroffene sein Widerspruchsrecht wahrnehmen, hat er substanziiert vorzubringen, warum sein schutzwürdiges Interesse gegenüber dem Verarbeitungsinteresse der verantwortlichen Stelle überwiegt; diese Abwägung ist unter strengen Maßstäben zu vollziehen. Im Rahmen der Interessenabwägung wird das Callcenter unter Umständen auch Nachweise verlangen können. Ist der Widerspruch berechtigt, darf mit den personenbezogenen Daten mit Wirkung für die Zukunft nicht mehr umgegangen werden.[359]

---

[357] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 35 Rn. 30.
[358] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 20 Rn. 57 ff.
[359] Simitis/*Dix*, BDSG, 7. Aufl. 2011, § 35 Rn. 56; ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 35 Rn. 10; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 35 Rn. 27 f.; *Gola*, DuD 2001, 278.

Personenbezogene Daten, für die trotz potenziellem Widerspruch eine Erhebung, Verarbeitung oder Nutzung vorgeschrieben ist, sind im Regelfall solche, die an staatliche Stellen zu übermitteln oder für diese bereitzuhalten sind.[360]

§ 20 Abs. 5 BDSG regelt das Widerspruchsrecht gegenüber öffentlichen Einrichtungen. Die Vorschrift ist in ihrem Wortlaut deckungsgleich mit der des § 35 Abs. 5 BDSG.

Ferner bleibt ein weiteres – allerdings nicht ausdrücklich manifestiertes – Widerspruchsrecht zu beachten. Es handelt sich um die Möglichkeit, einer auf Grundlage einer Einwilligung basierenden Datenverarbeitungserlaubnis zu widersprechen. Die Rücknahme einer entsprechenden Einwilligung bewirkt, dass jeglicher Datenumgang ex nunc rechtswidrig wird. Ein solcher Widerruf ist insofern an weniger strenge Voraussetzungen gebunden, als das Vorbringen besonderer, der Verarbeitung zuwiderlaufender Interessen im Regelfall nicht vorausgesetzt wird.[361]

3.1.3.6 Recht auf Schadenersatz

Entsteht dem Betroffenen ein Schaden, der aus einer unzulässigen oder unrichtigen Verarbeitung seiner Daten resultiert, ist die nichtöffentliche verantwortliche Stelle oder deren Träger gemäß § 7 BDSG zum Ersatz dieses Schadens verpflichtet. Die Haftung ist nicht auf eine Höchstsumme begrenzt und erfasst gleichermaßen die automatisierte wie die nichtautomatisierte Verarbeitung von personenbezogenen Daten.[362]

Die Verpflichtung des Callcenters auf Leistung von Schadenersatz besteht nach Satz 2 des § 7 BDSG nicht, soweit es den gebotenen Sorgfaltsmaßstab bei der Ausübung seiner Tätigkeit eingehalten hat. Der Callcenter-Betrieb muss lediglich den Nachweis erbringen, dass der Schaden trotz Einhaltung aller im konkreten Fall notwendigen Maßnahmen zur gesetzeskonformen Verwendung der personenbezogenen Daten entstanden ist.[363] Hält er sich an die zu gewährleistenden technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und dessen Anlage, wird im Regelfall anzunehmen sein, dass die erforderliche Sorgfalt gewahrt wurde.[364]

---

[360] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 35 Rn. 29.
[361] *Gola*, DuD 2001, 278 (279).
[362] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, 417 f.; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 7 Rn. 4.
[363] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 7 Rn. 24.
[364] *Wedde*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.4 Rn. 92.

Anders ist die Situation bei öffentlichen Callcentern: § 8 Abs. 1 BDSG enthält eine verschuldensunabhängige Schadenersatzverpflichtung. Falls ein Schaden eintritt, haftet das Callcenter im Rahmen der Gefährdungshaftung. Abs. 2 der Vorschrift sieht – weitergehend als der Schadenersatzanspruch gegenüber nichtöffentlichen Stellen aus § 7 BDSG – vor, dass sich die Ersatzpflicht auch auf immaterielle Schäden erstreckt. Erleidet ein Betroffener eine erhebliche Verletzung seines Persönlichkeitsrechts, so löst auch dies Schadenersatzansprüche aus.

Einen möglichen Schutz vor solchen Ansprüchen bieten Haftpflicht- und Rechtsschutzversicherungen. Sie mindern das Risiko, sich durch möglicherweise unbeabsichtigte unzulässige Datenverarbeitungen in eine finanzielle Notlage zu manövrieren.[365] Als sinnvoll kann sich im Übrigen die Dokumentation sämtlicher personenbezogener Datenverarbeitungsprozesse erweisen, mit der sich unter Umständen der Gegenbeweis des Nichtverschuldens antreten lässt.[366] Fraglich bleibt in diesem Zusammenhang, ob diese Dokumentation mit einem verhältnismäßigen Aufwand überhaupt durchgeführt werden kann.

3.1.4 Geeignete Methoden zur sicheren Authentifizierung der Kunden

Da in Gesprächen zwischen den Kunden und den Callcenter-Agenten in der Regel personenbezogene Daten übermittelt werden, beispielsweise im Gesundheitsbereich sogar besonders schützenswerte personenbezogene Daten betroffen sind, ist es für bestimmte Anwendungsszenarien unumgänglich, sichere Methoden zur Authentifizierung der Kunden anzuwenden.[367] Damit wird einerseits gewährleistet, dass nur Berechtigte Zugang zu den Telefondienstleistungen erlangen und ein eventuell vorhandenes Rechtemanagement die korrekte Zuweisung der zugehörigen Berechtigungen zu den jeweiligen Kunden realisieren kann. Andererseits lässt sich eine fehlerhafte Zuordnung der im Gespräch anfallenden Kundendaten zu einem anderen Kunden vermeiden; ein solches Problem kann entstehen, wenn mehrere Kunden – womöglich noch aus demselben Ort – denselben Namen tragen. Nach § 35 Abs. 1 Satz 1 oder § 20 Abs. 1 Satz 1 BDSG sind derartige fehlerhafte Zuordnungen zu berichtigen.[368] Der Zweck der CRM-Datenbank besteht darin, kundenbezogene Sachverhalte den jeweiligen Kunden zugeordnet zu speichern. Gerade dazu ist es erforderlich, Gewissheit darüber zu haben, mit welchem Kunden der Callcenter-Agent kommuniziert.

[365] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 7 Rn. 49 ff.
[366] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 7 Rn. 2.
[367] So auch *Gola*, Datenschutz im Call Center, 2. Aufl. 2006, 105 f.
[368] Dazu Kapitel 3.1.3.2 „Recht auf Berichtigung“.

Generell existieren unterschiedlichste Authentisierungsmethoden[369], wovon die meisten zum Identitätsnachweis und zur Autorisierung der Kunden über eine Telefonverbindung allerdings nicht eingesetzt werden können. Nachfolgend sind beispielhaft potenziell geeignete Methoden kurz dargestellt.

Eine einfache Möglichkeit zur Wiedererkennung von Kunden besteht in der Vergabe individueller Persönlicher Identifikationsnummern (PINs), die den einzelnen Kunden zugeordnet sind und die bei jedem Anmeldevorgang mitgeteilt werden müssen. Diese Variante birgt jedoch hohe Sicherheitsrisiken in sich; jeder, der sich Kenntnis über die PIN verschaffen kann und alle weiteren zur Authentifizierung notwendigen Informationen (etwa den Namen der Person) kennt, ist grundsätzlich in der Lage, sich als die der PIN zugeordnete Person auszugeben.

Einmalpasswörter, sogenannte Transaktionsnummern (TANs), ermöglichen im Zusammenhang mit einer PIN zusätzlichen Schutz. Ihr Einsatz erfolgt häufig beim Onlinebanking. Eine TAN erlaubt die einmalige Vornahme einer Aktion; danach verfällt sie und kann für weitere Vorgänge nicht mehr genutzt werden. Sie ist nur gültig in Bezug auf die PIN und eine konkrete Aktion. TANs liegen beim Kunden listenförmig vor und bergen daher prinzipiell dieselben Risiken in sich wie PINs. Beide Sicherungsmittel setzen auf den Aspekt Wissen und können daher in die Hände Unberechtigter gelangen. Um dieser Gefahr entgegenzuwirken, wurde das TAN-Verfahren im Laufe der Zeit modifiziert.[370]

Zu einer signifikant höheren Sicherheit kann beispielsweise die sogenannte Zwei-Faktor-Authentifizierung führen. Ihr Konzept setzt auf zwei unterschiedliche Elemente, namentlich auf Wissen und Sein. Das erste Element kann in einer PIN bestehen, während das zweite ein biometrisches Merkmal verkörpert. Insbesondere für Callcenter-Anwendungen bieten sich Lösungen an, die neben einer gültigen PIN die zugehörige Stimme des Kunden fordern. Die Missbrauchsmöglichkeit einer solchen Authentifizierungsmethode ist als gering einzuschätzen.[371]

Für bestimmte Anwendungsfälle muss darüber hinaus sichergestellt sein, dass der Callcenter-Agent selbst die PIN und TAN nicht zur Kenntnis nehmen kann. Eine

[369] Zur Frage der Eignung von qualifizierten elektronischen Signaturschlüssel- und Attributszertifikaten zum Identitätsnachweis ausführlich *Bösing*, Authentifizierung und Autorisierung im elektronischen Rechtsverkehr, 2005.
[370] Beim Mobile-TAN beispielsweise wird die TAN vom Dienstleister direkt auf das Mobiltelefon des Kunden gesendet.
[371] Angeboten wird eine solche Authentifizierungstechnik beispielsweise von der *VOICETRUST AG*, (http://www.voicetrust.de/de/zwei-faktor-authentifizierung.html); generell zur Eignung biometrischer Authentisierungsverfahren *Eckert*, IT-Sicherheit, 6. Aufl. 2009, 468 ff.

visuelle oder akustische Anzeige, ob PIN und TAN richtig sind, reicht vollkommen aus. Die Passworteingabe durch den Kunden lässt sich beispielsweise mittels Tastenfeld des Telefons vollziehen.

Zusammenfassend bleibt festzuhalten, dass die Notwendigkeit und das zu gewährleistende Sicherheitsniveau einer Authentifizierung einzelfallabhängig zu ermitteln sind. Die erforderliche Absicherung kann je nach Aufgabengebiet des Callcenters stark variieren: So sind an eine telefonische Bankkontoverwaltung selbstverständlich höhere Sicherheitsanforderungen zu stellen als an ein Callcenter, das Beschwerdemanagement betreibt. Generell gilt, dass mit wachsender Schutzwürdigkeit der Daten die Anforderungen an eine sichere Authentifizierungsmethode steigen.

3.2 Weitere Vorgaben zum Kundenschutz

Neben dem Datenschutzrecht existieren weitere rechtliche Vorgaben zum Schutz der Kunden, die es im Callcenter-Umfeld zu beachten gilt. Diese werden nachfolgend dargestellt.

3.2.1 Verbot von Werbeanrufen ohne Einwilligung

Unternehmen – speziell die der Werbewirtschaft – besitzen großes Interesse daran, ihre Werbebotschaft an ein möglichst großes Kundenpotenzial heranzutragen, um somit den Absatz der beworbenen Güter und Dienstleistungen zu erhöhen. Dazu bedienen sie sich häufig des Kommunikationsmediums Telefon.[372] Die telefonische Direktansprache ist jedenfalls ein einfaches, kostengünstiges und zeiteffizientes Instrument, potenziellen Kunden ein erstes Angebot zu unterbreiten.[373] Auch die Rückgewinnung von Kunden mittels telefonischer Kontaktaufnahme stellt eine nachvollziehbare Zielsetzung von Unternehmen dar.[374]

Für die Angerufenen bedeutet ein solches Vorgehen der Unternehmen in den meisten Fällen eine erhebliche Belästigung. Darüber hinaus besteht auch die konkrete Gefahr, in solchen Situationen zu – für den Kunden unvorteilhaften – Geschäftsabschlüssen gedrängt zu werden.[375] Aus genannten Gründen blieb der Gesetzgeber diesbezüglich nicht untätig und schuf das Gesetz zur Bekämpfung unerlaubter Tele-

[372] *Lettl*, GRUR 2000, 977.
[373] *Pauly/Jankowski*, GRUR 2007, 118 (122).
[374] *Lettl*, GRUR 2000, 977.
[375] *Hecker*, K&R 2009, 601.

fonwerbung[376], das am 4. August 2009 in Kraft treten konnte. Das Gesetz sieht Änderungen im Gesetz gegen den unlauteren Wettbewerb, im Bürgerlichen Gesetzbuch, in der BGB-Informationspflichten-Verordnung sowie im Telekommunikationsgesetz vor, die sämtlich dem Schutz der Verbraucher dienen sollen. Die Vorschriften befassen sich mit unerlaubten Werbeanrufen (sogenannte Cold Calls), unerwünschten Vertragsabschlüssen sowie der Pflicht zur Rufnummerübermittlung.

Die wettbewerbsrechtliche Neuerung betrifft das vorherige Einwilligungserfordernis für telefonische Direktmarketingmethoden und den mit ihm zusammenhängenden Ordnungswidrigkeitentatbestand.[377] Reichte vor der Gesetzesänderung die konkludente Einwilligung in Werbeanrufe aus, ist nun ein ausdrückliches Einverständnis erforderlich. Insofern wurde die Gesetzeslage zu Gunsten des Verbraucherschutzes verschärft.[378] Das Verbot des telefonischen Kontakts erstreckt sich jedoch nicht auf bereits mit dem Kunden bestehende Vertragsverhältnisse, wenn mit dem Anruf beispielsweise eine vertragliche Nebenpflicht erfüllt wird.[379]

Gemäß § 7 Abs. 2 Nr. 2 UWG handelt es sich bei Werbeanrufen ohne entsprechende vorausgegangene ausdrückliche Einwilligung des Verbrauchers um eine unzumutbare Belästigung, die i. V. m. Abs. 1 unzulässig ist. Bei anderen Marktteilnehmern als Verbrauchern muss mindestens eine mutmaßliche Einwilligung anzunehmen sein; eine solche setzt die Vermutung voraus, dass der Angerufene mindestens aufgrund konkreter Umstände ein Interesse an dem Werbeanruf hat.[380]

Grundsätzlich gilt § 4a Abs. 1 BDSG auch als Maßstab für die Wirksamkeit von Einwilligungserklärungen in Bezug auf Werbeanrufe. Soll das Einverständnis in den Empfang von Werbeanrufen mündlich ergehen, ist durch § 28 Abs. 3a Satz 1 BDSG vorgesehen, dass die Einwilligung vom Callcenter schriftlich bestätigt werden muss.[381] Dies ermöglicht dem Betroffenen zu prüfen, ob das Callcenter die Einwilligung korrekt dokumentiert hat.[382] Nicht ausreichend jedenfalls ist die Auf-

[376] Gesetz zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen, v. 29.7.2009, BGBl. I S. 2413.
[377] *Hecker*, K&R 2009, 601 (604).
[378] *Ohly*, in: Piper/Ohly/Sosnitza, UWG, 5. Aufl. 2010, § 7 Rn. 6; *Köhler*, NJW 2009, 2567 (2568); *Tonner/Reich*, VuR 2009, 95 (101); *von Wallenberg*, BB 2009, 1768.
[379] BT-Drs. 16/10734, 13; *Hecker*, K&R 2009, 601 (604).
[380] *Plath/Frey*, BB 2009, 1762 (1765); *Gola/Reif*, in: *Gesellschaft für Datenschutz und Datensicherheit e. V./ Zentralverband der deutschen Werbewirtschaft e. V.* (Hrsg.), Kundendatenschutz, 3. Aufl. 2011, Rn. 375; *Haug*, K&R 2010, 767.
[381] *Plath/Frey*, BB 2009, 1762 (1766); BT-Drs. 16/12011, 29; *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535 (537); eine telefonische Einwilligung setzt voraus, dass der Einwilligende den Anruf getätigt hat, ansonsten liegt ein Verstoß gegen § 7 Abs. 2 Nr. 2 UWG vor; so auch *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 44.
[382] BT-Drs. 16/12011, 29 f.

zeichnung – nach diesbezüglicher Einwilligung – einer über das Telefon getätigten Einwilligung und das Bereithalten dieser Erklärung zum jederzeitigen Abhören für den Kunden.[383] Falls die Einwilligung elektronisch abgegeben wird, ist ihre Protokollierung erforderlich, und der Kunde muss sie jederzeit ab- und widerrufen können.

Darüber hinaus besteht gemäß § 28 Abs. 3b BDSG ein Kopplungsverbot, welches untersagt, den Vertragsschluss von einer Einwilligung in Werbeanrufe abhängig zu machen, wenn gleichwertige Leistungen anderswo ohne Einwilligung nicht oder nur in nicht zumutbarer Weise in Anspruch genommen werden können; ein derart erzwungenes Einverständnis wäre nicht rechtswirksam.

Aus § 20 UWG ergibt sich eine Ordnungswidrigkeit, wenn vorsätzliche oder fahrlässige Verstöße gegen das aus § 7 Abs. 1 i. V. m. Abs. 2 Nr. 2 UWG resultierende Verbot der Werbung durch Telefonanrufe gegenüber Verbrauchern bei gleichzeitigem Fehlen einer entsprechenden Einwilligung vorliegen. Die Geldbuße in einem solchen Fall kann bis zu 50.000 Euro betragen. Zuständige Verwaltungsbehörde ist die Bundesnetzagentur. Täter im Sinne des § 20 UWG ist der Werbende; dies können der Auftraggeber, für den das Callcenter wirbt, der Betreiber des Callcenters und der Callcenter-Agent selbst sein.[384]

Praktische Konsequenzen für Callcenter ergeben sich insoweit, als sie eine sorgsame und stets aktuelle Dokumentation der Einwilligungserklärungen vorzunehmen haben.[385] Stellt der Auftraggeber dem Callcenter eine Liste mit Rufnummern bereit, sollte der Callcenter-Betreiber in den Fällen, in denen den Umständen nach berechtigte Zweifel an der Rechtmäßigkeit der Liste bestehen, prüfen, ob tatsächlich Einwilligungserklärungen in Bezug auf sämtliche Telefonnummern erstens erteilt und zweitens auch nicht zwischenzeitlich widerrufen wurden.[386] Jedenfalls ist der Auftraggeber unverzüglich darüber zu unterrichten.[387] Als denkbare Vorgehensweise kann die unter Vertragsstrafe gestellte Verpflichtung gelten, dass der Auftraggeber dem beauftragten Callcenter eine Liste mit Rufnummern, für die tatsächlich eine Einwilligung in Werbeanrufe vorliegt, zu übergeben hat.[388]

[383] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rn. 44.
[384] BT-Drs. 16/10734, 13; *Ohly*, in: Piper/Ohly/Sosnitza, UWG, 5. Aufl. 2010, § 20 Rn. 3; *von Wallenberg*, BB 2009, 1768 (1769).
[385] *Ohly*, in: Piper/Ohly/Sosnitza, UWG, 5. Aufl. 2010, § 20 Rn. 4.
[386] *Köhler*, NJW 2009, 2567 (2569).
[387] *Sutschet*, RDV 2004, 97 (98).
[388] *Köhler*, NJW 2009, 2567 (2569).

Aus Gründen der Vollständigkeit erfolgt der Hinweis, dass noch weitere Anspruchsgrundlagen gegen unzulässige Werbeanrufe existieren: So können Verbraucher auf Beseitigung, Unterlassung und Schadenersatz aus §§ 823 Abs. 1, 1004 analog BGB aufgrund Verletzung des allgemeinen Persönlichkeitsrechts klagen.[389] Ferner steht insbesondere Mitbewerbern, bestimmten Verbänden, weiteren qualifizierten Einrichtungen sowie den Industrie- und Handelskammern und den Handwerkskammern ein Anspruch auf Beseitigung, Unterlassung und Schadenersatz aus §§ 8 Abs. 3 Nr. 1 - 4, Abs. 1 und 9 Satz 1 UWG zu. Mit Ausnahme der Mitbewerber können die genannten Institutionen darüber hinaus einen Gewinnabschöpfungsanspruch aus § 10 UWG geltend machen.[390]

3.2.2 Regelungen beim Outsourcing von Callcenter-Dienstleistungen

Unter dem Begriff „Outsourcing" ist der verstärkte Trend zu fassen, Organisationsbereiche oder Aufgaben vollständig oder teilweise an externe, spezialisierte Dienstleister zu übertragen.[391] Das Grundprinzip des Outsourcings besteht in der Arbeitsteilung durch die Nutzung externer Ressourcen.[392]

Mit der Auslagerung bestimmter Aufgabenfelder können sich Unternehmen der Privatwirtschaft und die öffentliche Verwaltung[393] auf ihre jeweiligen Kernkompetenzen konzentrieren; damit lassen sich insbesondere Effizienzgewinne und Kosteneinsparungen innerhalb der Organisation realisieren.[394]

Beim Outsourcing von Callcenter-Dienstleistungen ist zwischen einer Auftragsdatenverarbeitung und einer Funktionsübertragung zu differenzieren. Die Feststellung, welche der beiden im konkreten Fall vorliegt, ist dabei keineswegs trivial, sondern lässt sich im Normalfall nur einzelfallabhängig vornehmen.[395] Das ausschlaggeben-

[389] *Köhler*, NJW 2009, 2567 (2568).
[390] BT.-Drs. 16/10734, 13; *Köhler*, NJW 2009, 2567 (2568).
[391] *Büllesbach/Rieß*, NVwZ 1995, 444.
[392] *Schwarz*, in: Hermes/Schwarz (Hrsg.), Outsourcing, 2005, 15 f.; DIN SPEC 1041 dient der standardisierten Gestaltung von Outsourcingprozessen, s. http://www.dinspec1041.de und *Klett/Hilberg*, CR 2010, 417 ff.
[393] Zu den Anforderungen an die Datenerhebung, -verarbeitung und -nutzung im Auftrag für öffentliche Stellen des Bundes ausführlich *Engelien-Schulz*, VR 2010, 361 ff.
[394] *Oecking/Westerhoff*, in: Köhler-Frost (Hrsg.), Outsourcing, 5. Aufl. 2005, 35 (37); *Rehberg*, Personalmagazin 11/2009, 63 (64); *Hoenike/Hülsdunk*, MMR 2004, 788; *Räther*, DuD 2005, 461 (462); *Jandach*, DuD 2001, 224; *Wronka*, RDV 2003, 132; *Klett/Hilberg*, CR 2010, 417; *Zerbst*, in: Schoolmann/Rieger (Hrsg.), Praxishandbuch IT-Sicherheit, 401 (402 f.); *Wöhe/Döring*, Einführung in die Allgemeine Betriebswirtschaftslehre, 23. Aufl. 2008, 145, sprechen von Rationalisierungsvorteilen durch Arbeitsteilung.
[395] *Plath/Frey*, BB 2009, 1762 (1767); *Vogel/Glas*, DB 2009, 1747 (1748).

de Kriterium stellt primär die Entscheidungsbefugnis über die Daten dar; sie begründet die datenschutzrechtliche Verantwortlichkeit. Auch muss die Konkretheit des Auftrags berücksichtigt werden: Beispielsweise je mehr Entscheidungsspielraum in Bezug auf die Erledigung des Auftrags aufseiten des Auftragnehmers vorhanden ist, desto wahrscheinlicher ist das Vorliegen einer – an strengeren Regelungen zu messenden – Funktionsübertragung.[396]

Wenn sich der Auftraggeber zur Durchführung seiner Datenverarbeitungsprozesse eines externen Hilfsorgans bedient, handelt es sich unter der Bedingung, dass die Art und der Umfang der Datenverarbeitung vom Auftraggeber genau vorgegeben werden und nach von ihm festgelegten Mustern erfolgen, um eine Auftragsdatenverarbeitung.[397] Geregelt ist sie in § 11 BDSG.

Im Bereich der Callcenter-Dienstleistungen sind verschiedene, auch in Kombination miteinander mögliche Konstellationen des Outsourcings denkbar: Zunächst kann ein Unternehmen ein eigenständiges, unternehmensfremdes Callcenter zur Übernahme des telefonischen Services beauftragen, wobei das Callcenter für mehrere Unternehmen gleichzeitig tätig zu sein vermag. Es ist auch möglich, dass ein Unternehmen zwar über ein eigenes Callcenter verfügt, welches bei seiner Aufgabenausführung jedoch auf einen anderen, unternehmensexternen Dienstleister zurückgreift. Die Speicherung von Kundendaten in einem CRM-System bei einem externen, spezialisierten Anbieter von CRM-Lösungen ist ein Beispiel hierfür.

Bei der Datenverarbeitung im Auftrag muss gemäß § 11 Abs. 1 Satz 1 BDSG gewährleistet sein, dass der beauftragte Dienstleister die Daten nur nach Anweisung seines Auftraggebers erhebt, verarbeitet oder nutzt. Der Auftraggeber übt insofern weiterhin die „Herrschaft“ über die Daten aus.[398] Darüber hinaus hat der Schwerpunkt der Beauftragung auf der praktisch-technischen Komponente zu liegen, und der Auftraggeber muss ohne Weiteres durch Weisungen auf die Auftragsdurchführung einwirken können.[399] Sind die genannten Voraussetzungen erfüllt, ist der Auftraggeber selbst für die Einhaltung der Datenschutzvorschriften verantwortlich. Die beauftragte Stelle muss insoweit als rechtliche Einheit mit ihrem Auftraggeber be-

[396] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 9; *Müglich*, CR 2009, 479 (481).
[397] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 11 Rn. 1; *Räther*, DuD 2005, 461 (465); *Polenz*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Rn. 47; *Gliss*, DSB 11/2008, 8 ff.; mit eigenem Ansatz zur Auslegung des Begriffs „Auftragsdatenverarbeitung“ *Elbel*, RDV 2010, 203 ff.; zu den EU-Standardvertragsklauseln im Zusammenhang mit der Auftragsdatenverarbeitung s. *Lensdorf*, CR 2010, 735 ff.
[398] *Brisch/Laue*, MMR 2009, 813 (817); *Wronka*, RDV 2003, 132; *Engelien-Schulz*, VR 2011, 1 (3).
[399] *Räther*, DuD 2005, 461 (465); *Engelien-Schulz*, VR 2010, 361 (362).

trachtet werden.[400] Betroffenenrechte, wie die Rechte auf Löschung, Berichtigung und Schadenersatz, sind gemäß § 11 Abs. 1 Satz 2 BDSG gegenüber dem Auftraggeber geltend zu machen. Falls der Betroffene fälschlicherweise das beauftragte Unternehmen für verantwortlich hält und ihm gegenüber seine Rechte wahrnehmen will, muss ihn der Auftragnehmer auf den Irrtum hinweisen und die Ansprüche des Betroffenen an den Auftraggeber weiterleiten.[401]

Aus § 11 Abs. 2 Satz 1 BDSG resultiert die auftraggeberseitige Verpflichtung, den künftigen Auftragnehmer sorgfältig auszuwählen. Im Rahmen dieses Auswahlprozesses sollen die getroffenen technischen und organisatorischen Maßnahmen des potenziellen Auftragnehmers besondere Beachtung finden, da auch Auftragsdatenverarbeiter die Voraussetzungen des § 9 BDSG sowie dessen Anlage zu erfüllen haben.[402] Die Erteilung des Auftrags bedarf der Schriftform und muss mindestens die in § 11 Abs. 2 Satz 2 Nr. 1 - 10 BDSG enthaltenen Bestandteile umfassen; es handelt sich also um eine nicht enumerative Aufzählung, die die gesetzlichen Mindestanforderungen an die Auftragsausgestaltung konkretisieren und zu höherer Rechtssicherheit führen soll.[403] So müssen Gegenstand und Dauer des Auftrags sowie Rückgabemodalitäten im Zusammenhang mit den an den Dienstleister übergebenen Datenträgern und Löschungsfristen zum Beispiel zwingend geregelt sein. Die Missachtung der Aufnahmepflicht von vorgeschriebenen Mindestinhalten ist nach § 43 Abs. 1 Nr. 2b BDSG bußgeldbewehrt.[404] Kontrollen zur Überprüfung, ob die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen ausreichen, sind sowohl vor Aufnahme der Datenverarbeitung als auch regelmäßig während dieser vom Auftraggeber durchzuführen und zu dokumentieren.[405]

Was den Umgang mit den Daten anbelangt, so ist der Auftragnehmer gemäß § 11 Abs. 3 BDSG streng an die Vorgaben seines Auftraggebers gebunden. Vermutet der Outsourcing-Dienstleister, dass die Datenverarbeitung rechtswidrig ist, hat er das

[400] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 11 Rn. 1.
[401] *Polenz*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Rn. 54.
[402] *Heckmann*, MMR 2006, 280 (282).
[403] *Vander*, K&R 2010, 292 (293); *Kühling/Bohnen*, JZ 2010, 600 (605); näher dazu *Hoeren*, DuD 2010, 688 ff.; zu den Zulässigkeitsvoraussetzungen für Unterauftragsverhältnisse, die von Auftragsdatenverarbeitern in einem anderen EU-Land eingegangen werden, *Moos*, CR 2010, 281 ff.
[404] *Hanloser*, MMR 2009, 594 (597).
[405] *Roßnagel*, NJW 2009, 2716 (2721); „Datenlecks“ beim Outsourcing-Dienstleister können dazu führen, dass Informationen unrechtmäßig in Hände Dritter gelangen und missbraucht werden. Eine Möglichkeit, solche undichten Stellen zu erkennen, bieten sogenannte Mystery-IDs; diese stellen fiktive Kundenadressen dar, denen tatsächlich existierende Kontaktadressen zugeordnet sind. Wird etwa eine telefonische Verbindung zu einer solchen Kontaktadresse aufgebaut, nimmt ein Mitarbeiter des Anbieters von Mystery-IDs den Anruf entgegen und identifiziert den Anrufer (*o. V.*, Direkt Marketing 12/2009, 01/2010, 22).

auslagernde Unternehmen unverzüglich darauf hinzuweisen. Der Auftragnehmer kann zwar personenbezogene Daten erheben, verarbeiten oder nutzen, dennoch trägt er grundsätzlich keine datenschutzrechtliche Verantwortung – bis auf diejenige, die aus den in § 11 Abs. 4 BDSG aufgezählten Vorschriften resultiert.[406] Diese betrifft zum Beispiel das Datengeheimnis, die notwendigen technischen und organisatorischen Maßnahmen, die Datenschutzkontrolle, die Aufsicht sowie bestimmte Bußgeld- und Strafvorschriften.

Eine Funktionsübertragung liegt demgegenüber vor, wenn dem Auftragnehmer bestimmte Aufgaben – so genügt bereits die Durchführung einer einzelnen Phase der Datenverarbeitung – zur selbstständigen Erledigung übertragen werden.[407] Besitzt das beauftragte Unternehmen beispielsweise Spielräume im Hinblick auf die konkrete Durchführung der Aufgaben, ist eine Funktionsübertragung anzunehmen.[408] Ein weiteres Indiz für das Vorliegen einer Funktionsübertragung ist das Eigeninteresse des Outsourcing-Dienstleisters an den Daten.[409] Eindeutiger ist die Situation, wenn eine selbstständige Aufgabenerledigung aufgrund fehlender Anweisungen und Vorgaben des Auftraggebers erfolgt; hier wird man von einer Funktionsübertragung ausgehen müssen.[410] Wenn also neben der reinen Datenverarbeitung auch die Aufgabe, für deren Erfüllung die Verarbeitung der Daten letztendlich notwendig ist, auf die externe Stelle ausgelagert wird, nimmt diese die Position der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG ein.[411] Die Übertragung der Daten an den beauftragten Dienstleister stellt mithin eine Datenübermittlung gemäß § 3 Abs. 4 Satz 2 Nr. 3 BDSG dar.[412] Der Auftragnehmer ist als Dritter im Sinne des § 3 Abs. 8 Satz 2 BDSG zu qualifizieren. Er hat die volle datenschutzrechtliche Verantwortung zu tragen.

Auch landesrechtlich ist die Auftragsdatenverarbeitung entsprechend der bundesgesetzlichen Vorgaben geregelt. Einige Landesdatenschutzgesetze schreiben vor, dass der Auftragnehmer, der für eine öffentliche Einrichtung tätig werden soll – falls er den landesdatenschutzrechtlichen Regelungen a priori nicht unterworfen ist – vertraglich zur Einhaltung der Gesetze verpflichtet werden muss. Darüber hinaus ist

[406] *Sutschet*, RDV 2004, 97 (98).
[407] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 11 Rn. 4; *Kramer/Herrmann*, CR 2003, 938 (939); *Vogel/Glas*, DB 2009, 1747 (1748).
[408] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 9.
[409] *Heghmanns/Niehaus*, wistra 2008, 161 (162 f.); *Wronka*, RDV 2003, 132 (133).
[410] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 9; *Müglich*, CR 2009, 479 (481).
[411] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 11 Rn. 2; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 9.
[412] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 9; *Bake/Blobel/Münch* (Hrsg.), Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, 3. Aufl. 2009, 65.

vertraglich festzulegen, dass der Auftragnehmer der Kontrolle durch den Landesbeauftragten für den Datenschutz unterliegt.[413]

Obwohl bei ausgelagerten Callcenter-Dienstleistungen in der weit überwiegenden Mehrheit zweifelsfrei eine Auftragsdatenverarbeitung[414] vorliegen wird, kann die Festschreibung – etwa auf vertraglicher Basis – durch Auftraggeber, Callcenter und gegebenenfalls weitere Auftragnehmer oder Unterauftragnehmer, wer die Verantwortung für Datenverarbeitungsprozesse trägt, die Rechtssicherheit aller Parteien erheblich erhöhen.

Das Gesprächsmanagement-System braucht nicht vollständig im Callcenter-Betrieb selbst eingerichtet zu werden, sondern dessen Komponenten können vielmehr auch an verschiedenen Orten stehen, die mittels Internet über eine Service-on-Demand-Architektur miteinander vernetzt sind, und die unterschiedliche Dienstleister verantworten und deren Betrieb sicherstellen. Daher ist einzelfallbezogen für jedes konkrete Implementierungsvorhaben des Gesprächsmanagement-Systems zu prüfen, welches Dienstleistungsunternehmen welche Stellung im Auftragsverhältnis einnimmt. Eine pauschale Einordnung, wer unter welchen Voraussetzungen an die Position des Auftraggebers, Auftragnehmers und gegebenenfalls Unterauftragnehmers tritt, lässt sich nicht vornehmen. Auch auf Unteraufträge ist die Regelung des § 11 BDSG anzuwenden. Die Berechtigung zur Begründung von Unterauftragsverhältnissen muss gemäß § 11 Abs. 2 Satz 2 Nr. 6 BDSG zwingend im Vertrag mit dem Auftragnehmer verankert sein.[415]

Nach § 10 Abs. 1 BDSG stellt die automatisierte Übermittlung personenbezogener Daten ein Abrufverfahren dar, für welches bestimmte Zulässigkeitsvoraussetzungen erfüllt sein müssen.

Die automatisierte Übertragung von Kundendaten aus dem CRM-System zum Frontend-System der Callcenter-Agenten verkörpert zum Beispiel im Grundsatz ein solches Abrufverfahren. § 10 BDSG gilt allerdings nicht für Dienstleister, die im Rahmen eines Auftragsverhältnisses für Callcenter Daten verarbeiten und bereitstellen, da in einer solchen Konstellation keine Beteiligung von Dritten im Sinne des §

[413] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 29; so etwa durch § 3 Abs. 4 BlnDSG und § 3 Abs. 3 HmbDSG.
[414] So auch BT-Drs. 16/12011, 40; *Sutschet*, RDV 2004, 97 ff., vertritt die Ansicht, dass Callcenter, die für andere Unternehmen tätig sind, stets nur die Stellung von Auftragsdatenverarbeiter im Sinne des § 11 BDSG einnehmen; diese Auffassung ist jedoch zu undifferenziert.
[415] *Hoeren*, DuD 2010, 688 (690).

3 Abs. 8 Satz 2 BDSG vorliegt.[416] Daher ist diese Vorschrift für den Betrieb des Gesprächsmanagement-Systems nicht relevant. Der Zusammenschluss der Stellen, die das System betreiben, wird in der Regel aus einer Mehrzahl von Auftragsverhältnissen bestehen.

[416] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 10 Rn. 3 ff.; *Hoeren*, NVwZ 2010, 1123 (1126), der einen Abruf erst dann als einen solchen qualifiziert, wenn er durch den Datenempfänger initiiert wurde.

4 Beschäftigtenbezogene Vorgaben

Der Schutz der Mitarbeiter ist durch zahlreiche Gesetze und Vorschriften geregelt. Verbindliche Vorgaben sind deshalb wichtig, um zu verhindern, dass Arbeitsverhältnisse zu Lasten der Beschäftigten gestaltet werden. In den seltensten Fällen wird von einer tatsächlichen Verhandlungsparität der Arbeitsvertragsparteien auszugehen sein. Dem Callcenter-Betreiber obliegen deshalb besondere Fürsorge- und Schutzpflichten. Der Schutzbedarf der Beschäftigten spiegelt sich allgemein unter anderem an den Vorschriften zum

- Arbeitszeitschutz,
- Frauenarbeits- und Mutterschutz,
- Betriebs- oder Gefahrenschutz,
- Jugendarbeitsschutz,
- Schwerbehindertenschutz,
- Lohnschutz sowie
- Heimarbeitsschutz

wider.[417]

Im Arbeitsrecht ist grundlegend zwischen Individual- und Kollektivebene zu unterscheiden. Die Individualebene gliedert sich in zwei Teile: einerseits in das Arbeitsvertragsrecht, welches die privatrechtliche Beziehung zwischen dem Arbeitgeber und den einzelnen Beschäftigten reglementiert, sowie andererseits in das Arbeitsschutzrecht, das sich ausdrücklich beispielsweise auf die oben genannten Bereiche erstreckt. Das Kollektivarbeitsrecht dagegen bezieht sich auf die Regelungen, die die arbeitsrechtlichen Kollektivorgane betreffen. Für privatwirtschaftliche Betriebe und Stellen des öffentlichen Dienstes wirkt das Kollektivrecht durch das Betriebsverfassungsgesetz beziehungsweise die Personalvertretungsgesetze. Auf überbetrieblicher und -behördlicher Ebene nehmen Gewerkschaften die Kollektivverantwortung für Beschäftigte wahr, die mittels Tarifverträgen auf die Gestaltung der Arbeitsverhältnisse einwirken.[418] Vorschriften des Kollektivarbeitsrechts können in Form von Gesetzen, Tarifverträgen und Betriebs- oder Dienstvereinbarungen bestehen. Hierarchisch betrachtet stehen Gesetze an oberster Stelle, vor Tarifverträgen.[419] Zwar findet sich das Regelungsinstrument Betriebs- oder Dienstvereinbarung auf der untersten Stufe wieder, dennoch kommt ihm eine erhebliche praktische Bedeu-

[417] MHA/*Richardi*, Band 1, 3. Aufl. 2009, § 4 Rn. 12.
[418] MHA/*Richardi*, Band 1, 3. Aufl. 2009, § 4 Rn. 14 ff.
[419] *Kilian*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Kollektivarbeitsrechtliche Probleme der Informationstechnologie im Betrieb, Rn. 12.

tung zu. Es ermöglicht, betriebs- oder dienststellenspezifisch auf die Ausgestaltung der Arbeitsverhältnisse – mit konkreten Bestimmungen etwa zur Nutzung der am Arbeitsplatz vorhandenen Technik – einzuwirken. Welche individual- und kollektivrechtlichen Regelungen in Bezug auf den Datenschutz der Callcenter-Mitarbeiter zu beachten sind, wird im Folgenden aufgezeigt.

4.1 Beschäftigtendatenschutz

Die seit Jahrzehnten geforderte „umfassende" gesetzliche Regelung des Beschäftigtendatenschutzes steht aktuell vor ihrer Verabschiedung. Als Schwierigkeit für die Praxis gilt die Tatsache, dass zu zahlreichen Fragestellungen im Hinblick auf den Beschäftigtendatenschutz bislang keine ausdrücklichen Vorschriften existieren. Die Rechtslage ergibt sich teilweise aus dem Zusammenwirken verschiedener allgemeiner Gesetze, wie dem Bundesdatenschutzgesetz und dem Betriebsverfassungsgesetz. Darüber hinaus bestehen essentielle Grundsätze für den Beschäftigtendatenschutz, die in Gerichtsentscheidungen entwickelt wurden. Die gesamte Rechtsmaterie ist im Regelfall aufgrund ihrer Komplexität für den einzelnen Beschäftigten kaum mehr zu durchschauen.[420]

Der Begriff „Beschäftigte" ist im Bundesdatenschutzgesetz in § 3 Abs. 11 BDSG legaldefiniert; unter ihn fallen insbesondere:

- Bewerber,
- Arbeitnehmer,
- in Bildungsmaßnahmen befindliche Tätige,
- Personen, die an Wiedereingliederungsmaßnahmen oder Aktivitäten zur Arbeitserprobung teilnehmen,
- Tätige aufgrund des Jugendfreiwilligendienstegesetzes,
- in Behindertenwerkstätten Tätige,
- arbeitnehmerähnliche Personen aufgrund ihrer wirtschaftlichen Unselbstständigkeit,
- Beamte, Richter des Bundes, Soldaten und
- Personen, mit denen ehemals ein Beschäftigungsverhältnis bestand.

An der umfassenden Reichweite des Terminus wird deutlich, dass damit nahezu sämtliche in Abhängigkeit tätige Beschäftigte erfasst sein sollen.[421]

[420] BT-Drs. 17/4230, 1.
[421] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 59a.

Innerhalb der Bearbeitungszeit der vorliegenden Arbeit traten mehrere Novellierungen[422] des Bundesdatenschutzgesetzes in Kraft, welche Berücksichtigung finden. Eine bedeutende Änderung trat am 1. September 2009 mit der Bundesdatenschutzgesetz-Novelle II[423] in Kraft: Mit Aufnahme des § 32 BDSG wurde der Beschäftigtendatenschutz im Bundesdatenschutzgesetz ausdrücklich festgeschrieben. Die Vorschrift des aktuellen § 32 BDSG stellt jedoch nichts anderes als die Willensbekundung des Gesetzgebers dar, den Beschäftigtendatenschutz in umfassender Form zeitnah auf den Weg zu bringen.

Perspektivisch gesehen werden vermutlich die Vorschriften der §§ 32 - 32l BDSG das Feld des Beschäftigtendatenschutzes konkreter und praxisgerechter als bislang reglementieren.[424] Der Gesetzgebungsprozess befindet sich zum Zeitpunkt der Abgabe der vorliegenden Arbeit in vollem Gange. Es besteht aktuell eine Vielzahl von Unklarheiten, die Nachbesserungen des Gesetzgebers erforderlich machen.

Die nachfolgenden Ausführungen zur Zulässigkeit des Umgangs mit personenbezogenen Daten der Mitarbeiter im Rahmen des Beschäftigungsverhältnisses richten sich nach der aktuellen Rechtslage. Darüber hinaus werden allgemein die einschlägigen Vorschriften des zukünftigen Beschäftigtendatenschutzes vorgestellt.

4.1.1 Zulässigkeit der Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten

Die Zulässigkeit des Umgangs mit personenbezogenen Daten der Beschäftigten durch den Arbeitgeber lässt sich auf verschiedene Erlaubnistatbestände stützen; diese Zulässigkeitsalternativen werden im Folgenden aufgezeigt.

Für öffentliche Stellen des Bundes gelten gemäß § 12 Abs. 4 BDSG – ebenso wie für nichtöffentliche Organisationen – die §§ 32 - 35 und § 28 Abs. 2 Nr. 2 BDSG. Die Vorgaben zum Beschäftigtendatenschutz sind also auch für Beschäftigte in diesem Bereich vollständig zu beachten. Was den Regelungsgegenstand des Beschäftigtendatenschutzes in den landesrechtlichen Bestimmungen anbelangt, so lässt sich konstatieren, dass der überwiegende Teil der Länder bereits seit langem umfassende

[422] BDSG-Novelle I zum 1.4.2010: BT-Drs. 16/13219, BT-Drs. 16/10529, BT-Drs. 16/10581; BDSG-Novelle II zum 1.9.2009 und 1.4.2010: BT-Drs. 16/13657, BT-Drs. 16/12011; BDSG-Novelle III zum 11.6.2010: BT-Drs. 16/11643.
[423] BT-Drs. 16/12011 und BT-Drs. 16/13657.
[424] BT-Drs. 17/4230, 1.

Gewährleistungen des Beschäftigtendatenschutzes im Rahmen ihrer Gesetzgebungskompetenzen geregelt hat.[425]

Durch § 12 Abs. 4 BDSG-E ist vorgesehen, dass der zukünftige Beschäftigtendatenschutz für Bundeseinrichtungen durch die §§ 32 - 34 Abs. 1 Satz 1 und 2, § 34 Abs. 6 - 8 Satz 1 sowie § 35 BDSG reglementiert sein soll.[426]

Aufgrund der Vielgestaltigkeit der jeweiligen landesrechtlichen Vorschriften zum Beschäftigtendatenschutz können diese Regelungen hier nicht dargestellt werden. Im Grundsatz lässt sich jedoch unterstellen, dass die Landesbestimmungen zu dieser Rechtsmaterie dasselbe Schutzniveau garantieren wie die des Bundesdatenschutzgesetzes. Zumindest für die Zukunft, das heißt nach der Neuregelung des Beschäftigtendatenschutzes auf bundesrechtlicher Ebene, ist zu erwarten, dass die Länder im Interesse der Rechtseinheitlichkeit durch Fortentwicklung ihrer jeweils gültigen Vorschriften zu einem einheitlichen Schutzstandard beitragen werden.[427]

4.1.1.1 Erlaubnis aus dem Bundesdatenschutzgesetz

4.1.1.1.1 Aktuelle Rechtslage

Die derzeitige Rechtslage sieht mit § 32 Abs. 1 Satz 1 BDSG vor, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses zulässig sind, wenn es für die

- Entscheidung über das Eingehen eines Beschäftigungsverhältnisses,
- Durchführung eines Beschäftigungsverhältnisses oder
- Beendigung eines solchen

erforderlich ist.

Diese Regelung präzisiert die bisherige Rechtfertigung für den Umgang mit Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG und verdrängt diese.[428] Die enge Zweckbegrenzung für den Bereich des Beschäftigtendatenschutzes schließt jedoch nicht aus, dass der Umgang mit Beschäftigtendaten zu anderen Zwecken als genannt zulässig ist; dieser kann bei-

[425] BR-Drs. 535/2/10, 8; so etwa in § 35 DSG M-V oder § 34 HDSG.
[426] BT-Drs. 17/4230, 5.
[427] BR-Drs. 535/2/10, 8.
[428] BT-Drs. 16/13657, 35.

spielsweise aufgrund „berechtigter Interessen“ des Arbeitgebers bei einer nichtöffentlichen Stelle gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt sein. Weiterreichende bereichsspezifische Datenschutzvorschriften werden durch den aktuellen § 32 BDSG genauso wenig verdrängt, wie die Möglichkeit der Einholung einer datenschutzrechtlichen Einwilligung aus § 4a BDSG nicht ausgeschlossen ist.[429]

Die Regelung des § 32 Abs. 1 Satz 1 BDSG ist jedenfalls dann einschlägig, wenn der Arbeitgeber seine vertraglichen Pflichten aus dem Arbeitsvertrag erfüllt. In diesem Zusammenhang bleibt die Datenverarbeitung zum Beispiel zur Lohnabrechnung und Personalverwaltung zulässig. Darüber hinaus besitzt der Arbeitgeber im Rahmen der Arbeitsvertragsbeziehung gewisse Befugnisse, wie das Weisungsrecht und das Recht, Verhalten oder Leistung seiner Mitarbeiter kontrollieren zu dürfen. Dies sind Handlungen, die im Sinne der Vorschrift als „erforderlich“ gelten.[430]

§ 32 Abs. 1 Satz 2 BDSG betrifft den besonderen Fall eines Verdachts, dass Straftaten innerhalb des Beschäftigungsverhältnisses durch Mitarbeiter begangen wurden. Die Vorschrift benennt die Voraussetzungen für die Erhebung, Verarbeitung oder Nutzung personenbezogener Beschäftigtendaten mit dem Zweck der Aufdeckung von Straftaten, die Mitarbeiter verübt haben.

Ein datenschutzrechtliches Novum besteht darin, dass gemäß § 32 Abs. 2 BDSG nicht nur automatisierte Datenverarbeitungsprozesse, sondern ebenso der nichtautomatisierte Umgang mit personenbezogenen Beschäftigtendaten durch den Arbeitgeber vom Schutzbereich des Beschäftigtendatenschutzes gedeckt ist, sofern er zum Zwecke des Beschäftigungsverhältnisses erfolgt. So können in Zukunft zum Beispiel handschriftliche Aufzeichnungen des Arbeitgebers in Bezug auf seine Mitarbeiter vom Datenschutzrecht erfasst sein.[431]

In § 32 Abs. 3 BDSG ist geregelt, dass die Beteiligungsrechte der Beschäftigtenvertretungen unberührt bleiben. So soll insbesondere das Recht des Betriebsrats aus § 87 Abs. 1 Nr. 6 BetrVG sowie das des Personalrats aus § 75 Abs. 3 Nr. 17 BPersVG, bei der Einführung und Anwendung bestimmter technischer Einrichtungen mitzubestimmen, nicht eingeschränkt werden.[432]

---

[429] BT-Drs. 16/13657, 35 f.; *Albrecht*, jurisPR-ITR 20/2009, 1 (2); *Maties*, RdA 2009, 261; *Timner/Schreier*, AuA Sonderausgabe 2010, 4.
[430] *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535 (538); BT-Drs. 16/13657, 36; *Löwisch*, DB 2009, 2782 (2785).
[431] *Bausewein*, DuD 2011, 94 ff.; kritisch hierzu *Franzen*, RdA 2010, 257 (258 f.); *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535 (539).
[432] BT-Drs. 16/13657, 37; *Albrecht*, jurisPR-ITR 20/2009, 1 (5).

4.1.1.1.2 Zu erwartende Rechtslage

Die zukünftig geltenden Regelungen zum Beschäftigtendatenschutz sind notwendig, da die aktuelle – und vorläufige – Vorschrift aufgrund ungeklärter Auslegungsspielräume und Fragen zu ihrer generellen Anwendbarkeit nach wie vor zur Rechtsunsicherheit in dieser Rechtsmaterie beiträgt.[433]

Aus dem Entwurf der Bundesregierung[434] zu dem in absehbarer Zeit in Kraft tretenden Beschäftigtendatenschutz geht hervor, dass dieses Rechtsgebiet sowohl nach verschiedenen Phasen des Beschäftigungsverhältnisses als auch nach dem Datenumgang differenziert geregelt werden soll: Es ist vorgesehen, jeweils eigenständige, allgemeine Vorschriften zur

- Daten*erhebung vor* Begründung des Beschäftigungsverhältnisses (§ 32 BDSG-E),
- Durchführung von Untersuchungen und Eignungstests *vor* Begründung des Beschäftigungsverhältnisses (§ 32a BDSG-E),
- Daten*verarbeitung* und *-nutzung vor* Begründung des Beschäftigungsverhältnisses
  (§ 32b BDSG-E),
- Daten*erhebung während des* Beschäftigungsverhältnisses (§ 32c BDSG-E),
- Daten*verarbeitung* und *-nutzung während des* Beschäftigungsverhältnisses (§ 32d BDSG-E) und
- Daten*erhebung* ohne Kenntnis des Beschäftigten zum Zweck der Prävention und Aufklärung von Straftaten und schwerer Pflichtverletzungen *während* des Beschäftigungsverhältnisses (§ 32e BDSG-E)

im Gesetz zu verankern.[435]

Mit den §§ 32f - 32i BDSG-E werden darüber hinaus voraussichtlich spezifische Regelungen, die den Einsatz von Videokameras, Ortungssystemen, biometrischen Verfahren sowie die Nutzung von Telekommunikationseinrichtungen im Beschäftigungsverhältnis betreffen, mit aufgenommen.[436]

Ebenso wie die derzeit gültige Regelung aus § 32 Abs. 2 BDSG den Beschäftigtendatenschutz nicht nur auf automatisierte Datenverarbeitungen beschränkt, ist es ge-

[433] *Mester*, DuD 2011, 79; *Tinnefeld/Petri/Brink*, MMR 2010, 727 (729).
[434] BT-Drs. 17/4230.
[435] BT-Drs. 17/4230, 6 ff.
[436] BT-Drs. 17/4230, 8 ff.

mäß § 27 Abs. 3 BDSG-E für den zukünftigen Beschäftigtendatenschutz vorgesehen.[437]

Der zukünftige § 27 Abs. 3 BDSG-E wird den Anwendungsbereich des Beschäftigtendatenschutzes regeln: Dieser gilt für Arbeitgeber im Sinne des künftigen § 3 Abs. 13 BDSG-E nur für die Datenerhebung, -verarbeitung oder -nutzung für Zwecke des Beschäftigungsverhältnisses. Erfolgt der Umgang mit Beschäftigtendaten zu anderen Zwecken, sind nicht die Vorschriften §§ 32 - 32l BDSG-E anwendbar, sondern die übrigen Vorschriften des Bundesdatenschutzgesetzes.[438]

Von besonderer Relevanz im Hinblick auf die Problemstellung der vorliegenden Arbeit ist § 32i BDSG-E, der die Nutzung von Telekommunikationsdiensten innerhalb des Beschäftigungsverhältnisses festschreibt. § 32i Abs. 1 BDSG-E regelt die Befugnis des Arbeitgebers, während des Telekommunikationsvorgangs mit den äußeren Rahmendaten der Telekommunikation[439] – etwa Nummern der beteiligten Anschlüsse und Dauer der Verbindung –umzugehen, soweit den Beschäftigten die Telekommunikation über die innerorganisatorische Kommunikationsanlage ausschließlich zu betrieblichen oder dienstlichen Zwecken gestattet ist. Der Arbeitgeber darf dies, soweit es erforderlich ist,

- den ordnungsgemäßen Betrieb von Telekommunikationsnetzen und -diensten sowie die Datensicherheit sicherzustellen,
- die Abrechnung der in Anspruch genommenen Dienste durchzuführen oder
- eine stichprobenhafte oder anlassbezogene Verhaltens- oder Leistungskontrolle zu realisieren.

Einschränkend ist jedoch zu berücksichtigen, dass keine Anhaltspunkte für überwiegende schutzwürdige Belange des Beschäftigten existieren dürfen. Diese können beispielsweise vorliegen, wenn anhand der Anschlussnummern für den Arbeitgeber erkennbar ist, dass ein bestimmter Mitarbeiter psychologische Unterstützung bei einer innerorganisatorischen Beratungsstelle sucht.[440] Im Fall einer personenbezogenen Verhaltens- oder Leistungskontrolle muss der betroffene Beschäftigte im Nachhinein – sobald durch die Unterrichtung keine Gefahr mehr für das Erreichen

[437] BT-Drs. 17/4230, 14.
[438] BT-Drs. 17/4230, 14.
[439] Aus dem Gesetzentwurf (s. BT-Drs. 17/4230, 42) ergibt sich, dass die „anfallenden Daten“ mit dem telekommunikationsrechtlichen Begriff „Verkehrsdaten“ deckungsgleich sind, der Terminus aber absichtlich, aufgrund einer klaren Unterscheidbarkeit zwischen erlaubter Privatnutzung und ausschließlich betrieblicher oder dienstlicher Nutzung der Telekommunikationsanlage, keine Verwendung findet.
[440] *Tinnefeld/Petri/Brink*, MMR 2010, 727 (733); BT-Drs. 17/4230, 20 f.

ihres Zwecks besteht – über eine solche in Kenntnis gesetzt werden.[441] Der Callcenter-Betreiber kann sein Kontrollrecht im Hinblick auf die äußeren Daten der Telekommunikation auf diese Vorschrift stützen.

Die Vorschrift des § 32i Abs. 2 BDSG-E hat die Kontrolle der Kommunikationsinhalte zum Gegenstand, bei einem Telefonat also das Geäußerte. Sie bezieht sich auf den laufenden Telekommunikationsvorgang. Während Satz 1 eine Regelung enthält, die allgemein auf Beschäftigungsverhältnisse zutrifft, bei denen die Nutzung der Telekommunikationseinrichtungen ausschließlich zu beruflichen Zwecken gestattet ist, trägt Satz 2 der besonderen Situation in Callcentern Rechnung. Hier stellt die telefonische Dienstleistung den wesentlichen Inhalt der Arbeitsaufgabe dar. Dem Arbeitgeber ist es unter weiteren Voraussetzungen gestattet, die Inhalte der Telefongespräche zur Verhaltens- oder Leistungskontrolle, auch ohne Kenntnis des Beschäftigten, im Einzelfall zu erheben, zu verarbeiten oder zu nutzen. Dabei müssen die folgenden zwei Bedingungen erfüllt sein:

- Erstens hat im Vorfeld einer Kontrollmaßnahme die Information des jeweiligen Callcenter-Mitarbeiters zu erfolgen, dass er in einem zeitlich beschränkten Rahmen mit einer Überwachung der Telefonate rechnen müsse. Die zeitliche Einschränkung dient dazu, eine lückenlose Kontrolle zu verhindern, um keinen zu großen Druck auf die Beschäftigten auszuüben. Unverzüglich nach Durchführung der Maßnahme obliegt dem Arbeitgeber die Pflicht, den Mitarbeiter über die Kontrollvorgänge in Kenntnis zu setzen.
- Zweitens gilt es, die Kommunikationspartner der Callcenter-Agenten, also die Kunden, über die Möglichkeit der Kontrollen aufzuklären und – ein bedeutender Aspekt – ihre dahingehende Einwilligung einzuholen.[442] Das in Echtzeit stattfindende Mithören von Telefonaten durch den Callcenter-Betreiber wird von der Rechtsvorschrift des § 32i Abs. 2 BDSG-E erfasst.

§ 32i Abs. 4 BDSG-E betrifft den Umgang mit den Verbindungs- und Inhaltsdaten abgeschlossener Telekommunikationsvorgänge der Beschäftigten. Unter „Telekommunikation“ ist gemäß § 3 Nr. 22 TKG „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“ zu verstehen. Wurden die Signale übertragen, ist die Telekommunikation mit deren Empfang abgeschlossen. An der Vorschrift des § 32i Abs. 4 BDSG-E ist bei-

[441] *Tinnefeld/Petri/Brink*, MMR 2010, 727 (733); BT-Drs. 17/4230, 21; *Hilbrans*, AuR 2010, 424 (426).
[442] BT-Drs. 17/4230, 9, 21, 42; zur grundsätzlich zulässigen Möglichkeit, auf die Schriftform der Einwilligung im Zusammenhang mit Callcenter-Dienstleistungen zu verzichten, s. Kapitel 3.1.1.1.3 „Erlaubnis aus einer Einwilligung“.

spielsweise die „klassische Frage“ nach der Zulässigkeit der Einsichtnahme von auf dem Arbeitsplatzcomputer der Beschäftigten im elektronischen Postfach gespeicherten E-Mails durch den Arbeitgeber zu beurteilen.[443] Bezogen auf die Situation im Callcenter wird die Regelung relevant, wenn eine Auswertung der äußeren Umstände der Telekommunikation, die zum Beispiel in der Telefonanlage gespeichert sind, oder wenn eine Kenntnisnahme der Inhalte aufgezeichneter Telefongespräche stattfindet. Die Zulässigkeit des Datenumgangs richtet sich dabei nach den §§ 32c und 32d BDSG-E. Diese betreffen allgemein die Datenerhebung beziehungsweise die Datenverarbeitung und -nutzung im Beschäftigungsverhältnis.

Nach § 32c Abs. 1 Satz 1 BDSG-E ist die Datenerhebung für die Zwecke der Durchführung, Beendigung und Abwicklung des Beschäftigungsverhältnisses grundsätzlich erlaubt, wenn sie hierzu erforderlich ist. Diese Situation liegt gemäß § 32c Abs. 1 Satz 2 Nr. 3 BDSG-E insbesondere vor, wenn der Arbeitgeber seine Rechte aus dem Beschäftigungsverhältnis wahrnimmt und Verhaltens- oder Leistungskontrollen durchführt. Die Datenerhebung muss nach Abs. 4 in ihrer Form und ihrem Ausmaß bezüglich ihres Zwecks verhältnismäßig sein. Lückenlos angelegte Kontrollen durch den Callcenter-Betreiber scheiden somit aus. Darüber hinaus ist das Direkterhebungsgebot aus § 32c Abs. 1 Satz 3 i. V. m. § 32 Abs. 6 BDSG-E zu beachten, wonach die Datenerhebung direkt beim Beschäftigten stattzufinden hat.[444]

§ 32d Abs. 1 BDSG-E erlaubt dem Arbeitgeber grundsätzlich die Verarbeitung und Nutzung von Beschäftigtendaten, soweit sie unter anderem nach § 32c BDSG-E erhoben worden sind. Darüber hinaus müssen die Daten für die Zwecke erforderlich sein, für die sie erhoben worden sind, oder für andere Zwecke, für die eine Erhebung nach den Vorschriften des Beschäftigtendatenschutzes zulässig wäre. Ferner haben Art und Ausmaß der Datenverarbeitung und -nutzung verhältnismäßig zu sein. Abs. 5 des § 32d BDSG-E sieht vor, dass eine derartige automatisierte Zusammenführung einzelner Personal- und Lebensdaten von Beschäftigten verboten ist, bei der ein Profil der geistigen und charakterlichen Eigenschaften entsteht.[445]

Bei näherer Betrachtung der dargestellten Normen fällt auf, dass die äußeren Rahmendaten und die Inhaltsdaten nach Abschluss der Telekommunikation weniger hohen Verarbeitungsrestriktionen unterliegen als es noch während des Telekommunikationsvorgangs der Fall ist. Die Problematik lässt sich anhand der folgenden paradoxen Situation verdeutlichen: Während der Umgang mit den äußeren Rahmendaten nach § 32i Abs. 1 Nr. 1 BDSG-E bei einem laufenden Telekommunikationsvor-

[443] BT-Drs. 17/4230, 21 f.
[444] BT-Drs. 17/4230, 17.
[445] BT-Drs. 17/4230, 7.

gang nur zur Gewährleistung eines ordnungsgemäßen Betriebs der Telekommunikationsanlage zulässig ist, können dieselben Daten gemäß § 32i Abs. 4 BDSG-E einen Sekundenbruchteil nachdem der Telekommunikationsvorgang abgeschlossen wurde, zur Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses eingesetzt werden.[446] Dies kann in der Praxis dazu führen, dass Arbeitgeber versuchen wollen, die strengeren Vorschriften aus § 32i Abs. 1 - 3 BDSG-E zu umgehen und den Datenumgang auf Grundlage des Abs. 4 zu vollziehen.[447] Es ist daher zu erwarten, dass der Gesetzgeber insbesondere bei dieser Vorschrift erhebliche Nachbesserungen vornehmen wird.

4.1.1.2 Erlaubnis aus einer anderen Rechtsvorschrift

Auch kollektivrechtliche Regelungsinstrumente, wie ein Tarifvertrag als überbetrieblicher Rahmen, eine betriebsspezifische Betriebsvereinbarung oder eine behördenindividuelle Dienstvereinbarung zur Reglementierung der Nutzung und Kontrolle der im Callcenter eingesetzten Techniken durch den Arbeitgeber, können als „andere Rechtsvorschrift“ im Sinne des § 4 Abs. 1 BDSG Anwendung finden.[448] In einem solchen Fall gehen die Vorschriften des Tarifvertrags, der Betriebs- oder Dienstvereinbarung denen des Bundesdatenschutzgesetzes vor. § 32 Abs. 3 BDSG schreibt ausdrücklich fest, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

4.1.1.2.1 Erlaubnis aus einer Betriebs- oder Dienstvereinbarung

4.1.1.2.1.1 Aktuelle Rechtslage

Betriebs- beziehungsweise Dienstvereinbarungen stellen für Arbeitgeber und Dienstherrn nach derzeitiger Rechtslage eine einfache und zugleich praktikable Möglichkeit dar, die Nutzung der Kommunikationsanlage und deren Kontrolle zu reglementieren, da sich auf diesem Weg ein erheblicher Verwaltungsaufwand umgehen lässt. Im Übrigen müsste der Betriebs- oder Personalrat – falls ein solcher in der Organisation existiert – ohnehin bei der Ausgestaltung einer individuellen Einwilligung herangezogen werden, da er gemäß § 87 Abs. 1 Nr. 6 BetrVG bezie-

[446] *Hilbrans*, AuR 2010, 424 (425).
[447] Mit derselben Befürchtung *Hilbrans*, AuR 2010, 424 (425).
[448] Dazu ausführlich *Sassenberg/Bamberg*, DuD 2006, 226 ff.; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, BDSG, § 4 Rn. 3; *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 3. Aufl. 2010, Rn. 345 ff.; *Rose*, DuD 2011, 136.

hungsweise § 75 Abs. 3 Nr. 17 BPersVG diesbezügliche Mitbestimmungsrechte besitzt. Was die Nutzung des Gesprächsmanagement-Systems durch öffentliche Callcenter anbelangt, so können die im Hinblick auf nichtöffentliche Stellen aufgezeigten Grundsätze übertragen werden: Der Personalrat verfügt über ein vergleichbares diesbezügliches Mitbestimmungsrecht wie der Betriebsrat.[449]

Im Zusammenhang mit der Einführung und Anwendung von elektronischen Informations- und Kommunikationsmitteln im Callcenter nimmt § 87 Abs. 1 Nr. 6 BetrVG die bedeutsamste Stellung ein. Das dort geregelte erzwingbare Mitbestimmungsrecht dient dem Persönlichkeitsschutz der Arbeitnehmer. Es sichert die Einhaltung des in § 75 Abs. 2 BetrVG verankerten allgemeinen Arbeitnehmerpersönlichkeitsrechts, wonach Arbeitgeber und Betriebsrat die freie Persönlichkeitsentfaltung der Arbeitnehmer zu schützen und zu fördern haben.[450]

Vorab ist festzuhalten, dass dem Arbeitgeber Verhaltens- oder Leistungskontrollen in Bezug auf seine Mitarbeiter zustehen müssen, damit er, als Gläubiger im Arbeitsverhältnis, überhaupt feststellen kann, ob die vertraglich geschuldete Arbeitspflicht adäquat erfüllt wird.[451] Der Callcenter-Betreiber kann sich zur Überwachung auch der technischen Infrastruktur bedienen. Das Mitbestimmungsrecht zielt darauf ab, die Arbeitnehmer vor den besonderen Gefahren der Technik zu schützen, die hauptsächlich in der dauerhaften Speicherung und damit ständigen Verfügbarkeit entsprechender Informationen über Mitarbeiter bestehen.[452]

Gemäß § 87 Abs. 1 Nr. 6 BetrVG verfügt der Betriebsrat bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, über ein Mitbestimmungsrecht. Dieses Mitbestimmungsrecht kommt allerdings nur zum Tragen, soweit keine gesetzliche oder tarifliche Regelung besteht. Die Öffnungsklausel des § 4 Abs. 1 BDSG erlaubt eine vom Bundesdatenschutzgesetz abweichende Reglementierung durch eine Betriebsvereinbarung.[453] § 87 Abs. 1 Nr. 6 BetrVG greift auch dann, wenn eine schon bestehende technische Einrichtung geändert, erweitert oder ergänzt wird und

[449] *BVerwG* v. 16.12.1987, NZA 1988, 513; *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 4 Rn. 306 ff.; nachfolgende Ausführungen zur Möglichkeit des Abschlusses einer Kollektivvereinbarung entstammen teilweise aus *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 76, 114 f.
[450] *Panzer*, Mitarbeiterkontrolle und neue Medien, 2004, 194.
[451] *Wiese*, RdA 2009, 344 (348); *Richardi*, in: Richardi (Hrsg.), Kommentar zum Betriebsverfassungsgesetz, 12. Aufl. 2010, § 87 Rn. 482.
[452] *Richardi*, in: Richardi (Hrsg.), Kommentar zum Betriebsverfassungsgesetz, 12. Aufl. 2010, § 87 Rn. 483.
[453] *Altenburg/von Reinersdorff/Leister*, MMR 2005, 222 (223); *Trittin/Fischer*, NZA 2009, 343 (344); *Menzler-Trott*, RDV 1999, 257.

sich dadurch ihre Anwendung anders gestaltet.[454] Dies ist etwa der Fall, wenn weitere Komponenten des Gesprächsmanagement-Systems an die im Callcenter bereits vorhandene IuK-Architektur angefügt werden.

Der Begriff „technische Einrichtung" ist nach dem *BAG*[455] und der h. M.[456] weit zu fassen: Zu verstehen sind darunter optische, mechanische, elektronische, akustische und sonstige Geräte, die ein bestimmtes Maß an Vergegenständlichung aufweisen. Callcenter-Arbeitsplätze weisen die geforderte Vergegenständlichung auf, da neben der erforderlichen Software – die zweifelsohne keine ausreichende Vergegenständlichung besitzt – verschiedene Hardwarekomponenten benötigt werden. Insofern ist auf das Gesamtsystem abzustellen.[457]

Unter den Überwachungsbegriff lassen sich Vorgänge unterordnen, die der Gewinnung von Informationen über Verhalten oder Leistung von Mitarbeitern dienen und regelmäßig aufgezeichnet werden, um sie letztendlich der menschlichen Wahrnehmung zugänglich zu machen oder auszuwerten.[458] Allein anhand der anfallenden Gesprächsprotokolle ist unstrittig eine Überwachung möglich.

Der Wortlaut der Vorschrift legt nahe, dass eine Verhaltens- oder Leistungskontrolle tatsächlich vollzogen oder mindestens beabsichtigt wird. Der Begriff des Bestimmtseins ist allerdings sehr weit auszulegen: Es genügt, wenn durch das System allein objektiv die Möglichkeit besteht, die Arbeitnehmer zu überwachen.[459] Diese Möglichkeit ist schon beim Einsatz herkömmlicher, in Callcentern verwendeter IuK-Anlagen gegeben; dazu bedarf es keiner speziellen Überwachungssoftware. Bereits die Auswertung der in der Telefonanlage gespeicherten Gesprächsprotokolle erlaubte eine detaillierte Kontrolle in zumindest quantitativer Hinsicht. Das Mitbe-

[454] *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 4 Rn. 292; *Böker/Kamp*, Betriebliche Nutzung von Internet, Intranet und E-Mail, 2003, 79.
[455] *BAG* v. 14.9.1984, NZA 1985, 28; *BAG* v. 6.12.1983, NJW 1984, 1476.
[456] *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 78 m. w. N.; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 14 Rn. 755 ff.; *Klebe*, NZA 1985, 44 ff.
[457] *Besgen/Prinz*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 2 Rn. 3; *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 78; ErfK/*Kania*, BetrVG, 11. Aufl. 2011, § 87 Rn. 48.
[458] *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 78 f.; *Altenburg/von Reinersdorff/Leister*, MMR 2005, 222 (223).
[459] St. Rspr. *BAG* v. 9.9.1975, NJW 1976, 261; *Richardi*, in: Richardi (Hrsg.), Kommentar zum Betriebsverfassungsgesetz, 12. Aufl. 2010, § 87 Rn. 478; *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 85; *Fitting et al*., HK BetrVG, § 87 Rn. 235; *Wohlgemuth*, CR 1988, 1005 (1008); *Linnenkohl/Schütz*, RDV 1987, 129 (136); *Löwisch*, DB 2009, 2782 (2786); zur Diskussion über die Notwendigkeit einer Unterscheidung zwischen Verhaltens- und Leistungsdaten sowie anderen beziehungsweise persönlichen Daten im Rahmen der elektronischen Informationsverarbeitung *Linnenkohl/Schütz/Rauschenberg*, NZA 1986, 769 ff.

stimmungsrecht besteht aber nicht, falls der Callcenter-Betreiber technische Anlagen einführt oder anwendet, die ausschließlich anonyme Daten erheben.[460]

Überwachungsgegenstand muss weiterhin das Verhalten oder die Leistung der Arbeitnehmer sein. Unter Verhalten versteht man jedes Tun und Unterlassen mit Relevanz zur Erfüllung der Arbeitsaufgabe. Insoweit wird die Leistung bereits vom Verhalten erfasst. Notwendig ist in diesem Zusammenhang nur, dass sich einzelne Verhaltensweisen bestimmten Mitarbeitern zuordnen lassen.[461] Unmöglich wäre dies etwa, wenn sich die Callcenter-Mitarbeiter unter derselben Nutzerkennung am Frontend-System anmelden und darüber hinaus ihren Sitzplatz in den Räumen des Callcenters unsystematisch wechseln könnten. Wenn jedoch der Überwachungsdruck, der auf einer Mitarbeitergruppe in ihrer Gesamtheit lastet, auch auf die einzelnen Mitglieder durchschlägt, wird das Beteiligungsrecht des Betriebsrats ausgelöst.[462]

Eine Leistungs- oder Verhaltenskontrolle der Mitarbeiter, die das Gesprächsmanagement-System nutzen, ist anhand zahlreicher Komponenten denkbar: Etwa das Frontend-System und die Telefonanlage bieten über die Auswertung von Logdateien und Verbindungsprotokollen hierzu ideale Ansatzpunkte. Im Ergebnis erfüllt die Einführung und Anwendung des Gesprächsmanagement-Systems im Callcenter die Voraussetzungen des § 87 Abs. 1 Nr. 6 BetrVG, sodass ein Mitbestimmungsrecht besteht.

Die Auslagerung einzelner mitbestimmungspflichtiger Komponenten oder Funktionen aus dem Callcenter führt nicht zur Aushebelung der Mitbestimmungspflicht der Beschäftigtenvertretung. Vielmehr muss durch geeignete Vertragsgestaltung mit dem externen Dienstleister sichergestellt sein, dass der Betriebsrat des Callcenters seine Mitbestimmungsrechte – bezogen auf die übertragenen mitbestimmungspflichtigen Aufgaben – auch beim Dienstleistungsunternehmen ausüben kann. Insbesondere der Vorschrift des § 11 BDSG zur Auftragsdatenverarbeitung kommt diesbezüglich hohe Relevanz zu.[463]

Die bedeutendste – aber nicht zwingende – Möglichkeit zur Wahrnehmung dieses Rechts besteht im Abschluss einer Betriebsvereinbarung, da nur durch sie unmittelbare Rechte und Pflichten der Arbeitgeber und Arbeitnehmer ausgelöst werden. Die

[460] *Weißnicht*, MMR 2003, 448 (452).
[461] *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 2003, S. 81; ErfK/*Kania*, BetrVG, 11. Aufl. 2011, § 87 Rn. 50.
[462] *Wohlgemuth*, CR 1988, 1005 (1008); *Gola*, ArbuR 1988, 105 (110).
[463] *Fitting et al*., HK BetrVG, § 87 Rn. 250; ErfK/*Kania*, BetrVG, 11. Aufl. 2011, § 87 Rn. 59.

Betriebsvereinbarung verkörpert einen kollektiven Normenvertrag privatrechtlicher Natur zwischen Arbeitgeber und Betriebsrat, der unmittelbar und zwingend auf die Arbeitsverhältnisse einwirkt.[464] Gemäß § 77 Abs. 2 BetrVG sind Betriebsvereinbarungen zwischen Arbeitgeber und Betriebsrat gemeinsam zu beschließen, schriftlich festzuhalten, im Regelfall von beiden Seiten zu unterzeichnen und an geeigneter Stelle im Betrieb auszulegen. Kann keine Einigung zwischen Arbeitgeber und Betriebsrat erzielt werden, entscheidet gemäß § 87 Abs. 2 BetrVG die Einigungsstelle, deren Spruch die Einigung ersetzt.[465]

Die Frage, ob durch eine Betriebsvereinbarung auch zu Ungunsten der Belegschaft vom Standard der Datenschutzgesetze abgewichen werden darf, wird in der Literatur unterschiedlich beantwortet.[466] Abgelehnt wird die Möglichkeit des Abschlusses derartiger Betriebsvereinbarungen wegen folgender Argumente: Durch die Betriebsvereinbarung könne lediglich eine Konkretisierung der Vorschriften des Bundesdatenschutzgesetzes vorgenommen werden, die aufgrund der Schutzwirkung des § 75 Abs. 2 BetrVG nur zu einer Verbesserung des Schutzes der Arbeitnehmer führen dürfe. Ziel einer Betriebsvereinbarung sei, die wirtschaftliche und soziale Unterlegenheit der einzelnen Arbeitnehmer auszugleichen und die der Vertragsbeziehung immanente Dysfunktionalität zu kompensieren. Überdies werde durch die Kollektivregelung eine pauschale Interessenabwägung für sämtliche Mitarbeiter vorgenommen, die mit dem Gesetzeszweck des Bundesdatenschutzgesetzes nicht vereinbar sei. Das Bundesdatenschutzgesetz biete individualrechtlichen Datenschutz. Interessenabwägungen seien stets im Einzelfall zu vollziehen. Auch sei zu bezweifeln, dass der Betriebsrat tatsächlich über die Macht verfüge, eine interessengerechte Regelung gegenüber dem Arbeitgeber durchzusetzen.[467]

Befürworter der Option, auch eine vom Bundesdatenschutzgesetz abweichende Betriebsvereinbarung zu Lasten der Arbeitnehmer beschließen zu können, argumentieren, dass die in § 4 Abs. 1 BDSG manifestierte Abdingbarkeit des Bundesdatenschutzgesetzes nicht an Einschränkungen gebunden sei. Dem Argument der ledig-

[464] *Lelley*, in: Worzalla (Hrsg.), Internet am Arbeitsplatz, 2006, Rn. 159.
[465] ErfK/*Kania*, BetrVG, 11. Aufl. 2011, § 87 Rn. 3; *Menzler-Trott*, RDV 1999, 257 (258).
[466] Befürwortend etwa ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 4 Rn. 3; *Thüsing/Forst*, RDV 2011, 163; *Franzen*, RdA 2010, 257 (259 f.); *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 3. Aufl. 2010, Rn. 355 ff.; *ders.*, ArbuR 1988, 105 (112); *ders.*, RDV 2002, 109 (116); *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 2003, 103 f.; *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 4 Rn. 3; *Latendorf/Rademacher*, CR 1989, 1105 (1106); kritisch *Kort*, RdA 1992, 378 (383); *Boewer*, RDV 1988, 13 (19); ablehnend *Linnenkohl/Rauschenberg/Schütz*, BB 1987, 1454 ff.
[467] *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 2003, 101 f.; *Tuchbreiter*, Beteiligungsrechte des Betriebsrats bei der Einführung und Anwendung moderner Kommunikationsmittel, 2007, 157 f.

lich individualschützenden Wirkung des Bundesdatenschutzgesetzes könne entgegnet werden, dass § 87 Abs. 1 Nr. 6 BetrVG die kollektivrechtliche Ergänzung zum individualrechtlichen Persönlichkeitsschutz aus dem Bundesdatenschutzgesetz darstelle.[468] Außerdem müsse berücksichtigt werden, dass auch durch eine individuelle Einwilligung der Arbeitnehmer eine weiter reichende Datenverarbeitung legitimiert werden könne.[469]

Das *BAG* gelangte in seiner Rechtsprechung zur Telefondatenüberwachung[470] jedenfalls zum Ergebnis, dass Betriebsvereinbarungen auch dann als eine „andere Rechtsvorschrift" anzusehen seien, wenn sie vom Schutzniveau des Bundesdatenschutzgesetzes abwichen. Betriebsvereinbarungen seien nicht lediglich darauf beschränkt, Konkretisierungen unbestimmter Rechtsbegriffe des Bundesdatenschutzgesetzes mit dem Fokus auf die jeweiligen betrieblichen Eigenheiten zu enthalten. Genauso wenig müssten sie den Datenschutz der Arbeitnehmer stärken. Das Bundesdatenschutzgesetz biete ferner keinen Mindeststandard an Datenschutz, von dessen Niveau nicht durch Betriebsvereinbarung nach unten hin abgewichen werden könne. Wegen des Günstigkeitsprinzips wäre gar keine ausdrückliche Festschreibung im Gesetz notwendig gewesen, wenn nur eine Verbesserung des Arbeitnehmerdatenschutzes möglich wäre.[471]

In dem Streit der Meinungen erscheint eine vermittelnde Lösung zutreffend. In § 4 Abs. 1 BDSG ist keine dahingehende Reglementierung enthalten, dass nicht auch negativ von den Vorschriften des Bundesdatenschutzgesetzes abgewichen werden darf. Würde das Bundesdatenschutzgesetz in diesem Zusammenhang als absolutes datenschutzrechtliches Mindestniveau angesehen, wäre die Öffnungsklausel in § 4 Abs. 1 BDSG überflüssig. Die Grenze der Gestaltungsmöglichkeit ist allerdings erreicht, wenn ein Verstoß gegen grundgesetzliche Wertungen, zwingende Gesetzesnormen oder arbeitsrechtliche Grundsätze, insbesondere gegen § 75 Abs. 2 BetrVG, vorliegt. Eine Betriebsvereinbarung mit beliebigem Inhalt kann somit nicht geschlossen werden, denn die Vorschrift des § 75 Abs. 2 BetrVG dient der Sicherstellung, dass das Persönlichkeitsrecht der Arbeitnehmer im Betrieb gewahrt bleibt. Überdies soll der Betriebsrat als Vertretung der Beschäftigten fungieren und deren Interessen gegenüber dem Arbeitgeber durchsetzen.[472] Im Ergebnis kann durch Betriebsvereinbarungen kein erheblich schlechterer Datenschutz, als ihn das Bundes-

[468] *Kort*, RdA 1992, 378 (385).
[469] *Tuchbreiter*, Beteiligungsrechte des Betriebsrats bei der Einführung und Anwendung moderner Kommunikationsmittel, 2007, 159.
[470] *BAG* v. 27.5.1986, NJW 1987, 674 = NZA 1986, 643.
[471] *Höld*, Die Überwachung von Arbeitnehmern, 2006, 125 ff.
[472] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 62; *Seifert*, DuD 2011, 98 (107).

datenschutzgesetz gewährleistet, zulässig herbeigeführt werden. Es sind jedoch Freiheiten in der Umsetzung der Vorschriften des Bundesdatenschutzgesetzes vorhanden und Anpassungen an die jeweiligen betrieblichen Gegebenheiten möglich.

4.1.1.2.1.2 Zu erwartende Rechtslage

§ 4 Abs. 1 BDSG, der allgemein die Zulässigkeit des Umgangs mit personenbezogenen Daten regelt, wird voraussichtlich um einen Satz erweitert, der Betriebs- und Dienstvereinbarungen ausdrücklich als Rechtsvorschriften im Sinne des Bundesdatenschutzgesetzes qualifiziert.[473] Mit der Aufnahme dieses Satzes soll die h. M. in Rechtsprechung und Literatur in Gesetzesform gegossen werden: Es solle – so der Gesetzentwurf – ausdrücklich zu keiner Änderung der aktuellen Rechtslage kommen.[474] § 32l Abs. 3 BDSG-E stützt diese Zielvorstellung, indem die Vorschrift festschreibt, dass die Rechte der Interessenvertretungen unberührt bleiben sollen. So ist jedenfalls auch zukünftig das Mitbestimmungsrecht der Beschäftigtenvertretung bei der Einführung und Anwendung von Systemen, die sich potenziell zur Leistungs- oder Verhaltenskontrolle eignen, zu beachten.[475]

§ 32l Abs. 5 BDSG-E untersagt ausdrücklich ein Abweichen von den gesetzlichen Bestimmungen zum Beschäftigtendatenschutz zu Lasten der Beschäftigten. Es gelte sicherzustellen, dass das gesetzliche Datenschutzniveau für Mitarbeiter nicht unterschritten werde.[476] Betriebsvereinbarungen hätten unter anderem die Funktion, den gesetzlichen Rahmen auf die jeweilige nichtöffentliche oder öffentliche Stelle zuzuschneiden und zu konkretisieren, damit die jeweiligen spezifischen Gegebenheiten Berücksichtigung finden können. Jedoch sollen sämtliche Vereinbarungen, die zu Ungunsten der Beschäftigten abgeschlossen werden, nicht zulässig sein.[477]

Der Abschluss einer Kollektivvereinbarung, die im Zusammenhang mit dem Gesprächsmanagement-System die mitarbeiterbezogenen Datenverarbeitungsvorgänge regeln soll, ist sowohl nach derzeitiger als auch nach zu erwartender Rechtslage empfehlenswert. Dem Betriebsrat steht ohnehin ein diesbezügliches Mitbestimmungsrecht zu. Eine entsprechende Vereinbarung dient der betriebsspezifischen Präzisierung unbestimmter Rechtsbegriffe und kann die Rechtssicherheit sowohl aufseiten der Arbeitgeber oder Dienstherrn als auch aufseiten der Arbeitnehmer

[473] BT-Drs. 17/4230, 5; *Tinnefeld/Petri/Brink*, MMR 2010, 727 (729); *Seifert*, DuD 2011, 98 (107).
[474] BT-Drs. 17/4230, 14.
[475] *Schuler*, DuD 2011, 126 (128).
[476] BT-Drs. 17/4230, 22; *Rose*, DuD 2011, 136.
[477] BT-Drs. 17/4230, 22.

maßgeblich erhöhen.[478] Ein weitergehender Umgang mit personenbezogenen Daten der Callcenter-Mitarbeiter durch den Arbeitgeber als er in den §§ 32 - 32l BDSG-E vorgesehen ist, wird sich aber künftig nicht mehr durch eine Kollektivvereinbarung zulässig herbeiführen lassen.

4.1.1.2.2 Erlaubnis aus einem Tarifvertrag

4.1.1.2.2.1 Aktuelle Rechtslage

Bei einem Tarifvertrag handelt es sich um einen zivilrechtlichen Vertrag, dessen Abschluss schriftlich erfolgen muss. Ein solcher Kollektivvertrag ist in einen schuldrechtlichen und einen normativen Teil aufgeteilt.[479] Gemäß § 1 Abs. 1 TVG regelt ein Tarifvertrag die Rechte und Pflichten der Vertragsparteien und verkörpert darüber hinaus einen Normenvertrag, der Inhalt, Abschluss und Beendigung von Arbeitsverhältnissen sowie betriebliche und betriebsverfassungsrechtliche Fragestellungen reglementiert. Der zwischen Gewerkschaften und Arbeitgeberverbänden, teilweise auch einzelnen Arbeitgebern, herbeigeführte Tarifvertragsabschluss bildet einen Ordnungsrahmen zur Festschreibung der Arbeitsbedingungen.[480]

Tarifverträge gelten gemäß § 4 Abs. 1 Satz 1 TVG unmittelbar und zwingend zwischen den Tarifparteien. Auch sie stellen andere Rechtsvorschriften im Sinne des § 4 Abs. 1 BDSG dar und können daher nach aktueller Rechtslage als Rechtfertigungsgrundlage für den Umgang mit personenbezogenen Daten von Mitarbeitern dienen.[481]

4.1.1.2.2.2 Zu erwartende Rechtslage

Durch § 32l Abs. 5 BDSG-E wird der Handlungsrahmen, den ein Tarifvertrag in Zukunft grundsätzlich bietet, festgeschrieben: Ein Abweichen von den gesetzlichen Regelungen zu Ungunsten der Beschäftigten darf nicht stattfinden.[482] Es gelten insoweit die bereits aufgezeigten Grundsätze der zu erwartenden Rechtslage in Bezug auf Betriebsvereinbarungen.

---

[478] *Fitting et al*., HK BetrVG, § 87 Rn. 255.
[479] *Kilian*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Kollektivvereinbarungen, Rn. 4.
[480] MHA/*Richardi*, Band 1, 3. Aufl. 2009, § 7 Rn. 6 ff.
[481] So auch *Sassenberg/Bamberg*, DuD 2006, 226 (227).
[482] BT-Drs. 17/4230, 22.

Die Möglichkeit, die Nutzung der in Callcentern eingesetzten IuK-Techniken und insbesondere deren Kontrollmöglichkeit durch Arbeitgeber auf tarifvertraglicher Ebene zu regeln, kommt praktisch nur selten in Frage. Hauptgrund dafür ist die Verschiedenartigkeit der IuK-Systeme, die in den mit dem Tarifvertrag erfassten Unternehmen und Behörden zum Einsatz gelangen. Es lassen sich kaum auf sämtliche Unternehmen oder öffentliche Stellen gleichermaßen anwendbare Vereinbarungen treffen.[483] Allenfalls die Aufstellung eines groben Handlungsrahmens mittels einer tariflichen Lösung erscheint sinnvoll.

4.1.1.3 Erlaubnis aus einer Einwilligung

4.1.1.3.1 Aktuelle Rechtslage

Eine weitere Legitimationsgrundlage zum Umgang mit personenbezogenen Daten der Mitarbeiter des Callcenters besteht nach aktueller Rechtslage in deren diesbezüglichem Einverständnis. Die grundsätzlichen Wirksamkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung nach § 4a BDSG wurden bereits ausführlich im Zusammenhang mit dem Umgang mit Kundendaten behandelt. Insofern wird auf diese Ausführungen verwiesen.[484]

Die im Rahmen eines Beschäftigungsverhältnisses abzugebende datenschutzrechtliche Einwilligung durch den Callcenter-Mitarbeiter kann beispielsweise als diesbezügliche Klausel im Arbeitsvertrag oder in Form einer Zusatzvereinbarung zum Arbeitsvertrag gestaltet sein. Soll die Einwilligungserklärung zusammen mit anderen schriftlichen Erklärungen – etwa dem Arbeitsvertrag – abgegeben werden, ist sie in ihrem äußeren Erscheinungsbild deutlich hervorzuheben. Erforderlich ist eine markante drucktechnische Anbringung der Formulierung, die sich vom restlichen Text abhebt. Verstärken lässt sich die Erkennbarkeit beispielsweise durch Fettdruck.[485] Die intendierte Warnfunktion der Schriftform erfüllt nur solange ihren Zweck, wie die Arbeitnehmer erkennen können, was mit ihren Daten geschieht.[486]

Darüber, ob eine im Arbeitsverhältnis durch Arbeitnehmer erteilte datenschutzrechtliche Einwilligung überhaupt wirksam sein kann, besteht in der Literatur weitge-

[483] In Bezug auf die tarifvertragliche Regelungsmöglichkeit der Internet- und E-Mail-Nutzung am Arbeitsplatz *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 2003, 59.
[484] Dazu ausführlich Kapitel 3.1.1.1.3 „Erlaubnis aus einer Einwilligung“.
[485] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 4a Rn. 2.
[486] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 60; *BGH* v. 19.9.1985, NJW 1986, 46.

hend Uneinigkeit.[487] Der zentrale Streitpunkt besteht in der Frage, ob und inwieweit es einem Arbeitnehmer im Arbeitsverhältnis oder bei der Begründung eines solchen überhaupt möglich ist, eine freie Entscheidung darüber zu treffen, ob er die Einwilligung erteilen will oder nicht. Aufgrund der großen Bedeutung dieses Aspekts erfolgt nachfolgend eine ausführliche Erörterung.

Von tatsächlicher Freiwilligkeit kann allgemein nur die Rede sein, wenn der Mitarbeiter bei Versagen der Einwilligung keine negativen Konsequenzen befürchten muss – und ihm umgekehrt keine Leistungen verwehrt werden, in deren Genuss er gekommen wäre, hätte er die Einwilligung erteilt (sogenanntes Kopplungsverbot).[488] Der Mitarbeiter sieht sich jedoch im Arbeitsverhältnis mit der wirtschaftlichen Machtposition des Arbeitgebers konfrontiert. Diese Tatsache kann dazu führen, dass sich der Arbeitnehmer unter Druck gesetzt fühlt und sich in einer Zwangslage befindet, die die privatautonome Entscheidung beeinträchtigen kann.[489] Der Arbeitnehmer ist deshalb gemäß § 4a Abs. 1 S. 2 BDSG auf sein Verlangen hin, oder soweit es im konkreten Einzelfall notwendig erscheint, über die Folgen einer verweigerten Einwilligung aufzuklären.

Gegner der Auffassung, dass eine freiwillige – und damit rechtswirksame – datenschutzrechtliche Einwilligung im Rahmen des Beschäftigungsverhältnisses überhaupt abgegeben werden kann, stützen ihre Argumentation hauptsächlich auf den Druck, der auf den Beschäftigten laste.[490] Man stelle sich das anschauliche Beispiel eines Arbeitsvertragsabschlusses vor: Unterschreibt der Arbeitnehmer hier nicht eine diesbezügliche Einwilligungserklärung, wird der Arbeitsvertrag wohl erst gar nicht zustande kommen.[491] In solchen Fällen kann zweifelsohne von Freiwilligkeit

[487] *Trittin/Fischer*, NZA 2009, 343 (344); die Möglichkeit einer datenschutzrechtlichen Einwilligung im Rahmen des Arbeitsverhältnisses ablehnend etwa *Hilbrans*, AuR 2010, 424 (426); befürwortend etwa *Weißgerber*, Arbeitsrechtliche Fragen bei der Einführung und Nutzung vernetzter Computerarbeitsplätze, 2003, 130 ff.; *Erler*, Die private Nutzung neuer Medien am Arbeitsplatz, 2003, 97 f.; *Zscherpe*, MMR 2004, 723 (727); *Gola*/*Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 6 ff.*; Lambrich/Cahlik*, RDV 2002, 287 (293); kritisch *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 4a Rn. 5a; *Duhr et al.*, DuD 2002, 5 (13); *Panzer*, Mitarbeiterkontrolle und neue Medien, 2004, 161; *Wedde*, DuD 2004, 169 ff.; *Petri/Kieper*, DuD 2003, 609 (611); Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 91.

[488] *Panzer*, Mitarbeiterkontrolle und neue Medien, 2004, 161; *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 59; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4a Rn. 63; *Iraschko-Luscher*, DuD 2006, 706 (708).

[489] *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 3. Aufl. 2010, Rn. 324 ff.; *Koeppen*, Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz, 2007, 182; *Gliss/Kramer*, Arbeitnehmerdatenschutz, 2006, 35; *Forst*, RDV 2010, 150 (151).

[490] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 4a Rn. 21.

[491] *Erler*, Die private Nutzung neuer Medien am Arbeitsplatz, 2003, 97; *Koeppen*, Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz, 2007, 182; dazu näher *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 59.

keine Rede sein. Auch kann eine freiwillige Einwilligung nicht durch Drohung oder arglistige Täuschung herbeigeführt werden.[492]

Befürworter hingegen argumentieren, ohne die Möglichkeit der Erteilung einer datenschutzrechtlichen Einwilligung im Rahmen von Arbeitsbeziehungen sei Arbeitnehmern jegliche Möglichkeit zur Abgabe von Willenserklärungen innerhalb des Arbeitsverhältnisses genommen. Sie erkennen auch, dass in bestimmten Situationen, wie im Bewerbungsgespräch, eine gewisse Disparität der Vertragsparteien vorliegt. Jedoch könne dies nicht soweit führen, dass den Arbeitnehmern sämtliche Autonomie entzogen werde.[493]

Auch hinsichtlich der Einwilligung ist eine vermittelnde Lösung des Meinungsstreits zutreffend: Der Umstand, dass sich (potenzielle) Arbeitnehmer nicht auf derselben „Verhandlungshöhe" wie der (potenzielle) Arbeitgeber befinden, dürfte in den meisten Fällen gegeben sein. Aus diesem Grund mangelt es in solchen Situationen an Freiwilligkeit. Trotzdem kann nicht generell unterstellt werden, dass ein erheblicher Druck auf die Arbeitnehmer ausgeübt wird. Daher muss stets die konkrete Situation betrachtet werden. Gerade was den Abschluss von Arbeitsverträgen – um das obige Beispiel nochmals aufzugreifen – im Bereich der Callcenter-Dienstleistungen anbelangt, so müssen hier spezifische Grundsätze gelten. Richtet man den Blick beispielsweise auf das Telefonbanking, so wird deutlich, dass in diesem Dienstleistungsbereich Aufzeichnungen der Gespräche aus Beweisgründen unumgänglich sind. Der potenzielle Arbeitnehmer sollte hier dennoch durch seine Einwilligung zum Ausdruck bringen, dass er mit den Aufnahmen einverstanden ist. In diesem speziellen Fall hat der Arbeitnehmer nur die Möglichkeit, den Arbeitsvertrag, der eine entsprechende Klausel enthält, zu unterzeichnen oder auf den Arbeitsplatz zu verzichten. Die Eingriffstiefe in das Persönlichkeitsrecht hat dem potenziellen Mitarbeiter aber bekannt zu sein, damit er entscheiden kann, ob er die Arbeitsbedingungen akzeptieren will.[494] Dieses Beispiel macht allerdings auch deutlich, dass datenschutzrechtliche Einwilligungen nicht das geeignete Instrument für generelle Lösungen darstellen. Allgemeine Lösungen sollten mittels Kollektivvereinbarungen herbeigeführt werden.

Dient die vorgesehene Gesprächsaufzeichnung der Callcenter-Telefonate demgegenüber lediglich der Leistungskontrolle oder Qualitätssicherung, sind andere Maßstäbe anzulegen: Hier kann die Einwilligung nicht ausufernde Überwachungsmaß-

[492] *Zscherpe*, MMR 2004, 723 (726).
[493] *Lambrich/Cahlik*, RDV 2002, 287 (292 f.); in Bezug auf einen Aufhebungsvertrag *BAG* v. 14.2.1996, NJW 1996, 2593; *Lorenz*, JZ 1997, 277 (281).
[494] *Gola*, RDV 2002, 109 (112).

nahmen durch den Arbeitgeber rechtfertigen, sondern muss sich daran orientieren, was betrieblich als erforderlich anzusehen ist.[495] So sind etwa dauerhaft angelegte Überwachungsmaßnahmen mit dem Zweck der lückenlosen Verhaltens- oder Leistungskontrolle auch nicht durch ein Einverständnis der betroffenen Mitarbeiter zulässig zu vollziehen.

Die gesetzlich vorgesehene Rechtfertigungsgrundlage der Einwilligung in personenbezogene Datenverarbeitungsvorgänge ist Ausdruck des informationellen Selbstbestimmungsrechts.[496] Um dieses ausüben zu können, sind Regelungen notwendig, die die Freiwilligkeit der Einwilligung schützen. Ein Beispiel hierfür ist das auf bestimmte Aspekte eingeschränkte Fragerecht des Arbeitgebers, das ihm in Vorstellungsgesprächen mit Bewerbern zusteht und selbst durch Einwilligung nicht ausgedehnt werden kann. Es lassen sich durch eine entsprechende Einwilligung keine zwingenden arbeitsrechtlichen Grundsätze überwinden.[497] Derartige Beschränkungen in der Einwilligungsmöglichkeit müssen jedoch nicht für sämtliche denkbaren Situationen im Arbeitsleben gelten. Die Einwilligung durch den Arbeitnehmer kann letztlich auch zu positiven Konsequenzen für ihn und zur Ausübung seines Selbstbestimmungsrechts führen.[498] Darüber hinaus bleibt zu berücksichtigen, dass selbst durch eine individuelle Einwilligung der Arbeitnehmer keine weiter reichende Datenverarbeitung zulässig wird, als es das Arbeitnehmerpersönlichkeitsrecht zulässt.[499]

Die Einwilligung in den Umgang mit personenbezogenen Mitarbeiterdaten, erst recht für die Durchführung bestimmter Kontrollen zur Qualitätssicherung, kann allenfalls dann Verbindlichkeit erlangen, wenn die Daten einen erkennbaren Bezug zum Arbeitsverhältnis aufweisen. Weitergehend muss der Arbeitgeber gerechtfertigte Gründe für den Umgang mit den Daten besitzen.[500] Das Kriterium der Freiwilligkeit hat in jedem Fall erfüllt zu sein, was im Zusammenhang mit Kontrollmaßnahmen fraglich erscheint. Daher ist eine Kollektivvereinbarung vielen einzelnen Einwilligungen vorzuziehen. Im Bereich der Callcenter-Dienstleistungen sind jedenfalls berechtigte Interessen des Callcenter-Betreibers im Hinblick auf den Umgang mit Mitarbeiterdaten mit dem Zweck der Qualitätskontrolle anzuerkennen; Kontrollmaßnahmen müssen allerdings verhältnismäßig ausgestaltet sein.[501]

---

[495] *Gola*, RDV 2002, 109 (112); *ders*., RDV 2005, 105 (107).
[496] *Forst*, RDV 2010, 150.
[497] *Gola*/*Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 7.
[498] *Thüsing*, RDV 2010, 147 (148).
[499] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 85.
[500] MHA/*Reichold*, Band 1, 3. Aufl. 2009, § 88 Rn. 23.
[501] Mit demselben Ergebnis *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 4 Rn. 154.

Die Beweislast, dass die Einwilligung tatsächlich auf der freien Entscheidung des einzelnen Beschäftigten beruht, trägt der Arbeitgeber. Kann er diesen Nachweis nicht erbringen, ist die Einverständniserklärung unwirksam und damit der Umgang mit den personenbezogenen Daten unzulässig.[502] Wurden solche Daten bereits verarbeitet, sind sie gemäß §§ 20 Abs. 2 Nr. 1 und 35 Abs. 2 Nr. 1 BDSG unverzüglich zu löschen. Einzelfallabhängig hat der Arbeitgeber Schadenersatzzahlungen gemäß §§ 7 und 8 BDSG, eine Geldbuße gemäß § 43 Abs. 2 Nr. 1 BDSG oder eine Strafe gemäß §§ 44 Abs. 1 i. V. m. 43 Abs. 2 Nr. 1 BDSG zu befürchten.[503]

Die datenschutzrechtliche Einwilligung muss gemäß § 4a Abs. 1 S. 3 BDSG schriftlich erteilt werden, soweit nicht eine andere Form aufgrund besonderer Umstände angemessen ist. Ein besonderer Umstand kann beispielsweise bei außerordentlicher Eilbedürftigkeit vorliegen. Davon darf im Rahmen der Begründung und Durchführung von Beschäftigungsverhältnissen nicht ausgegangen werden.[504]

Eine individuelle Einwilligung durch Arbeitnehmer, die dem Callcenter-Betreiber weitergehende Befugnisse im Umgang mit den Arbeitnehmerdaten einräumt, als diese bereits in einer Betriebs- oder Dienstvereinbarung festgelegt sind, könnte in der betrieblichen Praxis zu erheblichen Friktionen zwischen dem Arbeitgeber und der Beschäftigtenvertretung führen. Die mit der Einwilligung angestrebte Erweiterung der Verarbeitungslegitimation führte faktisch zum Unterlaufen der zwischen den Betriebsparteien ausgehandelten und miteinander vereinbarten Vorschriften; die praxisgerechte Regelungsmöglichkeit mittels Kollektivvereinbarung könnte dadurch zum „zahnlosen Tiger“ werden. Eine vertrauensvolle Zusammenarbeit von Arbeitgeber oder Dienstherr und Beschäftigtenvertretung, wie sie durch § 2 Abs. 1 BetrVG und § 2 Abs. 1 BPersVG und den entsprechenden landesgesetzlichen Regelungen zum Personalvertretungsrecht gefordert wird, würde dadurch verfehlt.

Aus diesem Grund gelangt das Günstigkeitsprinzip zur Anwendung, das Abweichungen von den Regelungen der Kollektivvereinbarung grundsätzlich nur zu Gunsten der Beschäftigten erlaubt.[505] Ausnahmsweise kann von der Kollektivvereinba-

[502] *Koeppen*, Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz, 2007, 183; *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 68; dazu *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 60.
[503] *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 68; zu den zivilrechtlichen Folgen des § 44 BDSG s. *Wybitul/Reuling*, CR 2010, 829 ff.
[504] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 60.
[505] *Gola*, RDV 2002, 109 (116); *Rose*, DuD 2011, 136; *Richardi*, RdA 1983, 201 (215).

rung zu Ungunsten der Beschäftigten abgewichen werden, wenn die Vereinbarung eine entsprechende Öffnungsklausel enthält.[506]

Voraussetzung für die Anwendbarkeit dieses Prinzips ist allerdings das Vorliegen einer Konkurrenzsituation zwischen der Regelung der Kollektivvereinbarung und der einzelvertraglichen Abrede. Wenn die Kollektivvereinbarung und die einzelvertragliche Abrede nicht denselben Gegenstand betreffen, so ist die einzelvertragliche Vereinbarung sowohl zu Gunsten als auch zu Lasten der Beschäftigten zulässig.[507]

Analog zur Einwilligung zum Umgang mit Kundendaten gilt auch für Einwilligungen im Arbeitsverhältnis der Grundsatz, dass man nur dann auf sie zurückgreifen sollte, wenn keine Rechtsvorschrift den Datenumgang bereits erlaubt, da die Möglichkeit ihrer Verweigerung und Rücknahme gravierende Probleme darstellen. Eine systematische Technikeinführung und -anwendung am Arbeitsplatz vermag durch Einwilligungen, die im Einzelfall verweigert werden können, nicht gestützt zu werden. Falls keine Möglichkeit der Verweigerung besteht, fehlt es an der Freiwilligkeit der Einwilligung.

4.1.1.3.2 Zu erwartende Rechtslage

Mit dem zukünftigen § 32l Abs. 1 BDSG-E stellen sich die dargestellten Fragen nicht mehr: Die Vorschrift regelt, dass Einwilligungen im Rahmen des Beschäftigungsverhältnisses nur noch in den gesetzlich ausdrücklich genannten Fällen in Betracht kommen.[508] Dies bedeutet konkret, dass die Rechtfertigungsgrundlage der Einwilligung gemäß § 4 Abs. 1 BDSG im Rahmen von Beschäftigungsverhältnissen nicht mehr generell einen zulässigen Umgang mit personenbezogenen Beschäftigtendaten herbeiführen kann.[509]

Gesetzlich explizit festgeschriebene Fälle, in denen zukünftig eine Einwilligung in Betracht kommt, betreffen gemäß

---

[506] *Fitting et al*., HK BetrVG, § 77 Rn. 197; ErfK/*Kania*, BetrVG, 11. Aufl. 2011, § 77 Rn. 79 f.; *Raatz*, DB 1972, 1 (4); das Pendant zur arbeitsvertragsoffenen Betriebsvereinbarung verkörpert der betriebsvereinbarungsoffene Arbeitsvertrag, dazu MHA/*Matthes*, Band 2, 3. Aufl. 2009, § 238 Rn. 85 f.; *Blomeyer*, NZA 1996, 337 (344); *Richardi*, RdA 1983, 201 ff.; *Däubler*, ArbuR 1984, 1 ff.

[507] *Richardi*, in: Richardi (Hrsg.), Kommentar zum Betriebsverfassungsgesetz, 12. Aufl. 2010, § 77 Rn. 145; *Höfling/Burkiczak*, NJW 2005, 469.

[508] *Körner*, Moderner Datenschutz für die Beschäftigten: Ein Ende der Skandale?, 2010, 4 f. (abrufbar unter: www.hugo-sinzheimer-institut.de/fileadmin/user_data_hsi/Dokumente/Gutachten_Arbeitnehmerdatenschutz_HSI.pdf); *Timner/Schreier*, AuA Sonderausgabe 2010, 4 (5); *Seifert*, DuD 2011, 98 (106).

[509] BT-Drs. 17/4230, 22.

- § 32 Abs. 6 Satz 4 BDSG-E die Erhebung von Beschäftigtendaten bei Dritten,
- § 32a Abs. 1 Satz 2 BDSG-E ärztliche Untersuchungen von Beschäftigten und Weitergabe des Untersuchungsergebnisses,
- § 32a Abs. 2 Satz 2 BDSG-E die Durchführung von Eignungstests und Weitergabe des Ergebnisses,
- § 32b Abs. 3 BDSG-E die weitere Speicherung von Beschäftigtendaten trotz Nichtzustandekommens eines Beschäftigungsverhältnisses,
- §§ 32c Abs. 3 i. V. m. 32a Abs. 1 Satz 2, Abs. 2 Satz 2 BDSG-E ärztliche Untersuchungen und die Durchführung von Eignungstests bei bestehenden Zweifeln an der Eignung von Beschäftigten sowie bei einem beabsichtigten Arbeitsplatz- oder Tätigkeitswechsel,
- § 32h Abs. 1 Satz 2 BDSG-E den Umgang mit Lichtbildern von Beschäftigten,
- § 32i Abs. 2 Satz 1 BDSG-E den Umgang mit Inhaltsdaten der ausschließlich zu beruflichen Zwecken erlaubten Telefonie und
- § 32i Abs. 2 Satz 2 BDSG-E den Umgang mit Inhaltsdaten der Telefonate bei Callcenter-Dienstleistungen.

Die Möglichkeit zur Abgabe einer Einwilligung im Zusammenhang mit Callcentern aus § 32i Abs. 2 Satz 2 BDSG-E betrifft gar nicht die Beschäftigten, sondern die Kunden; Letztere müssen einwilligen, damit der Callcenter-Betreiber Gesprächsinhalte zum Zwecke einer Verhaltens- oder Leistungskontrolle zur Kenntnis nehmen darf. Es bleibt kein Spielraum für die Rechtfertigung irgendwelcher erweiterten Datenverarbeitungsbefugnisse – im Verhältnis zu den im Gesetz bereits verankerten Befugnissen – durch Einwilligung der Callcenter-Mitarbeiter.

Die strikte Beschränkung der Einwilligungsmöglichkeit auf bestimmte Sachverhalte kann in der betrieblichen und dienstlichen Praxis unweigerlich zur Benachteiligung der Beschäftigten führen – sollte die Regelung tatsächlich im Gesetz verankert werden. Es wird stets Situationen geben, in denen das grundsätzliche Einwilligungsverbot nicht nur zu Gunsten der Mitarbeiter, sondern auch zu deren Nachteil wirkt.[510]

Der Lösungsweg bei der Reglementierung von Verhaltens- oder Leistungskontrollen in Callcentern wird künftig über kollektive Regelungen in Form von Betriebs- oder Dienstvereinbarungen gesucht werden müssen. Kollektivvereinbarungen sind ein adäquates Instrument für die im Bereich der Callcenter vorzufindende technikdurchdrungene Praxis.

[510] *Seifert*, DuD 2011, 98 (106).

4.1.2 Informationspflichten

Aus Gründen der Transparenz existieren datenschutzrechtliche Informationspflichten, die es Betroffenen ermöglichen, ihr informationelles Selbstbestimmungsrecht wahrzunehmen. Der Callcenter-Betreiber unterliegt in seiner Eigenschaft als Arbeitgeber gegenüber seinen Mitarbeitern bestimmten Informationspflichten, wenn er mit personenbezogenen Daten der Beschäftigten umgeht. Die im Hinblick auf Kunden bereits dargestellten Informationspflichten in Kapitel 3.1.2 „Informationspflichten“ gelten grundsätzlich auch mitarbeiterbezogen. Auf ihre Darstellung kann daher hier verzichtet werden.

Der zukünftig zu erwartende Beschäftigtendatenschutz sieht mit § 32j BDSG-E eine eigenständige Regelung zur besonderen Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten vor. Diese konkretisiert die Informationspflicht aus § 42a BDSG für Beschäftigungsverhältnisse. Unverzüglich nach Feststellung durch den Arbeitgeber, dass bei ihm gespeicherte Beschäftigtendaten unrechtmäßig übermittelt worden oder auf andere Weise zur Kenntnis Dritter gelangt sind, hat er gemäß § 32j Satz 1 BDSG-E die betroffenen Beschäftigten darüber zu informieren. Die diesbezügliche, unmittelbare Information der zuständigen Aufsichtsbehörde ist weitergehend für die Fälle vorgeschrieben, in denen schwerwiegende Beeinträchtigungen der Rechte oder der schutzwürdigen Interessen der Beschäftigten drohen.[511] Mit dem Verweis auf § 42a Satz 3, 4 und 6 BDSG werden die Anforderungen an den Inhalt der Unterrichtung gestellt und das grundsätzliche Verwendungsverbot der Information im Rahmen eines Straf- oder Ordnungswidrigkeitenverfahrens manifestiert.[512]

4.1.3 Rechte der Beschäftigten

Werden personenbezogene Daten von Arbeitnehmern erhoben, verarbeitet oder genutzt, stehen den Beschäftigten – als „Betroffene“ im datenschutzrechtlichen Sinne – grundsätzlich dieselben Rechte wie den Kunden zu. Sie besitzen darüber hinaus die Möglichkeit, sich mit ihrem Anliegen vertrauensvoll an die Beschäftigtenvertretung zu wenden, falls eine solche in der verantwortlichen Stelle eingerichtet ist.

Um eine Wiederholung der Ausführungen zu den Betroffenenrechten zu vermeiden, wird auf Kapitel 3.1.3 „Rechte der Kunden“ verwiesen. Die dort dargestellten Rech-

[511] BT-Drs. 17/4230, 9.
[512] Dazu bereits Kapitel 3.1.2.2 „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten“.

te gelten ebenso für die Beschäftigten des Callcenters, die sie gegenüber ihrem Arbeitgeber geltend machen können.

4.1.4 Ausgewählte Kontrollmaßnahmen in Bezug auf Beschäftigte im Callcenter

Im Callcenter wird die Arbeitsleistung maßgeblich mit der Nutzung der Telefonanlage erbracht. Damit der Arbeitgeber die Leistungserbringung seiner Mitarbeiter beurteilen kann, muss er sie in einem gewissen Rahmen kontrollieren dürfen. Kontrollen sind daher grundsätzlich zulässig, dürfen jedoch nicht zu tief in das Persönlichkeitsrecht der Callcenter-Mitarbeiter eingreifen; die konkreten Kontrollvorhaben sind einzelfallbezogen einer Verhältnismäßigkeitsprüfung zu unterziehen.[513]

Der Betreiber eines Callcenters verfügt – zumindest theoretisch – über ein breites Spektrum an Möglichkeiten, seine Mitarbeiter in ihrem Arbeitskontext zu überprüfen. Die voranschreitende Verschmelzung moderner Netzwerktechnik mit Kommunikationstechnik bietet hierzu ideale Voraussetzungen.

Die nachfolgend vorgenommene datenschutzrechtliche Beurteilung der Kontrollmaßnahmen des Arbeitgebers beschränkt sich auf die am weitesten verbreiteten Möglichkeiten sowie auf eine weitere Alternative, die gerade aufgrund der spezifischen Eigenschaften des Gesprächsmanagement-Systems realisiert werden kann. Es handelt sich dabei um

1. offenes und verdecktes Mithören der Gespräche (Monitoring) mit oder ohne Aufzeichnung,
2. Durchführung von Testanrufen (Mystery Calls) mit oder ohne Aufzeichnung,[514]
3. Auswertung der äußeren Umstände der Telefonate[515] und
4. automatisierte Sprach- und Emotionserkennung.

[513] Die nachfolgenden Ausführungen basieren, mit Ausnahme der Bewertung der automatisierten Sprach- und Emotionserkennung, im Wesentlichen auf *Hoss*, Callcenter: Mitarbeiterkontrollen auf dem datenschutzrechtlichen Prüfstand, 2010 (abrufbar unter: http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-010050732848/3/HossCallcenter.pdf).
[514] *Dannhorn/Mohnke*, AuA 2006, 210; *Wedde*, DuD 2004, 21 f.
[515] *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 34 f.

4.1.4.1 Mithören mit und ohne Aufzeichnung der Gespräche

In der Praxis lässt sich das Mithören der Telefonate grundsätzlich auf zwei Arten realisieren: durch offenes oder verdecktes Mithören.

Beim offenen Mithören ist der Callcenter-Mitarbeiter über den Überwachungsvorgang im Bilde. Dazu kann sich der „Kontrolleur" neben den Berater setzen, eventuell zusätzlich von einem Headset Gebrauch machen und somit unmittelbar Kenntnis vom Gesprächsverlauf erlangen.[516] Auch durch Aufschalten des Arbeitgebers in ein laufendes Telefonat bei gleichzeitiger, für beide Gesprächsteilnehmer wahrnehmbarer Anzeige dieses Vorgangs lässt sich das offene Monitoring praktizieren.[517] Es gilt an dieser Stelle anzumerken, dass der Gesprächspartner des Callcenter-Beraters allerdings im Vorfeld die Möglichkeit haben muss, entweder in den Mithörvorgang[518] einzuwilligen oder ihn abzulehnen, um eine Strafbarkeit des Mithörenden nach § 201 StGB auszuschließen.[519] Ohne diese Option resultierte eine Persönlichkeitsrechtsverletzung des Gesprächspartners. Dem Einwilligungserfordernis kann insbesondere bei Outbound-Callcentern, die beispielsweise Werbeanrufe tätigen, nur schwer Rechnung getragen werden, da kaum Akzeptanz der Angerufenen zu erwarten ist.[520] Die Problematik ließe sich aber zumindest entschärfen, wenn lediglich das Gesprochene des Callcenter-Mitarbeiters mitgehört würde.[521]

Über die Zulässigkeit des offenen Mithörens von Telefongesprächen im Callcenter hatte das *BAG*[522] zu entscheiden. Dabei ging es um die Frage, ob die Telefongespräche eines neu eingestellten, sich in Probezeit befindlichen Mitarbeiters in einem Callcenter vom Arbeitgeber mitgehört werden dürfen, um die Arbeitsqualität zu verbessern. Eine Betriebsvereinbarung sah die Mithörmöglichkeit vor. Das *BAG* gelangte zum Ergebnis, dass die kollektivrechtliche Regelung nicht zu beanstanden sei, da die Eingriffe in schonendster Art erfolgten. Die vorgesehenen Mithörmaßnahmen erstreckten sich lediglich auf die Probezeit und erfolgten ferner mit voller Kenntnis des Mitarbeiters, da das Mithören nur direkt am Arbeitsplatz des Callcen-

[516] *Dannhorn/Mohnke*, AuA 2006, 210.
[517] Ähnlich der Funktion „Aufschalten", wie sie bei ISDN-Anlagen realisiert wurde (s. dazu *Hammer/ Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 155 ff.).
[518] Dies trifft analog auf das verdeckte Mithören und insbesondere das Aufzeichnen der Gespräche zu. In Bezug auf beabsichtigtes Mithören kann die Einwilligung des Gesprächspartners unproblematisch direkt am Telefon erteilt werden, da das grundsätzliche Schriftformerfordernis in diesem Zusammenhang unangemessen wäre.
[519] *Vietmeyer/Byers*, MMR 2010, 807 (809); *Voigt*, DuD 2008, 780.
[520] *Voigt*, DuD 2008, 780.
[521] *Gola*, Datenschutz im Call Center, 2. Aufl. 2006, 47.
[522] *BAG* v. 30.8.1995, NZA 1996, 218.

ter-Mitarbeiters vollzogen werden durfte.[523] Stimmen in der Literatur vertreten zutreffend die Auffassung, dass Callcenter-Mitarbeiter das Mithören auch nach der Probezeit hinnehmen müssen, sofern es verhältnismäßig ausgestaltet ist; davon ist jedenfalls dann auszugehen, wenn die Kontrolle offen und lediglich über kurze Zeiträume hinweg durchgeführt wird.[524]

Das Wissen des Arbeitnehmers um die Überwachung kann sich stark auf die Validität der gewonnenen Ergebnisse auswirken. Der Berater wird besonders bemüht sein, eine gute Beurteilung zu erhalten, wenn er weiß, dass sein Telefonat der Kontrolle unterliegt. Deshalb könnte das verdeckte Mithören (Silent Monitoring) ein geeignetes Mittel darstellen, aussagekräftige Erkenntnisse über das tatsächliche Telefonierverhalten des Beraters zu erlangen.

Vor Inkrafttreten der Bundesdatenschutzgesetz-Novelle II bestanden in Bezug auf nichtöffentliche Callcenter sowohl beim offenen als auch beim verdeckten Mithören bundesdatenschutzgesetzlich keine Bedenken. Die Vorschriften des Bundesdatenschutzgesetzes griffen bei nichtöffentlichen Stellen generell gemäß § 1 Abs. 2 Nr. 3 BDSG erst, wenn sich ein Datenumgang mit Datenverarbeitungsanlagen vollzog oder der Umgang in oder aus nicht automatisierten Dateien erfolgte. Die aktuelle Gesetzeslage sieht durch den zusätzlich ins Bundesdatenschutzgesetz aufgenommenen § 32 BDSG vor, dass auch für nicht automatisierte Vorgänge und bei fehlendem Dateibezug das Bundesdatenschutzgesetz für Beschäftigungsverhältnisse gilt. Damit werden nun Sachverhalte, die einst ausschließlich über das allgemeine Persönlichkeitsrecht zu beurteilen waren, von den Regelungen des Bundesdatenschutzgesetzes erfasst.[525] § 32 BDSG ist als lex specialis im Verhältnis zur früheren gesetzlichen Verarbeitungsbefugnis von beschäftigtenbezogenen Daten aus – dem auch geänderten – § 28 Abs. 1 Satz 1 Nr. 1 BDSG vorrangig anzuwenden.[526] Die Vorschrift enthält die zum Beschäftigtendatenschutz durch die Rechtsprechung entwickelten Grundsätze.[527] Auch schon vor der jüngsten Änderung des Bundesdatenschutzgesetzes hatte der Arbeitgeber das Persönlichkeitsrecht seiner Mitarbeiter zu achten. Diese Verpflichtung wurde mit der Gesetzesnovellierung für jeglichen Umgang mit beschäftigtenbezogenen Daten einfachgesetzlich manifestiert. Im Grunde genommen ersetzte lediglich eine Generalklausel die andere – inhaltlich ergeben sich keine Änderungen.[528]

[523] *Wedde*, DuD 2004, 21 (25); *BAG* v. 30.8.1995, NZA 1996, 218.
[524] *Dannhorn/Mohnke*, AuA 2006, 210 (211).
[525] *Roßnagel*, NJW 2009, 2716 (2717); *Erfurth*, NJOZ 2009, 2914 (2924).
[526] *Roßnagel*, NJW 2009, 2716 (2721); *Deutsch/Diller*, DB 2009, 1462.
[527] BT-Drs. 16/13657, 37; entwickelt wurden die Grundsätze in den Urteilen *BAG* v. 15.7.1987, DB 1987, 2571 und *BAG* v. 12.9.2006, NZA 2007, 269.
[528] *Thüsing*, NZA 2009, 865 (869).

Das offene Mithören der Telefonate – sofern es jeweils nur kurzfristig angelegt ist und somit die Berater nicht ständig unter Druck setzt – wird im Hinblick auf das Datenschutzrecht nach aktueller Gesetzeslage mit § 32 Abs. 2 BDSG nicht zu beanstanden sein. Die Rechtmäßigkeit der Kontrolle ist anhand ihrer Erforderlichkeit festzustellen. Die Gesetzesbegründung[529] zum § 32 BDSG weist ausdrücklich darauf hin, dass Arbeitgebern zur Durchführung des Beschäftigungsverhältnisses bestimmte Rechte – insbesondere auf Leistungs- oder Verhaltenskontrollen – zustehen. Maßgeblich dafür, wie weit die Kontrollen reichen dürfen, ist das Ergebnis der Auslegung des Merkmals „Erforderlichkeit". Liegt lediglich eine Nützlichkeit der zu erhebenden Mitarbeiterdaten vor, reicht dies für die zulässige Durchführung des Vorhabens nicht aus.[530] Im Ergebnis wird sich die Prüfung der Erforderlichkeit mit der Anwendung der Generalklausel der „Zweckbestimmung", die nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG vor der Gesetzesnovelle problembezogen geprüft werden musste, decken.[531]

Verdeckte Mithörmaßnahmen sind dagegen an strengeren Maßstäben zu messen: Nach der Rechtsprechung des *BVerfG*[532] verletzt das heimliche Abhören eines Dienstgesprächs durch den Arbeitgeber das Recht am eigenen Wort. Selbst das Bewusstsein des Arbeitnehmers über die grundsätzliche Mithörmöglichkeit durch den Arbeitgeber beseitigt diesen grundrechtlichen Schutz nicht.[533]

Eine direkte Übertragung der Entscheidungsgrundsätze auf Kontrollen bei Callcenter-Mitarbeitern ist jedoch nicht möglich: Der Entscheidung lag ein Sachverhalt zu Grunde, bei dem der Arbeitnehmer mit dem Mithören des Arbeitgebers nicht rechnete, es sich somit um *heimliches* Mithören handelte. Beim Silent-Monitoring hingegen findet das Mithören nur verdeckt statt, das heißt die Mitarbeiter wurden auf das Mithören hingewiesen.[534] Verdecktes Mithören muss zu Ausbildungszwecken sowie zur Überprüfung der dienstlichen Aufgabenerfüllung ausnahmsweise zulässig sein, wenn die Mitarbeiter Kenntnis davon haben und die Kontrollen verhältnismäßig ausgestaltet sind.[535] Das Ziel der Kontrolle darf sich nicht durch offenes Mithören erreichen lassen. Die Information der Arbeitnehmer muss aber nicht unmittelbar vor jeder einzelnen Kontrollmaßnahme erfolgen, da dies das Vorhaben „verdeckte" Kontrolle ad absurdum führte.

[529] BT-Drs. 16/13657.
[530] *Däubler*, NZA 2001, 874 (876).
[531] *Deutsch/Diller*, DB 2009, 1462 (1463) m. w. N.; *Erfurth*, NJOZ 2009, 2914 (2918) m. w. N.
[532] *BVerfG* v. 19.12.1991, NJW 1992, 815 ff.
[533] *Raffler/Hellich*, NZA 1997, 862 (863).
[534] *Jordan/Bissels/Löw*, BB 2008, 2626 (2628).
[535] *Mengel*, BB 2004, 1445 (1449); *Dannhorn/Mohnke*, AuA 2006, 210 (211).

Das Aufzeichnen der Telefongespräche, beispielsweise zum Zweck der anschließenden Analyse und der Ableitung von potenziellem Schulungsbedarf der Berater, kann gleichermaßen beim offenen wie auch verdeckten Monitoring erfolgen. Besonderes Charakteristikum des Mitschneidens von Gesprächen ist, dass die jeweiligen Inhalte, also das gesprochene Wort, ihre Flüchtigkeit einbüßen und praktisch jederzeit vom Arbeitgeber zur Kenntnis genommen werden können.[536] Nicht nur die Gesprächsinhalte selbst, sondern auch die für die Tätigkeit als Callcenter-Mitarbeiter essentiellen „Nebenprodukte" des Gesprochenen, wie Stimmlage, Sprechgeschwindigkeit und Ausdrucksweise, welche Rückschlüsse auf die Stimmung und Verfassung des jeweiligen Mitarbeiters zulassen, sind von der Aufzeichnung erfasst.

Vor Inkrafttreten der Bundesdatenschutzgesetz-Novelle II war bei Aufzeichnungen der Telefonkommunikation danach zu differenzieren, ob die Gespräche analog, das heißt auf Tonband, oder digital festgehalten wurden. Bei analogen Mitschnitten fand das Bundesdatenschutzgesetz keine Anwendung, da keine Datenverarbeitungsanlagen und ferner keine Dateien tangiert sind. Durch die Gesetzesnovelle wurde diese Unterscheidung obsolet, da jetzt – wie bereits aufgezeigt – sämtliche Datenverarbeitungsprozesse im Rahmen des Beschäftigungsverhältnisses durch § 32 BDSG erfasst werden. Von der Nutzung veralteter analoger Tonträgersysteme ist heutzutage ohnehin nicht mehr auszugehen. Vielmehr finden digitale, computerunterstützte Aufnahmetechniken Verwendung.[537] Im Rahmen des Gesprächsmanagement-Systems kommen nur digitale Mitschnitte der Gespräche in Betracht.

Das Bundesdatenschutzgesetz erlaubt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten gemäß § 4 Abs. 1 BDSG nur, soweit es selbst oder eine andere Rechtsvorschrift diese Vorgänge zulässt. Im Übrigen benötigt man für eine zulässige Durchführung der genannten Vorgänge stets die Einwilligung des betroffenen Arbeitnehmers. § 4 Abs. 1 BDSG stellt eine gesetzliche Legitimation für einen Grundrechtseingriff dar.

Bei Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person handelt es sich gemäß § 3 Abs. 1 BDSG um personenbezogene Daten. Die Eckdaten eines Telefonats, zum Beispiel gewählte Rufnummer, Gesprächszeitpunkt und -dauer, fallen genauso unter § 3 Abs. 1 BDSG

[536] *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 35.
[537] *Jordan/Bissels/Löw*, BB 2008, 2626 (2629); *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 93 f.

wie die Gesprächsinhalte.[538] Eine zielgerichtete Datenbeschaffung über den Betroffenen erfüllt gemäß § 3 Abs. 3 BDSG den Tatbestand des „Erhebens“ von Daten.[539]

§ 32 Abs. 1 Satz 1 BDSG erlaubt dem Arbeitgeber den Umgang mit personenbezogenen Daten seiner Mitarbeiter, wenn der Umgang für Zwecke des Arbeitsverhältnisses erforderlich ist. Erforderlich ist eine Maßnahme dann, wenn sie für den verfolgten Zweck das Mittel mit der geringsten Eingriffstiefe darstellt. Es steht außer Frage, dass Leistungskontrollen durch den Callcenter-Betreiber die arbeitsvertraglichen Hauptpflichten erfassen und legitim sind. Sie müssen somit von den Beschäftigten hingenommen werden. Ob es für diese Kontrolle allerdings notwendig ist, dass das gesprochene Wort der Arbeitnehmer unbedingt festgehalten werden muss, bleibt zunächst fraglich. Das Arbeitsverhalten oder die Arbeitsleistung der Berater lassen sich auch mit weit geringeren Einschnitten in ihr Persönlichkeitsrecht überprüfen: Offenes oder verdecktes Mithören ohne Aufzeichnung der Gespräche sind als völlig ausreichende Möglichkeiten zur Mitarbeiterbeurteilung zu betrachten.[540] Die dauerhafte Verfügbarkeit des gesprochenen Worts der Mitarbeiter für den Arbeitgeber führte zu einer massiven Verletzung des Persönlichkeitsrechts der betroffenen Arbeitnehmer. Im Ergebnis kann § 32 BDSG genauso wenig wie der nach früherer Gesetzeslage heranzuziehende § 28 Abs. 1 Satz 1 Nr. 1 BDSG dazu dienen, Verhaltens- oder Leistungskontrollen anhand aufgezeichneter Telefonate zu rechtfertigen. Selbst wenn die mitgeschnittenen Gespräche nicht dauerhaft, sondern lediglich kurzfristig gespeichert werden sollen, wäre die Aufnahme unzulässig; der Eingriff in das Persönlichkeitsrecht der Mitarbeiter ist bereits hier zu tiefgehend. Höchstens ein hinreichend begründeter Verdacht auf eine Straftat könnte als Eingriffsrechtfertigung dienen.

Neben dem gesetzlichen Erlaubnistatbestand aus § 32 BDSG kommt für die zulässige Durchführung von Kontrollmaßnahmen ausnahmsweise die Einwilligung[541] der Arbeitnehmer in Betracht. Die Einwilligung nach § 4a BDSG ist in der Praxis jedoch problematisch, da grundsätzliche Zweifel an ihrer Freiwilligkeit bestehen können.[542] Neben der individuellen Einwilligung der Mitarbeiter im Callcenter in die Kontrolle durch den Arbeitgeber kommt – falls ein Betriebs- oder Personalrat vor-

[538] *Mengel*, BB 2004, 1445 (1448).
[539] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn 24.
[540] *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 100 f.; wohl auch *Dannhorn/Mohnke*, AuA 2006, 210 (212).
[541] S. zur zulässigen Ausgestaltung der Einwilligung des Gesprächspartners (Opt-in-/Opt-out-Modell) ausführlich *Voigt*, DuD 2008, 780 ff.; *Olbert*, Recht im Call Center, 2001, 128, betrachtet die Einwilligung als unabdingbare Zulässigkeitsvoraussetzung für die Umsetzung von Mithörmaßnahmen durch den Arbeitgeber.
[542] *Gliss/Kramer*, Arbeitnehmerdatenschutz, 2006, 35; dazu Kapitel 3.1.1.1.3 „Erlaubnis aus einer Einwilligung“.

handen ist – der Abschluss einer entsprechenden Betriebs- beziehungsweise Dienstvereinbarung[543] in Frage; gemäß § 87 Abs. 1 Nr. 6 BetrVG beziehungsweise § 75 Abs. 3 Nr. 17 BPersVG besteht ein diesbezügliches Mitbestimmungsrecht.[544]

Einen Sonderfall bei der Aufzeichnung von Gesprächen stellt beispielsweise die Dokumentation von Vertragsabschlüssen dar. Aufgrund drohender Streitfälle kann es für den Callcenter-Betreiber notwendig sein, die Zustimmungserklärung des Kunden zum Vertragsschluss aufzuzeichnen und solange zu archivieren, bis die Ansprüche aus dem Vertrag nicht mehr streitig sein können. Soll keine separate schriftliche Bestätigung des Vertrags durch Kunden stattfinden, kann der Callcenter-Betreiber im Zweifel praktisch nur mithilfe eines entsprechenden Mitschnitts beweisen, dass und welche Willenserklärungen am Telefon abgegeben wurden.[545]

Wenn der Zweck einer solchen Aufzeichnung durch den Callcenter-Betreiber nur darin besteht, im Streitfall vor Gericht die abgegebenen Willenserklärungen beweisen zu können, ist die Aufnahme im Hinblick auf die Mitarbeiter im Callcenter grundsätzlich als datenschutzrechtlich zulässig einzustufen. Allerdings muss dann sichergestellt sein, dass solche Aufnahmen gesondert archiviert und keinesfalls zu Verhaltens- oder Leistungskontrollen der Mitarbeiter herangezogen werden. Dies ist durch einen entsprechenden Systemschutz zu gewährleisten. Haben die Callcenter-Mitarbeiter Kenntnis von derartigen Mitschnitten sowie deren Zweck und liegen die weiteren genannten Voraussetzungen vor, ist eine für den Zweck der Beweissicherung im Geschäftsverkehr durchgeführte Gesprächsaufzeichnung als erforderlich zu betrachten und damit zulässig.[546]

Ebenso muss der Kunde im Vorfeld über die bevorstehende Aufnahme des Gesprächs(abschnitts) und ihren Zweck informiert werden. Um sicherzugehen, sollte auch trotz dieser besonderen Situation eine ausdrückliche Einwilligung des Kunden in die Aufzeichnung eingeholt werden. Im äußersten Fall besitzt er somit immer noch die Möglichkeit, das Telefonat zu beenden, um der Aufzeichnung zu entgehen. Einschränkende Voraussetzung bei der Einwilligung in die Aufnahme des Gesprächs ist jedoch, dass das Kopplungsverbot eingehalten wird.

[543] S. dazu ausführlich *Reska*, Call Center, 2006; Kapitel 4.1.1.2.1 „Erlaubnis aus einer Betriebs- oder Dienstvereinbarung“.
[544] *Menzler-Trott*, RDV 1999, 257.
[545] *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 95 f.; *Oberwetter*, NZA 2008, 609 (611).
[546] So auch *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 96 und *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 32 Rn. 17.

4.1.4.2 Durchführung von Testanrufen

Eine Alternative zum Abhören der Callcenter-Gespräche besteht in der Durchführung verdeckter Testanrufe (Mystery Calls) durch den Arbeitgeber. Es liegt in der Natur der Sache, dass sich diese Methode nur bei Inbound-Callcentern einsetzen lässt. Analog zu den Testanrufen bei Inbound-Callcentern wäre für Outbound-Callcenter ein Vorgehen denkbar, bei dem die automatische Wählvorrichtung (Predictive Dialer) so konfiguriert wird, dass eine automatische Verbindung zu einem fiktiven Kunden hergestellt wird, ohne dass der Berater davon Kenntnis hat.

Mystery Calls eignen sich zur Feststellung, ob der betreffende Callcenter-Berater über die erforderlichen Fachkenntnisse verfügt und einen professionellen Umgang mit Kunden pflegt.[547] Jeder Berater muss sich ohnehin stets darüber im Klaren sein, dass seine Gesprächspartner ohne Weiteres die Möglichkeit besitzen, sich an den Betreiber des Callcenters zu wenden, um diesen auf etwaiges Fehlverhalten der Berater hinzuweisen und über die Servicequalität in Kenntnis zu setzen.[548]

Vor Inkrafttreten der Bundesdatenschutzgesetz-Novelle II waren Mystery Calls datenschutzrechtlich als unproblematisch einzustufen. Wenn keine Aufzeichnung der Gespräche stattfand, fiel diese Methode zur Kontrolle – analog dem Mithören der Gespräche ohne Mitschneiden – nicht in den Anwendungsbereich des Datenschutzrechts, da bei Testanrufen weder Datenverarbeitungsanlagen zum Einsatz gelangen, noch der Umgang mit personenbezogenen Daten in irgendeiner Form in oder für Dateien erfolgt.

Mit Inkrafttreten des aktuellen § 32 BDSG hat sich dies geändert: Da nun jegliche Datenerhebung zum Zwecke des Beschäftigungsverhältnisses durch den Arbeitgeber über seine Mitarbeiter gemäß § 32 Abs. 2 BDSG dem Datenschutzrecht unterliegt, sind auch Mystery Calls am Kriterium der Erforderlichkeit zu messen. Die mitarbeiterbezogene Leistungsüberprüfung anhand von Testanrufen ist für die Durchführung des Beschäftigungsverhältnisses von Callcenter-Mitarbeitern als durchaus notwendig anzusehen, da sich der Arbeitgeber mit der Maßnahme ein aussagekräftiges Bild über die Leistungsfähigkeit und -bereitschaft seiner Belegschaft machen kann, das sich mit keiner anderen „milderen“ Maßnahme derart valide gewinnen lässt. Unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes bestehen keine Bedenken, wenn die Mitarbeiter mit Testanrufen durch den Arbeitgeber konfrontiert werden, die in ausreichend großen Zeitabständen stattfinden.

[547] A. A. *Jordan/Bissels/Löw*, BB 2008, 2626 (2627), die Mystery Calls als ungeeignete Methode betrachten, Fachkenntnisse und Soft Skills der Callcenter-Berater „abzufragen“.
[548] *Gola*, Datenschutz im Call Center, 2. Aufl. 2006, 70; *Dannhorn/Mohnke*, AuA 2006, 210 (212).

Eine weitere Legitimationsgrundlage – neben dem gesetzlichen Erlaubnistatbestand aus § 32 Abs. 2 BDSG – zur Durchführung von Anrufen zur Leistungsüberprüfung ist die Einwilligung der Mitarbeiter, die ausnahmsweise unter Sicherstellung der Freiwilligkeit eingesetzt werden kann. Daneben kommt eine diesbezügliche Betriebs- oder Dienstvereinbarung in Frage.

Eine Aufzeichnung der Testanrufe darf aufgrund der bereits beim Mitschneiden von Telefonaten angeführten Argumente grundsätzlich nicht stattfinden. Insofern ist auf die obigen Ausführungen zu verweisen.[549]

4.1.4.3 Auswertung der äußeren Umstände der Telefonate

Die Rahmendaten der Kommunikation (etwa Gesprächszeitpunkt, Gesprächsdauer und gewählte Rufnummer) sowie die Daten zum Status des jeweiligen Beraters (wie Abwesenheitszeiten, Anzahl angenommener Gespräche, Nachbearbeitungszeiten) lassen sich problemlos anhand der Telefonanlage ermitteln. Dabei erhobene Daten können entweder in Echtzeit oder zu jedem beliebigen späteren Zeitpunkt eingesehen werden.[550] Zusätzlich lassen sich die gewonnenen Daten grafisch oder tabellarisch darstellen, was ihre genaue Analyse erleichtert. Somit erhält der Arbeitgeber zumindest in quantitativer Hinsicht umfassende Informationen über die Arbeitsleistung seiner Mitarbeiter.

Bei den Telefondaten handelt es sich um personenbezogene Daten gemäß § 3 Abs. 1 BDSG, da beide Gesprächspartner regelmäßig anhand der jeweiligen Anschlussnummer identifizierbar sind. Es liegt darüber hinaus eine automatisierte Verarbeitung gemäß § 3 Abs. 2 BDSG vor, wenn die personenbezogenen Daten in der Telefonanlage gespeichert und zur Auswertung aufbereitet werden.[551] Folglich bedarf es einer datenschutzrechtlichen Befugnis zur Durchführung dieser Datenverarbeitungsvorgänge. Neben der ausdrücklichen Einwilligung des Mitarbeiters in die Auswertung der Telefondaten oder einer entsprechenden Betriebs- oder Dienstvereinbarung kommt die Erforderlichkeit des Datenumgangs zur Durchführung des Beschäftigungsverhältnisses gemäß § 32 Abs. 1 Satz 1 BDSG als Ermächtigungsgrundlage in Betracht.

[549] S. dazu Kapitel 4.1.4.1 „Mithören mit und ohne Aufzeichnung der Gespräche“.
[550] *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 34 f.
[551] *Kilian*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Kollektivarbeitsrechtliche Probleme der Informationstechnologie im Betrieb, Rn. 62.

Wenn es sich um die Erstellung sogenannter Bedienplatzreports handelt, ist dem Callcenter-Betreiber die Überwachungsbefugnis bis zu einem gewissen Grad zuzugestehen.[552] Die Kontrolle im Hinblick auf die Erfassung und Auswertung der angefallenen Telefondaten ist insoweit zulässig, als sie im Rahmen einer Abwägung zwischen Arbeitgeber- und Arbeitnehmerinteressen verhältnismäßig ausfällt.[553] In diesem Zusammenhang könnte etwa ein Vorgehen als verhältnismäßig anzusehen sein, bei dem die durch die Telefonanlage erfassten Daten an lediglich zehn Tagen pro Monat mitarbeiterspezifisch ausgewertet würden.[554] Unzulässig dagegen sind sämtliche Maßnahmen, die eine lückenlose Telefondatenüberwachung zuließen; anhand dieser Daten könnte ein Persönlichkeitsprofil der Mitarbeiter in Bezug auf einen bestimmten Lebensbereich gebildet werden. Dies stellt in jedem Fall eine Verletzung des in § 75 Abs. 2 BetrVG und § 68 Abs. 1 Nr. 2 BPersVG manifestierten Persönlichkeitsschutzes dar und überschreitet somit die Grenze einer zulässigen Überwachung.[555]

Denkbar sind grundsätzlich gruppenbezogene Auswertungen, die sich auch dauerhaft anlegen ließen, ohne an datenschutzrechtliche Grenzen zu stoßen. Sie gäben einen Überblick etwa über einen bestimmten Mitarbeiterkreis innerhalb des Callcenters; die mitarbeiterspezifische Komponente bliebe dabei unberücksichtigt.

4.1.4.4 Sprach- und Emotionserkennung

Die an den Callcenter-Arbeitsplätzen eingesetzte Kommunikationssoftware enthält ein Analysemodul, das die automatisierte Auswertung der durchgeführten Gespräche ermöglicht. Berechtigte Personen, wie der Teamleiter oder Trainer, haben Einblick in die Ergebnisse und können auf deren Grundlage Handlungs- und Schulungsbedarf seitens der Callcenter-Mitarbeiter ableiten. Diese Software enthält ein vordefiniertes Rechte- und Rollenmodell, das sich ändern und somit an die individuellen betrieblichen Eigenheiten anpassen lässt.

Die zentrale Funktion dieser Anwendung stellt die Spracherkennung dar, die feststellt, ob und wann bestimmte Schlüsselwörter auf dem Agentenkanal fallen. Somit

[552] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 32 Rn. 17; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 4. Aufl. 2008, Rn. 662.
[553] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 32 Rn. 15 ff.
[554] *Grobys*, Die Überwachung von Arbeitnehmern in Call Centern, 2007, 86; a. A. *Olbert*, Recht im Call Center, 2001, 129, der grundsätzlich davon ausgeht, dass die gänzliche Erfassung, Speicherung und Auswertung der Rahmendaten der Telekommunikation zulässig sei.
[555] *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 3. Aufl. 2010, Rn. 215; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 4. Aufl. 2008, Rn. 663 f.

kann beispielsweise ermittelt werden, ob der Callcenter-Mitarbeiter sich an den Gesprächsleitfaden gehalten und das Gespräch gemäß seiner Vorgaben durchgeführt hat. Auch die Sprechgeschwindigkeit und Deutlichkeit der Aussprache des Callcenter-Mitarbeiters lassen sich bestimmen und evaluieren. Die Ergebnisse dieser Auswertungsvorgänge können für den Betrachter in tabellarisch oder grafisch übersichtlicher Darstellung erfolgen.

Nachfolgende Abbildung zeigt exemplarisch die Ergebnisse der agentenspezifischen automatisierten Auswertung der Telefongespräche:

Abb. 5: Agentenspezifische Auswertung eines Telefonats.
Quelle: itCampus Software- und Systemhaus GmbH.

Aus Sicht des Datenschutzes kann die in Echtzeit ablaufende automatisierte Gesprächsauswertung eine zulässige Möglichkeit darstellen, die Qualität der Telefonate zu überprüfen. Der Eingriff in das informationelle Selbstbestimmungsrecht der Callcenter-Mitarbeiter ist in diesem Fall gering und hinzunehmen, wenn

- die Agenten von der Durchführung dieser Kontrollmaßnahme Kenntnis haben,
- die Auswertung der durch die Kontrolle erlangten Ergebnisse nur stichprobenweise erfolgt und
- eine regelmäßige Löschung der Kontrollergebnisse durchgeführt wird.

Eine derart gestaltete Kontrollmaßnahme lässt sich durch § 32 Abs. 1 Satz 1 BDSG legitimieren. Wie bereits bei den alternativen Kontrollen aufgezeigt wurde, sind bestimmte Verhaltens- oder Leistungskontrollen – bis zu einem gewissen Grad – zur Durchführung des Beschäftigungsverhältnisses erforderlich.

Bei der vorgesehenen automatisierten Gesprächsauswertung wird lediglich festgestellt, ob der Callcenter-Mitarbeiter sämtliche relevanten Informationen an den Kunden heranträgt, und ob er dies in einer angemessenen Sprechgeschwindigkeit ausführt. Es sind insoweit nur einzelne, aber für den Gesprächserfolg essentielle Wörter von der Kontrolle betroffen. Alles was zwischen diesen Schlüsselwörtern gesprochen wird, unterliegt nicht der Überprüfung. Der Callcenter-Agent vermag das Gespräch mit Kunden situationsbedingt zu gestalten und individuelle Akzente zu setzen. Kunden können beispielsweise mit Zwischenfragen, für deren Beantwortung in der Regel kein vorgegebener Gesprächsleitfaden vorliegt, erheblichen Einfluss auf den Gesprächsinhalt und -verlauf nehmen.

Was die Validität der automatisiert ermittelten Gesprächsergebnisse anbelangt, muss eine Fehlerrate von etwa 5 % berücksichtigt werden. Eine undeutliche Aussprache des Callcenter-Agenten oder Störgeräusche können dazu führen, dass die Spracherkennung einzelne Wörter nicht oder nicht eindeutig erkennt. Auch eine Funktionsstörung des Spracherkennungsmoduls kommt grundsätzlich als Fehlerquelle in Betracht. Aus diesen Gründen sind bei anhaltend schlechten Ergebnissen eines Mitarbeiters, die die automatisierte Auswertung ergibt, geeignete Maßnahmen zu ergreifen, die der Validierung der Ergebnisse dienen. Zu nennen sind

- Konfrontation des entsprechenden Callcenter-Mitarbeiters mit den negativen Resultaten und Einräumen einer Möglichkeit zur Stellungnahme,
- Durchführung anlassbezogener (verdeckter) Mithörvorgänge und
- Anhören gegebenenfalls vorliegender Telefonatmitschnitte – deren zulässige Aufzeichnung vorausgesetzt –, bei denen negative Resultate festgestellt wurden.

Obwohl die Vorschrift des § 6a BDSG nicht auf die automatisierte Gesprächsauswertung anwendbar ist, entspricht die dargestellte Vorgehensweise im Kern seinem Schutzgedanken. Die Regelung soll allgemein verhindern, dass Menschen einer Entscheidung unterworfen sind, die ausschließlich durch elektronische Datenverarbeitung getroffen wurde.[556] Die in § 6a Abs. 1 Satz 1 BDSG geforderte Bewertung von Persönlichkeitsmerkmalen liegt mit einer Beurteilung der beruflichen Leistungsfähigkeit und des Verhaltens vor.[557] Insoweit wird die automatisierte Gesprächsauswertung eingeschlossen. § 6a BDSG ist jedoch in diesem Fall nicht anwendbar, da keine automatisiert getroffene *Entscheidung* aus den Auswertungsergebnissen resultiert. Die Ergebnisse selbst stellen keine Entscheidung dar, sie bestehen vielmehr in einer Leistungsbeurteilung. Selbst unter der Prämisse, dass die Auswertungsergebnisse eine Entscheidung im Sinne des § 6a BDSG wären, obliegt es dennoch dem Vorgesetzten, über das weitere (arbeitsrechtliche) Vorgehen zu entscheiden; die Letztverantwortung liegt also noch immer bei einem Menschen. Insbesondere der Tatsache, dass sich eine bestimmte Fehlerwahrscheinlichkeit bei der Worterkennung nicht vermeiden lässt, wird mit den oben dargestellten Handlungsalternativen ausreichend Rechnung getragen.

Die nachfolgende Darstellung zeigt beispielhaft die Erkennung bestimmter Schlüsselwörter durch das Analysemodul, die im Gespräch genannt werden müssen:

[556] Dazu ausführlich Kapitel 3.1.1.4.4.2 „Automatisierte Einzelentscheidung“.
[557] *Bergmann/Möhrle/Herb*, BDSG, 42. Ergänzungslieferung, Stand: Januar 2011, § 6a Rn. 8.

Abb. 6: Automatische Erkennung von Schlüsselwörtern.
Quelle: itCampus Software- und Systemhaus GmbH.

Eine weitere, mit der automatisierten Gesprächsauswertung verknüpfte Funktion besteht in der emotionsinduzierten Rückmeldung an den Callcenter-Mitarbeiter. Diese gibt dem Mitarbeiter über das Frontend-System ein Feedback über den emotionalen Verlauf des Telefongesprächs und kann beispielsweise zwischen einem harmonischen und einem angespannten Gespräch sowie zwischen einzelnen Gesprächsphasen unterscheiden.

Situationsabhängig wird dem Callcenter-Mitarbeiter durch den Stress-Level-Indikator signalisiert, welche Gesprächsatmosphäre aktuell herrscht.[558] Befindet sich der Wert im negativen Anzeigebereich, so sollte der Agent deeskalierend auf den Kunden einwirken. Als Hilfestellung können in solchen Situationen entsprechende Gesprächsleitfäden eingeblendet werden.

Für Berechtigte, wie Vorgesetzte und Trainer, sind die Bewertungsergebnisse in Bezug auf die Emotionalität der Telefongespräche agentenindividuell einsehbar. Daraus lassen sich Rückschlüsse auf die Freundlichkeit und unter Umständen auf die Serviceorientierung des einzelnen Agenten ziehen. Hat ein Mitarbeiter durch-

[558] S. dazu Kapitel 3.1.1.4.3 „Sprach- und Emotionserkennung“.

gängig schlechte Bewertungen erhalten, liegt die Vermutung nahe, dass er über eine unzureichende Arbeitsmotivation verfügt. In einem solchen Fall kommen die bereits im Hinblick auf die automatisierte Spracherkennung aufgezählten Maßnahmen zur Überprüfung dieses Umstands in Betracht.

Die automatisierte Emotionserkennung unterscheidet sich im Vergleich zur automatisierten Gesprächsauswertung datenschutzrechtlich nicht, wenn sie unter denselben Voraussetzungen vollzogen wird. Insofern lässt sich auf die Ausführungen zur Zulässigkeit der automatisierten Gesprächsauswertung verweisen.

4.2 Weitere Vorgaben zum Beschäftigtenschutz

4.2.1 Beteiligung der Beschäftigtenvertretung

Ganz allgemein dienen das Betriebsverfassungs- und Personalvertretungsrecht in erster Linie dem Beschäftigtenschutz. Die Beschäftigten benötigen diesen Schutz, da sie im Verhältnis zu ihrem Arbeitgeber oder Dienstherrn in persönlicher und wirtschaftlicher Abhängigkeit stehen. Der Arbeitgeber oder Dienstherr verfügt über die Dispositionsbefugnis im Hinblick auf ihre Arbeitskraft. Um einen Ausgleich des Machtungleichgewichts zwischen den Arbeitsvertragsparteien herbeizuführen, wird die Kompetenz zur Alleinentscheidung durch den Arbeitgeber begrenzt.[559] Im Übrigen soll eine vertrauensvolle Zusammenarbeit zwischen Arbeitgeber und Arbeitnehmervertretung, einschließlich ihrer jeweiligen Verbände, ermöglicht und gefördert werden.

Der Betriebsrat vertritt die Interessen der Arbeitnehmer und setzt diese gegenüber dem Arbeitgeber durch.[560] Ihm kommt gemäß § 80 Abs. 1 Nr. 1 BetrVG die wichtige allgemeine Aufgabe zu, darüber zu wachen, dass die zu Gunsten der Arbeitnehmer wirkenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen eingehalten werden. Die vergleichbare Vorschrift im Bundespersonalvertretungsrecht findet sich in § 68 Abs. 1 Nr. 2 BPersVG. Es bestehen diesbezüglich keine relevanten Abweichungen, der Schutzauftrag ist grundsätzlich derselbe.[561] Auch die Personalvertretungsgesetze der Länder haben die in § 68 BPersVG getroffenen Regelungen im Wesentlichen übernommen.[562]

[559] *Fitting et al*., HK BetrVG, § 1 Rn. 1 f.; ErfK/*Koch*, BetrVG, 11. Aufl. 2011, § 1 Rn. 1.
[560] MHA/*Matthes*, Band 2, 3. Aufl. 2009, § 236 Rn. 1.
[561] *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 2 Rn. 144.
[562] *Gräfl*, in: Richardi/Dörner/Weber (Hrsg.), Kommentar zum Personalvertretungsrecht, 3. Aufl. 2008, § 68 Rn. 112 f.

§ 1 Abs. 1 Satz 1 BetrVG sieht vor, dass in Betrieben mit in der Regel wenigstens fünf ständig wahlberechtigten Arbeitnehmern – von denen drei wählbar sind – Betriebsräte gewählt werden. Die Wahl eines Betriebsrats liegt im freien Ermessen der Arbeitnehmer, obgleich der Wortlaut dieser Vorschrift nahe legt, sie sei verpflichtend.[563] Die vergleichbare personalvertretungsrechtliche Vorschrift ist im § 12 Abs. 1 BPersVG verankert: Hiernach werden in allen Dienststellen, in denen in der Regel mindestens fünf Wahlberechtigte beschäftigt und von denen drei wählbar sind, Personalräte gebildet.

Generell stehen dem Betriebsrat folgende Beteiligungsrechte in betrieblichen Angelegenheiten zu:

- Unterrichtungsrechte (zum Beispiel §§ 80 Abs. 2 Satz 1, 99 Abs. 1 Satz 1, 111 BetrVG),
- Anhörungs- und Vorschlagsrechte (zum Beispiel §§ 92 Abs. 2, 102 BetrVG),
- Beratungsrechte (zum Beispiel §§ 90 Abs. 2, 111 BetrVG) und
- Mitbestimmungsrechte (zum Beispiel Zustimmungsverweigerungsrechte § 99 Abs. 2 BetrVG, Zustimmungserfordernisse und Initiativrechte §§ 87 Abs. 1, 103 BetrVG).[564]

Seine Beteiligungsrechte beziehen sich neben allgemeinen Aufgaben auf die Bereiche soziale Angelegenheiten, Gestaltung des Arbeitsplatzes, des Arbeitsablaufs und der Arbeitsumgebung sowie personelle und wirtschaftliche Angelegenheiten.[565]

Im Betriebsverfassungsrecht sind für bestimmte Sachverhalte mehr oder weniger starke Mitbestimmungsrechte des Betriebsrats verankert, während das Personalvertretungsrecht des Bundes bei denselben Gegebenheiten schwächere Beteiligungsrechte vorsieht. Demgegenüber bestehen jedoch Mitbestimmungsrechte aus dem Bundespersonalvertretungsrecht, die im Betriebsverfassungsrecht keine Entsprechung finden.[566] Die Personalvertretungsgesetze der Länder weichen in einzelnen Vorschriften teilweise stark voneinander ab.[567]

Wie bereits im Kaptitel 3.1.1.2.1 „Erlaubnis aus einer Betriebs- oder Dienstvereinbarung“ dargelegt wurde, verfügt die Beschäftigtenvertretung über erhebliche Ein-

[563] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 112.
[564] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 112 f.; zu weiteren Beteiligungsrechten des Betriebsrats außerhalb der Betriebsverfassung *Pulte*, NZA 1996, 913 ff.
[565] *Preis*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 28. Ergänzungslieferung 2011, Teil 22.2 Rn. 73.
[566] *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 2 Rn. 147.
[567] Einen Überblick hierüber gibt *Thannheiser*, Computer Fachwissen 3/1999, 13 (16 ff.).

flussmöglichkeiten in Bezug auf den innerorganisatorischen Beschäftigtendatenschutz.

Das bedeutendste Mitbestimmungsrecht des Betriebsrats im Zusammenhang mit der Einführung und Anwendung des Gesprächsmanagement-Systems im Callcenter findet sich in § 87 Abs. 1 Nr. 6 BetrVG. Hiernach kommt dem Betriebsrat ein Mitbestimmungsrecht zu, soweit keine diesbezügliche gesetzliche oder tarifliche Regelung existiert. Falls der Callcenter-Betreiber das Gesprächsmanagement-System ohne die Zustimmung des Betriebsrats einführt, kann der Betriebsrat die Beseitigung und die Unterlassung der Benutzung des Systems durchsetzen. Die Erlaubnis des Betriebsrats ist vor der Einführung der Technik einzuholen. Liegt eine solche nicht vor – unerheblich, ob die Zustimmung nicht eingeholt oder ob sie verweigert wurde –, ist deren Einführung rechtswidrig. In einem solchen Fall besteht für die Mitarbeiter keine Verpflichtung, das Gesprächsmanagement-System zu nutzen. Trotz dieses Leistungsverweigerungsrechts hinsichtlich der Nutzung der unzulässig eingeführten Technik gilt der Anspruch auf Entgeltfortzahlung der Callcenter-Mitarbeiter weiter.[568] Die entsprechende Vorschrift im Personalvertretungsrecht auf Bundesebene findet sich in § 75 Abs. 3 Nr. 17 BPersVG.

4.2.2 Bildschirmarbeitsverordnung

Die zunehmende Verbreitung moderner Computer-, Informations- und Kommunikationstechniken am Arbeitsplatz führte zu einer steigenden Zahl an eingesetzten visuellen Ausgabegeräten (Bildschirmgeräte). Neben zahlreichen Vorzügen der Techniken etablierten sich gleichzeitig spezifische Gesundheitsprobleme durch die dauerhafte Nutzung der Bildschirme. Solche negativen Auswirkungen sind primär Augenbeschwerden, Kopfschmerzen, körperliche Verspannungen, Schmerzen und Abnutzung der Muskeln, Sehnen sowie Gelenke von Armen und Händen der Beschäftigten. Da das damalige Arbeitsschutzrecht noch keine Regelungen zum Schutz der Arbeitnehmer vor gesundheitlichen Gefahren enthielt, die von Bildschirmgeräten ausgehen, musste eine entsprechende Verordnung erst noch auf den Weg gebracht werden.[569]

Generell gilt § 18 ArbSchG als Ermächtigungsgrundlage für den Erlass von Verordnungen, die zur Sicherung und Verbesserung des Gesundheitsschutzes und der

[568] *Fitting et al.*, HK BetrVG, § 87 Rn. 256; *Besgen/Prinz*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 2 Rn. 23 ff.
[569] *Kreizberg*, in: Kollmer/Klindt (Hrsg.), Arbeitsschutzgesetz, 2. Aufl. 2011, BildscharbV, Rn. 1 ff.

Sicherheit der Beschäftigten am Arbeitsplatz dienen. Die Bildschirmarbeitsverordnung wurde auf Grundlage dieser Vorschrift erlassen. Sie setzt die Richtlinie 90/270/EWG über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit an Bildschirmgeräten um und regelt insbesondere die Anforderungen an die Gestaltung der Arbeitsplätze, die mit einem Bildschirmgerät ausgestattet sind. Ihr Gültigkeitsbereich erstreckt sich grundsätzlich auf alle Arbeitsplätze mit Bildschirmgeräten. Ausnahmen sind ausdrücklich in § 1 Abs. 2 Nr. 1 - 6 BildscharbV aufgeführt. Geschützt werden nach § 2 Abs. 3 BildscharbV nur solche Arbeitnehmer, die gewöhnlich zu einem nicht unwesentlichen Teil ihrer Arbeitszeit das Bildschirmgerät einsetzen. Das *BAG*[570] entschied zum Begriff der Versetzung, dass von einem wesentlichen Anteil bereits bei etwa einem Fünftel der täglichen oder wöchentlichen Arbeitszeit auszugehen sei.[571]

Die Verordnung enthält in § 3 Vorgaben zur Beurteilung der Arbeitsbedingungen, die eine Evaluation der existierenden Gesundheits- und Sicherheitsaspekte betreffen. Darüber hinaus werden durch § 4 BildscharbV Anforderungen an die Gestaltung der Bildschirmarbeitsplätze gestellt. In § 5 BildscharbV sind Forderungen bezüglich des Arbeitsablaufs enthalten, Pausen und Mischarbeit betreffend, die der Belastungsreduktion der Mitarbeiter dienen. Ferner beinhaltet § 6 BildscharbV eine Vorschrift zur Untersuchung der Augen und des Sehvermögens.[572]

Konkrete Anforderungen, die ein Bildschirmarbeitsplatz erfüllen muss, enthält der Anhang zur Bildschirmarbeitsverordnung. Die dort aufgeführten Erfordernisse beziehen sich auf die Komplexe Bildschirmgerät und Tastatur (zum Beispiel Größe der Zeichendarstellung und ergonomische Bedienmöglichkeit), Arbeitsumgebung (wie Bewegungsfreiheit), Zusammenwirken zwischen Mensch und Arbeitsmittel (beispielsweise Benutzerfreundlichkeit) sowie sonstige Arbeitsmittel (etwa adäquate Arbeitsfläche).[573]

Darüber hinaus existiert ein Mitbestimmungsrecht des Betriebsrats gemäß § 87 Abs. 1 Nr. 7 BetrVG bezüglich Regelungen über den Gesundheitsschutz im Rahmen gesetzlicher Vorschriften oder im Rahmen von Unfallverhütungsvorschriften.[574] Das Mitbestimmungsrecht erstreckt sich auf Regelungen über die Arbeitsunterbrechung durch andere Tätigkeiten oder Pausen, auf Details zur Augenuntersuchung sowie

[570] *BAG* v. 2.4.1996, NZA 1997, 112.
[571] *Aufhauser*, Das Deutsche Bundesrecht, BildscharbV, 2011, § 2.
[572] Hierzu ausführlich *Opfermann/Rückert*, AuA 1997, 69 ff.
[573] *Kilian*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 29. Ergänzungslieferung, Stand: Februar 2011, Kollektivarbeitsrechtliche Probleme der Informationstechnologie im Betrieb, Rn. 114.
[574] *BAG* v. 2.4.1996, NZA 1996, 998.

auf Gestaltungsfragen der Bildschirmarbeitsplätze.[575] Der Personalrat besitzt ein Mitbestimmungsrecht aus § 75 Abs. 3 Nr. 11 BPersVG im Hinblick auf Maßnahmen zur Verhinderung von Dienst- und Arbeitsunfällen und anderen Gesundheitsschädigungen. Die Personalvertretungsgesetze der Länder enthalten vergleichbare Regelungen.

Ein weiteres Mitbestimmungsrecht ergibt sich aus § 87 Abs. 1 Nr. 6 BetrVG, der die Einführung und Anwendung technischer Einrichtungen, die sich zur Überwachung von Verhalten oder Leistung der Arbeitnehmer eignen[576], betrifft. Dieses Recht des Betriebsrats wird relevant, wenn etwa Eingabefehler oder Eingabegeschwindigkeit am Bildschirmarbeitsgerät festgehalten und ausgewertet werden können.[577] Das bundespersonalvertretungsrechtliche Pendant zu dieser Vorschrift findet sich in § 75 Abs. 3 Nr. 17 BPersVG. In den Landespersonalvertretungsgesetzen sind ebenfalls entsprechende Vorschriften festgeschrieben.

Was den Aspekt der Überwachungsmöglichkeit durch den Arbeitgeber anbelangt, so enthält die Bildschirmarbeitsverordnung in Nr. 22 ihres Anhangs eine diesbezügliche Vorschrift. Kontrollen in qualitativer und quantitativer Hinsicht dürfen durchgeführt werden, wenn die Benutzer davon wissen.[578] Die Kenntnis der Kontrolle ist weit auszulegen: Es reicht aus, wenn sich Mitarbeiter allgemein bewusst sind, dass ihre Leistung technisch überwacht wird oder überwacht werden kann. Der Arbeitgeber muss auch nicht auf konkrete Kontrollaktivitäten hinweisen, sondern es genügt, dass dieses Wissen beispielsweise aus allgemeinen Erfahrungssätzen hergeleitet werden kann.[579]

Das im Callcenter eingesetzte Frontend-System, das den Berater im Gespräch unter anderem mit hilfreichen Informationen unterstützt, erfüllt die Voraussetzungen eines Bildschirmarbeitsplatzes im Sinne der Rechtsverordnung. Folglich müssen Callcenter-Betreiber, die das Gesprächsmanagement-System einsetzen, die Vorschriften der Bildschirmarbeitsverordnung beachten.

[575] *Kreizberg*, in: Kollmer/Klindt (Hrsg.), Arbeitsschutzgesetz, 2. Aufl. 2011, BildscharbV, Rn. 14; *Fabricius*, BB 1997, 1254 ff.
[576] *BAG* v. 9.9.1975, NJW 1976, 261 st. Rspr.
[577] *Kreizberg*, in: Kollmer/Klindt (Hrsg.), Arbeitsschutzgesetz, 2. Aufl. 2011, BildscharbV, Rn. 15.
[578] *Duisberg/Picot*, CR 2009, 823 (826); *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 39.
[579] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 39.

4.3 Rechte des Arbeitgebers

Der Arbeitgeber ist eigenständiger Träger von Grundrechten und verfügt somit unter anderem über verschiedene Rechte hinsichtlich der Begründung, Ausgestaltung und Beendigung von Beschäftigungsverhältnissen.[580] Diese resultieren insbesondere aus der allgemeinen Handlungsfreiheit gemäß Art. 2 Abs. 1, der Berufsfreiheit gemäß Art. 12 Abs. 1 und dem Eigentumsrecht gemäß Art. 14 GG.

Anzumerken ist im Zusammenhang mit den Rechten des Arbeitgebers, dass öffentliche Callcenter sowohl Angestellte als auch – in sehr seltenen Fällen – Beamte beschäftigen; falls Beamte im Callcenter zum Einsatz kommen, arbeiten sie in der Regel als Führungskräfte. Aus diesem Grund konzentrieren sich hier die Aussagen auf das Weisungsrecht und die Sanktionsrechte gegenüber Angestellten. Dabei gelten dieselben Rechte für nichtöffentliche wie für öffentliche Callcenter-Betreiber.

Auch Beamte sind gemäß § 35 BeamtStG weisungsgebunden. Bei Dienstvergehen durch Beamte greifen jedoch nicht die „klassischen“ Sanktionsrechte. Dienstvergehen werden mit Disziplinarmaßnahmen geahndet. Disziplinarische Maßnahmen gegen Beamte sind nach § 5 BDG

- Verweis,
- Geldbuße,
- Kürzung der Dienstbezüge,
- Zurückstufung und
- Entfernung aus dem Beamtenverhältnis.

Auf Landesebene gibt es weitgehend vergleichbare Bestimmungen.

Nachstehend folgen Ausführungen zu den wichtigsten Rechten des Arbeitgebers, der das Callcenter betreibt, gegenüber der Mitarbeitergruppe der Angestellten.

4.3.1 Weisungsrecht

Der Arbeitgeber besitzt gemäß § 106 GewO ein Weisungsrecht – auch Direktionsrecht genannt – im Hinblick auf die detaillierte Ausgestaltung des Arbeitsverhältnisses. Da der Arbeitsvertrag nicht jegliche Leistungspflicht des Arbeitnehmers explizit regeln kann, steckt er regelmäßig nur den Rahmen ab, innerhalb dessen das

[580] AnwK-ArbR/*Wilms*, GG, Art. 12 Rn. 60.

Arbeitsverhältnis durch Weisungen näher bestimmt werden kann.[581] Dem Arbeitgeber steht es zu, Arbeitsinhalt, -zeit und -ort nach billigem Ermessen zu konkretisieren und festzulegen. Billiges Ermessen liegt dann vor, wenn die wesentlichen Umstände des Falles abgewogen werden und beiderseitige Interessen angemessene Berücksichtigung finden.[582] Das Weisungsrecht verkörpert ein einseitiges Leistungsbestimmungsrecht im Sinne der §§ 315 ff. BGB.

Der Beschäftigte begibt sich durch Abschluss des Arbeitsvertrags in die Weisungsabhängigkeit vom Arbeitgeber. Innerhalb des Arbeitsverhältnisses verfügt der Arbeitgeber im Rahmen der arbeitsrechtlichen Grenzen über die Dispositionsbefugnis der Arbeitskraft des Beschäftigten.[583] Dies gilt jedoch nicht unbeschränkt; das Weisungsrecht findet dort seine Grenze, wo Bestimmungen des Arbeitsvertrags, einer Betriebs- oder Dienstvereinbarung, eines Tarifvertrags oder gesetzliche Vorschriften die Arbeitsleistung festlegen. Je enger derartige Festlegungen gefasst sind, desto geringer ist der arbeitgeberseitige Spielraum zur Ausübung des Weisungsrechts.[584] Gesetzliche Vorgaben, die sich restriktiv auf die Direktionsbefugnis auswirken, finden sich insbesondere in Arbeitnehmerschutz- und Arbeitszeitvorschriften.[585]

Da es bei der Wahrnehmung des Direktionsrechts immer zu Kollisionen mit grundrechtlich abgesicherten Rechtspositionen des Arbeitnehmers kommt, muss § 241 Abs. 2 BGB beachtet werden.[586] Nach dieser Vorschrift sind auf Rechte, Rechtsgüter und Interessen des Arbeitnehmers Rücksicht zu nehmen. Im Übrigen entfalten auch Grundrechte ihre Wirkung mittelbar auf das Arbeitsverhältnis.[587] So dient § 75 Abs. 2 BetrVG auch dem Schutz des informationellen Selbstbestimmungsrechts der Mitarbeiter in privatwirtschaftlichen Unternehmen. § 68 Abs. 1 Nr. 2 BPersVG sowie die entsprechenden Bestimmungen der Landespersonalvertretungsgesetze schützen die informationelle Selbstbestimmung der im öffentlichen Bereich Beschäftigten.[588]

[581] *Neumann*, in: Landmann/Rohmer, GewO, Band I, 57. Ergänzungslieferung, Stand: 1. Juli 2010, § 106 Rn. 7 f.; *Wank*, in: Tettinger/Wank, GewO, 7. Aufl. 2004, § 106 Rn. 3; ErfK/*Preis*, GewO, 11. Aufl. 2011, § 106 Rn. 2.
[582] *Neumann*, in: Landmann/Rohmer, GewO, Band I, 57. Ergänzungslieferung, Stand: 1. Juli 2010, § 106 Rn. 12.
[583] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 114.
[584] ErfK/*Preis*, GewO, 11. Aufl. 2011, § 106 Rn. 5.
[585] *Wank*, in: Tettinger/Wank, GewO, 7. Aufl. 2004, § 106 Rn. 13 ff.
[586] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, GewO, § 106.
[587] *BVerfG* v. 15.1.1958, GRUR 1958, 254.
[588] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 247.

Die Technik des Gesprächsmanagement-Systems verkörpert ein Arbeitsmittel, mit dem der Mitarbeiter seine Arbeitsaufgabe zu erfüllen hat; insofern ist mindestens das „Wie“ der Arbeitserledigung betroffen, welches sich auf den inhaltlichen Teil der Direktionsbefugnis bezieht. Wenn die Anweisung zur Benutzung des Gesprächsmanagement-Systems innerhalb des arbeitsvertraglichen Spielraums liegt und dabei nicht gegen bestehende Gesetze verstoßen wird, sind Weisungen an den Callcenter-Mitarbeiter zur Nutzung dieses Systems vom Arbeitsvertrag gedeckt.

4.3.2 Sanktionsrechte

Bei arbeitsvertraglichen und anderen Pflichtverletzungen durch die Mitarbeiter des Callcenters, die etwa in der Nichteinhaltung von Verboten, im unsachgemäßen Umgang mit der eingesetzten Technik, in Verstößen gegen Anweisungen oder konkrete Nutzungsregelungen sowie in der Vornahme strafbarer Handlungen bestehen können, steht es dem Arbeitgeber zu – in Abhängigkeit von der Schwere der Pflichtverletzung – Sanktionen zu verhängen. Nachfolgend werden die bedeutendsten Sanktionsmittel[589] des Callcenter-Betreibers kurz aufgezeigt.

4.3.2.1 Ermahnung

Die Ermahnung stellt eine durch den Gläubiger an den Schuldner gerichtete eindeutige und bestimmte Aufforderung zur Erbringung der geschuldeten Leistung dar.[590] Gerade bei geringfügigen Verstößen bietet es sich für den Arbeitgeber an, den betreffenden Mitarbeiter lediglich zu ermahnen.[591] Auch für die Fälle, in denen der Nachweis einer Pflichtverletzung des Callcenter-Mitarbeiters nicht eindeutig gelingt, verkörpert die Ermahnung ein geeignetes Sanktionsinstrument, das dem Arbeitnehmer gleichzeitig zu erkennen gibt, dass entsprechende Verhaltensweisen nicht geduldet werden. Eine Ermahnung kann ferner dann in Betracht kommen, wenn gegen eine bestimmte Arbeitsanweisung – wie eine geänderte Vorgabe zur Benutzung des Gesprächsmanagement-Systems – verstoßen wurde, die der Mitarbeiter jedoch nicht kannte. Sie erfordert weder eine bestimmte Fristsetzung noch eine Androhung negativer arbeitsrechtlicher Konsequenzen.[592]

---

[589] Die Darstellung der Sanktionsmittel basiert im Wesentlichen auf *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 91 ff.
[590] *von Hase*, NJW 2002, 2278 (2280).
[591] Moll/*Eisenbeis*, MAH Arbeitsrecht, § 16 Rn. 20.
[592] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 91.

4.3.2.2 Abmahnung

Eine Legaldefinition für den Begriff der Abmahnung existiert nicht. Der Abmahnung kommt allerdings im Arbeitsrecht eine besondere Bedeutung zu: Einerseits gilt sie als grundsätzliche Voraussetzung für eine spätere verhaltensbedingte Kündigung, andererseits ist sie gleichzeitig auf den Fortbestand des Arbeitsverhältnisses gerichtet – sie erfüllt insofern eine Doppelfunktion. Da die Abmahnung regelmäßig einer Kündigung aus verhaltensbedingten Gründen vorausgehen muss, sind insbesondere ihre notwendigen formellen Voraussetzungen zu berücksichtigen.[593]

Die rechtswirksame Abmahnung muss mindestens die

- Darlegung des konkret zu bezeichnenden Fehlverhaltens,
- Rüge des Fehlverhaltens,
- Aufforderung zu künftigem vertragskonformem Verhalten und die
- unmissverständliche Androhung arbeitsrechtlicher Konsequenzen für den Wiederholungsfall

enthalten.[594]

Generell besteht für den Ausspruch einer Abmahnung Formfreiheit, sie kann folglich auch mündlich erteilt werden. Davon ist jedoch dringend abzuraten. Zur Dokumentation und ausreichenden Beweissicherung ist die schriftliche Ausfertigung notwendig.[595]

Für den Ausspruch der Abmahnung existiert keine Ausschlussfrist, innerhalb derer der Mitarbeiter abzumahnen ist. Als Empfehlung gilt dennoch, die Abmahnung innerhalb von zwei Wochen nach Kenntnisnahme der Pflichtverletzung zu erteilen, nicht zuletzt um der ihr innewohnenden Warnfunktion Nachdruck zu verleihen.[596]

4.3.2.3 Kürzung der Vergütung

Der Callcenter-Betreiber verfügt über das Recht, die Gegenleistung – namentlich die Vergütung – für die geschuldete Arbeit entsprechend zu kürzen, sollten Arbeitnehmer ihrer Arbeitspflicht in nicht genügendem Maße nachkommen. Da das Ar-

[593] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 91.
[594] *Hunold*, NZA-RR 2000, 169 (170 ff.).
[595] Moll/*Eisenbeis*, MAH Arbeitsrecht, § 16 Rn. 5.
[596] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 91.

beitsverhältnis nach § 611 BGB ein synallagmatisches Austauschverhältnis darstellt, können Arbeitnehmer, die ihre Privatangelegenheiten im Unternehmen während der Arbeitszeit verrichten, nicht den vollen Vergütungsanspruch geltend machen.[597] Im Ergebnis ist es dasselbe, wenn die Mitarbeiter des Callcenters durch Betrug bei der Zeiterfassung den Betrieb vorzeitig verlassen, oder wenn der Arbeitszeitdiebstahl durch die Erledigung von Privatangelegenheiten während der Arbeitszeit realisiert wird.

Nachprüfen lässt sich die erbrachte Arbeitsleistung der Arbeitnehmer im Callcenter relativ leicht anhand bestimmter Kennzahlen, die etwa mithilfe der Telefonanlage des Gesprächsmanagement-Systems gebildet werden können. Eine Größe kann beispielsweise die Anzahl bearbeiteter Anrufe innerhalb eines bestimmten Zeitraums darstellen. Auch bei Anwendung einer nur stichprobenweise stattfindenden Kontrolle besteht eine hohe Wahrscheinlichkeit, Mitarbeiter zu entdecken, die regelmäßig ihre Arbeitsaufgabe vernachlässigen.

4.3.2.4 Ordentliche Kündigung

Die ordentliche Kündigung des Arbeitsverhältnisses bestimmt sich nach den Vorschriften der §§ 620 ff. BGB. Wichtig ist in diesem Zusammenhang, dass gemäß § 23 Abs. 1 Satz 3 KSchG in Betrieben mit regelmäßig mehr als zehn Arbeitnehmern weitere Vorschriften des Kündigungsschutzgesetzes zu beachten sind. Sonderregelungen gelten für Arbeitsverhältnisse, die vor dem 31. Dezember 2003 bestanden haben. Der Grund für die zusätzlichen Kündigungsschutzvorschriften des Kündigungsschutzgesetzes ist, die Arbeitnehmer vor sozial ungerechtfertigten Kündigungen zu schützen.[598]

Falls der erweiterte Anwendungsbereich des Kündigungsschutzgesetzes eröffnet ist, so gilt – problembezogen – nach § 1 Abs. 2 Satz 1 KSchG die Kündigung als sozial gerechtfertigt, wenn sie durch Gründe, die im Verhalten des Callcenter-Mitarbeiters liegen, bedingt ist.[599] Der ordentlichen, fristgerechten Kündigung muss in der Regel eine einschlägige Abmahnung vorausgehen. Der entsprechende Arbeitnehmer soll die Möglichkeit haben, sein Verhalten zu korrigieren. Die Rechtfertigung der Kündigung besteht in einer negativen Zukunftsprognose. Für den Fall, dass der Kündigung keine einschlägige oder eine nicht wirksame Abmahnung vorausging, fehlt es

[597] *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 3. Aufl. 2010, Rn. 379.
[598] ErfK/*Kiel*, KSchG, 11. Aufl. 2011, § 23 Rn. 9; *Zundel*, NJW 2006, 3467 (3468); *Freund/Knoblauch/Eisele*, Praxisorientierte Personalwirtschaftslehre, 6. Aufl. 2003, 54.
[599] Ausführlich zur verhaltensbedingten Kündigung *Berkowsky*, NZA-RR 2001, 57 ff.

an einer Legitimation zur Kündigung. Im Ergebnis bleibt eine solche Kündigung unwirksam.[600] Existiert ein Betriebs- oder Personalrat, ist dieser hinzuzuziehen. Die Anhörung gilt als zwingende Wirksamkeitsvoraussetzung für die Kündigung.[601]

Selbst nur geringfügige Pflichtverletzungen im Kontext der Nutzung des Gesprächsmanagement-Systems können in ihrer Summe dazu führen, dass sie erheblich ins Gewicht fallen.[602] Will der Callcenter-Betreiber eine Kündigung darauf stützen, muss er jedes pflichtwidrige abmahnungsrechtfertigende Verhalten seiner Mitarbeiter abmahnen, um die spätere ordentliche Kündigung überhaupt auf eine substanziierte Grundlage stellen zu können.

Für ein derart gravierendes Fehlverhalten, dass eine Abmahnung ausnahmsweise entbehrlich ist, kommt regelmäßig die außerordentliche Kündigung in Betracht.

4.3.2.5 Außerordentliche Kündigung

Eine außerordentliche Kündigung gemäß § 626 BGB erlaubt dem Callcenter-Betreiber die sofortige Trennung vom Mitarbeiter, ohne eine Frist einhalten zu müssen.[603] Sie ist gemäß § 626 Abs. 1 BGB aus wichtigem Grund zulässig, wenn Tatsachen vorliegen, bei denen dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und beiderseitiger Interessenabwägung der Fortbestand des Arbeitsverhältnisses bis zum Ende der Kündigungsfrist beziehungsweise bis zur Beendigung eines befristeten Arbeitsvertrags nicht zugemutet werden kann.[604] Begeht der Callcenter-Mitarbeiter mittels des Gesprächsmanagement-Systems Straftaten oder schwerwiegende schuldhafte Pflichtverletzungen im Arbeitsverhältnis, kann die außerordentliche Kündigung eine angemessene Reaktion des Arbeitgebers darstellen.[605] Sie verkörpert das schärfste arbeitsrechtliche Sanktionsmittel des Arbeitgebers.

Die in § 626 BGB geregelte außerordentliche Kündigung kann nur bei Vorliegen eines wichtigen Grundes ausgesprochen werden. Ob ein solcher gegeben ist, wird anhand einer zweistufigen Prüfung ermittelt:

---

[600] *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 94.
[601] *Bernhardt/Barthel*, AuA 2008, 150 (152); *Benecke*, in: Richardi/Dörner/Weber (Hrsg.), Kommentar zum Personalvertretungsrecht, 3. Aufl. 2008, § 79 Rn. 11.
[602] *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 3 Rn. 196a.
[603] *Freund/Knoblauch/Eisele*, Praxisorientierte Personalwirtschaftslehre, 6. Aufl. 2003, 56.
[604] *Dörner*, in: Ascheid/Preis/Schmidt (Hrsg.), Kündigungsrecht, 3. Aufl. 2007, BGB, § 626 Rn. 6.
[605] *Kramer*, NZA 2004, 457 (461).

1. Auf der ersten Stufe erfolgt eine Untersuchung des Sachverhalts dahingehend, ob die begangene Pflichtverletzung einen wichtigen Grund an sich darstellen kann. Die besonderen Umstände des Einzelfalls werden auf dieser Stufe vollständig außer Acht gelassen.[606]
2. Die konkreten Umstände des Einzelfalls und die Interessen beider Vertragsparteien bilden die zweite Stufe der Beurteilung, ob eine außerordentliche Kündigung gerechtfertigt erscheint. In diesem Zusammenhang gilt es zu beachten, dass der Kündigungszweck nicht in der Sanktion der Pflichtverletzung besteht, sondern in der Vermeidung künftiger potenzieller Pflichtverletzungen.[607]

Darüber hinaus ist die zweiwöchige Ausschlussfrist gemäß § 626 Abs. 2 Satz 1 BGB einzuhalten. Diese Frist beginnt erst zu laufen, wenn der Kündigungsberechtigte die kündigungsrechtfertigenden Tatsachen möglichst abschließend aufgeklärt hat. Dazu soll auch der zu Kündigende selbst angehört werden.[608] Ferner gilt es, den Betriebs- oder Personalrat – sofern ein solcher besteht – anzuhören.

Es ist auf eine weitere Kündigungsform hinzuweisen, namentlich die (außerordentliche) Verdachtskündigung.[609] Sie kommt bereits beim bloßen Verdacht auf eine schwere Pflichtverletzung oder eine Straftat in Betracht. Die im Arbeitsverhältnis erforderliche Vertrauensgrundlage muss durch den Verdacht so erschüttert sein, dass eine weitere Zusammenarbeit nicht mehr zumutbar ist.[610] Dem Verdacht müssen objektive Tatsachen zu Grunde liegen, die den Ausspruch einer außerordentlichen Kündigung rechtfertigen.[611]

4.3.2.6 Schadenersatz

Potenzielle Schadenersatzansprüche des Callcenter-Betreibers gegenüber seinen Mitarbeitern können sich aus der vertraglichen oder deliktischen Haftung ergeben. Die Regelung des vertraglichen Schadenersatzanspruchs enthält § 280 Abs. 1 BGB. Erfasst werden damit grundsätzlich sämtliche Arten von Pflichtverletzungen. Diese Vorschrift muss im Arbeitsverhältnis i. V. m. § 619a BGB gesehen werden, wonach der Arbeitgeber die Pflichtverletzung sowie das Vertretenmüssen des Arbeitneh-

[606] *Bernhardt/Barthel*, AuA 2008, 150.
[607] *Bernhardt/Barthel*, AuA 2008, 150; *BAG* v. 31.5.2007, NZA 2007, 922.
[608] *Dörner*, in: Ascheid/Preis/Schmidt (Hrsg.), Kündigungsrecht, 3. Aufl. 2007, BGB, § 626 Rn. 125 ff.; *Besgen/Prinz*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 1 Rn. 115.
[609] Dazu ausführlich *Langner/Witt*, DStR 2008, 825 ff.; *Dörner*, NZA 1992, 865 ff.
[610] *Langner/Witt*, DStR 2008, 825.
[611] *Bernhardt/Barthel*, AuA 2008, 150 (153).

mers zu beweisen hat.[612] Der Anspruch des Arbeitgebers erstreckt sich auf den verursachten Schaden, der durch eine schuldhafte Verletzung der Haupt- oder Nebenleistungspflichten aus dem Arbeitvertrag durch den Arbeitnehmer entsteht.[613]

Ein deliktischer Schadenersatzanspruch kann aus einer unerlaubten Handlung gemäß § 823 Abs. 1 BGB resultieren. Von der Vorschrift sind nur absolute Rechte erfasst. Da ein Vermögensschaden, der nicht die Folge einer Eigentumsverletzung darstellt, kein absolutes Recht verkörpert, ist eine primäre deliktische Arbeitnehmerhaftung in Bezug auf das Vermögen des Arbeitgebers ausgeschlossen.[614] Eine vorsätzliche Schadenverursachung durch einen Mitarbeiter begründet sogar einen uneingeschränkten Haftungsanspruch, wenn sich der Vorsatz nicht nur auf die Pflichtverletzung selbst, sondern auch auf den Schadenseintritt erstreckt.[615]

4.3.2.7 Strafanzeige

Deckt der Callcenter-Betreiber zufällig oder durch Kontrollmaßnahmen strafbare Handlungen auf, die mittels des Gesprächsmanagement-Systems durch Mitarbeiter verübt wurden, sollte er diese bei den zuständigen Strafverfolgungsbehörden anzeigen. Zu den in Rede stehenden strafbaren Handlungen zählen in diesem Zusammenhang insbesondere die Verbreitung ehrverletzender, wahrheitswidriger oder beleidigender Behauptungen über andere Personen sowie betrügerische Vorgehensweisen, um Kunden zu einem Geschäftsabschluss zu bewegen.[616] Besonders vor dem Hintergrund, ins Visier der Strafermittlungsbehörden zu gelangen, und dem damit einhergehenden Imageverlust und finanziellen Schaden, führt an einer Anzeigenerstattung praktisch kein Weg vorbei. Liegt ein Fall einer schweren, in § 138 StGB aufgezählten Straftat vor, hat der Arbeitgeber sogar die Strafverfolgungsbehörden unverzüglich zu benachrichtigen.

Erfüllen Mitarbeiter des Callcenters Straftatbestände, bleibt es dem Arbeitgeber unbenommen, neben der Strafanzeige auch arbeitsrechtliche Maßnahmen zu ergreifen. Je nach Schwere der Tat stellen die ordentliche oder die außerordentliche Kündigung geeignete Sanktionsmittel dar.

---

[612] HK-BGB/*Schulze*, § 280 Rn. 1 ff.
[613] *Elschner*, Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2004, 93 f.
[614] *Elschner*, Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2004, 94; HK-BGB/*Schulze*, § 823 Rn. 1 ff.
[615] *Lelley*, in: Worzalla (Hrsg.), Internet am Arbeitsplatz, 2006, Rn. 82; *BAG* v. 18.4.2002, NZA 2003, 37.
[616] *Besgen/Prinz*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 1 Rn. 95 ff.

5 Telekommunikations- und strafrechtliche Aspekte

Das Bereitstellen von Serviceleistungen durch Callcenter erfordert eine technische Infrastruktur, über die die Kommunikation zwischen Callcenter-Agenten und Kunden durchgeführt werden kann. Fraglich ist zunächst, ob und inwieweit dies zur Anwendbarkeit der Vorschriften des Telekommunikationsgesetzes (TKG) führt.

Das Telekommunikationsrecht bildet den rechtlichen Rahmen der elektronischen Kommunikation. Mit der Liberalisierung des Telekommunikationsmarktes und dem Wegfallen des staatlichen Monopols entstand die Notwendigkeit eines Regelwerks, das die technische Infrastruktur und die Telekommunikationsdienstleistungen reglementiert.[617] Vor Inkrafttreten des Telekommunikationsgesetzes im Jahr 1996 wurden telekommunikationsbezogene Sachverhalte durch das Fernmelderecht geregelt.[618]

Der primäre Gesetzeszweck des Telekommunikationsgesetzes besteht gemäß § 1 TKG in der Herstellung eines wettbewerbsorientierten Marktes im Telekommunikationsbereich, im Vorantreiben leistungsfähiger technischer Infrastrukturen sowie in der angemessenen und ausreichenden, flächendeckenden Bereitstellung von Dienstleistungen.

Der siebte Teil des Telekommunikationsgesetzes enthält bereichsspezifische Regelungen zum Schutz der Nutzer der TK-Anlage. Sie bestehen einerseits im einfachgesetzlichen Fernmeldegeheimnis und andererseits in telekommunikationsspezifischen Datenschutzvorschriften; teilweise kommt es zu Überschneidungen der beiden Regelungsbereiche.[619]

Das Fernmeldegeheimnis ist partiell durch § 206 StGB strafrechtlich abgesichert. Besondere Relevanz im Zusammenhang mit Callcentern erlangt ferner der Straftatbestand des § 201 StGB: Er stellt das rechtswidrige Abhören und Aufzeichnen von Telefonaten unter Strafe. Im Hinblick auf die Mitarbeiter im Callcenter bedeutet dies, dass eine rechtswidrige Arbeitnehmerüberwachung nicht nur zivilrechtliche, sondern auch strafrechtliche Konsequenzen mit sich bringen kann.[620]

---

[617] *Holznagel/Ricke*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, TKG, § 1 Rn. 1.
[618] *Geppert/Roßnagel*, Telemediarecht, 8. Aufl. 2010, Einführung XVI.
[619] *Eckhardt*, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 4, lit. L, Rn. 1 ff.
[620] *Höld*, Die Überwachung von Arbeitnehmern, 2006, 137.

5.1 Reichweite des Fernmeldegeheimnisses

Auf grundrechtlicher Ebene dient Art. 10 Abs. 1 GG unter anderem dem Schutz des Fernmeldegeheimnisses. Verpflichtet werden dadurch nur Staatsorgane, zum Beispiel Strafverfolgungsbehörden.[621] Das Abwehrrecht gegen die Kenntnisnahme der Inhalte sowie der näheren Umstände der Kommunikation durch staatliche Stellen soll den freien Kommunikationsaustausch im Fernmeldeverkehr gewährleisten. Dabei ist unerheblich, welche Inhalte – zum Beispiel private oder geschäftliche – kommuniziert werden. Dasselbe gilt für die Art der Übermittlung: Analoge und digitale Übertragungsverfahren (beispielsweise Telefonie, E-Mail) werden genauso erfasst wie sämtliche Ausdrucksformen (etwa Sprache, Bilder, Töne).[622] Die näheren Umstände enthalten insbesondere Informationen darüber, welche Personen und Anschlüsse an der Kommunikation beteiligt sind, das Datum, die Dauer und Uhrzeit der Verbindungen einschließlich fehlgeschlagener Verbindungsversuche.[623]

Grundrechtsberechtigt sind sämtliche natürlichen und inländischen juristischen Personen.[624] Das Grundrecht schützt die gewonnenen Informationen nicht lediglich beim ersten Eingriff (Erhebung), sondern auch in allen weiteren Verarbeitungsphasen: So ist die Speicherung, Verwendung und Weitergabe der dem Fernmeldegeheimnis unterliegenden Daten unzulässig, wenn sie unter Eingriff in das Fernmeldegeheimnis erhoben wurden.[625]

Abs. 2 des Art. 10 GG enthält Möglichkeiten zur Beschränkung des Grundrechts. Solche Restriktionen können gemäß Art. 10 Abs. 2 Satz 1 GG in förmlichen Bundes- oder Landesgesetzen vorgesehen sein. Auch eine aufgrund Art. 80 Abs. 1 GG erlassene Rechtsverordnung kann als Eingriffsrechtfertigung dienen.[626] Darüber hinaus existiert durch Satz 2 die Besonderheit, dass der Rechtsweg für Betroffene durch Gesetz versperrt werden kann, soweit der Eingriff dem Schutz der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes dient. Als Ausgleich ist jedoch vorgesehen, dass anstelle des Rechtswegs die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt. So beschneidet beispielsweise das Gesetz zur Beschränkung

[621] *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, TKG, § 88 Rn. 2 f.
[622] *Bock*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 88 Rn. 2.
[623] *Hermes*, in: Dreier (Hrsg.), GG, Band I, 2. Aufl. 2004, Art. 10 Rn. 42.
[624] *Hermes*, in: Dreier (Hrsg.), GG, Band I, 2. Aufl. 2004, Art. 10 Rn. 26.
[625] *Hermes*, in: Dreier (Hrsg.), GG, Band I, 2. Aufl. 2004, Art. 10 Rn. 16.
[626] *Krüger*, in: Sachs (Hrsg.), GG, 2. Aufl. 1999, Art. 10 Rn. 31.

des Brief-, Post- und Fernmeldegeheimnisses[627] das Grundrecht des Fernmeldegeheimnisses.[628]

Das grundrechtlich abgesicherte Fernmeldegeheimnis aus Art. 10 Abs. 1 GG enthält neben dem Abwehrrecht gegenüber dem Staat auch einen Schutzauftrag an diesen. Im Rahmen der Privatisierung des staatlichen Fernmeldewesens wurde daher das Fernmeldegeheimnis einfachgesetzlich in das 1996 in Kraft getretene Telekommunikationsgesetz aufgenommen.[629] Aktuell dient § 88 TKG dem Schutz privater Kommunikationsteilnehmer untereinander. Die Vorschrift ist unter weiteren Voraussetzungen auch von den Betreibern privatrechtlicher und öffentlich-rechtlicher Callcenter zu beachten.[630]

Dem Fernmeldegeheimnis unterliegen gemäß § 88 Abs. 1 TKG die Inhalte des Telekommunikationsvorgangs sowie seine näheren Umstände, primär die daran Beteiligten. Ebenso werden die näheren Umstände erfolgloser Verbindungsversuche erfasst. Unter „Telekommunikation“ ist gemäß § 3 Nr. 22 TKG der „technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“ zu fassen. § 3 Nr. 23 TKG enthält die Legaldefinition des Terminus „Telekommunikationsanlagen“: Sie sind technische Einrichtungen oder Systeme, die sich zum Senden, Übertragen, Vermitteln, Empfangen, Steuern oder Kontrollieren von als Nachrichten identifizierbare elektromagnetische oder optische Signale eignen.

Der persönliche Schutzbereich des § 88 TKG umfasst sowohl natürliche als auch juristische Personen und Personenvereinigungen, die Rechte und Pflichten erwerben und in eigenem Namen geltend machen können.[631]

§ 88 Abs. 2 Satz 1 TKG adressiert den „Diensteanbieter“ als den zur Einhaltung des Fernmeldegeheimnisses Verpflichteten. Der „Diensteanbieter“ stellt einen bedeutenden Betriff im Telekommunikationsrecht dar. Er ist in § 3 Nr. 6 TKG legaldefiniert: Hiernach gilt jeder als Diensteanbieter, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an deren Erbringung mitwirkt. Unter „geschäftsmäßigem Erbringen von Telekommunikationsdiensten“ ist gemäß § 3 Nr. 10 TKG das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne

[627] Artikel 10-Gesetz – G 10.
[628] BeckOK/*Baldus*, GG, Ed. 11, Stand: 1. Juli 2011, Art. 10 Rn. 58.
[629] *Hermes*, in: Dreier (Hrsg.), GG, Band I, 2. Aufl. 2004, § 10 Rn. 23; *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, TKG, § 88 Rn. 2.
[630] Dazu BT-Drs. 13/3609, 53; *Hanebeck/Neunhoeffer*, K&R 2006, 112 (113).
[631] *Bock*, in: Beck’scher TKG-Kommentar, 3. Aufl. 2006, § 88 Rn. 19; *Eckhardt*, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 4, lit. L, Rn. 47.

Gewinnerzielungsabsicht zu fassen. Die Legaldefinition des Begriffs „Telekommunikationsdienste“ findet sich wiederum in § 3 Nr. 24 TKG: Sie umfassen in der Regel entgeltlich erbrachte Dienste, die vollständig oder zumindest zum größeren Teil in der Signalübertragung über Telekommunikationsnetze bestehen sowie die Übertragung in Rundfunknetzen.

Bei der Erbringung des Telekommunikationsdienstes ist nicht auf eine Gewerblichkeit, sondern lediglich auf eine Geschäftsmäßigkeit abzustellen; diese ist regelmäßig gegeben, wenn der Dienst nachhaltig, also dauerhaft angeboten wird.[632] Weiterhin gilt es zu beachten, dass von der Bestimmung des § 3 Nr. 10 TKG nicht nur spezielle Telekommunikationsunternehmen erfasst sind, sondern sämtliche „gewöhnliche“ Unternehmen, die durch die Bereitstellung und den Gebrauch von beispielsweise herkömmlichen Telefonanlagen einen Telekommunikationsdienst erbringen.[633] Die erforderliche Drittbezogenheit ist gegeben, wenn sich das Telekommunikationsangebot an andere – ganz gleich, ob natürliche oder juristische Personen – richtet.[634] Somit sind sowohl betriebsinterne Netzwerke (sogenannte Corporate Networks), deren Nutzung Dritten angeboten wird, als auch Telekommunikationsanbieter für die Allgemeinheit erfasst. Eine Gewinnerzielungsabsicht des Diensteanbieters muss nicht vorliegen.[635] Auch ein sonstiges kommerzielles Interesse ist nicht relevant.[636]

§ 206 StGB stellt unter anderem die Nichtbeachtung des Fernmeldegeheimnisses unter Strafe. Auch dem strafrechtlichen Fernmeldegeheimnis unterliegen gemäß § 206 Abs. 5 Satz 2 und 3 StGB der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Beteiligten, sowie die näheren Umstände erfolgloser Verbindungsversuche.

Die Vorschrift des § 206 StGB enthält insgesamt vier Straftatbestände, von denen nur ein Straftatbestand im Zusammenhang mit Callcenter-Prozessen besondere Relevanz erlangt: Wer nach § 206 Abs. 1 StGB einer anderen Person Tatsachen mitteilt, die dem Fernmeldegeheimnis unterliegen und ihm als Inhaber oder Beschäftigtem eines Unternehmens, das geschäftsmäßig Telekommunikationsdienste erbringt,

[632] *Dann/Gastell*, NJW 2008, 2945 (2946); *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 18 ff.
[633] *Gola*, MMR 1999, 322 (323); *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 20.
[634] *Eckhardt*, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 1, lit. B, Rn. 52.
[635] *Vietmeyer/Byers*, MMR 2010, 807 (808).
[636] *Bock*, in: Beck’scher TKG-Kommentar, 3. Aufl. 2006, § 88 Rn. 23.

zur Kenntnis gelangt sind, dem droht eine Freiheitsstrafe bis zu fünf Jahren oder eine Geldstrafe.

Eine strafrechtliche Sanktion aufgrund einer Verletzung des Fernmeldegeheimnisses droht dem Callcenter-Betreiber als Diensteanbieter jedoch nicht bereits dann, wenn er zum Beispiel lediglich vom Inhalt eines Telekommunikationsvorgangs Kenntnis nimmt, allerdings keine Mitteilung über Tatsachen, die durch das Fernmeldegeheimnis geschützt sind, an andere Personen macht. Die bloße Kenntnisverschaffung steht nicht unter Strafe, sondern wird nur durch § 88 TKG untersagt.[637] Deshalb ist in diesem Fall die durch § 201 StGB geschützte Vertraulichkeit des gesprochenen Wortes mit in die Betrachtung einzubeziehen.[638]

Falls die Verletzung des Fernmeldegeheimnisses aus § 88 TKG gleichzeitig einen Verstoß gegen allgemeines Datenschutzrecht darstellt, kann eine Ordnungswidrigkeit gemäß § 43 oder eine Straftat gemäß § 44 BDSG vorliegen.[639]

§ 88 Abs. 3 Satz 1 TKG erlaubt es dem Diensteanbieter, vom Inhalt und den näheren Umständen der Telekommunikation Kenntnis zu nehmen, soweit dies für die geschäftsmäßige Erbringung des Dienstes inklusive für den Schutz der technischen Systeme erforderlich ist. Die Erforderlichkeit muss einzelfallabhängig, insbesondere in Abhängigkeit des jeweils vorliegenden Telekommunikationsdienstes, festgestellt werden. Anhaltspunkte für die Erforderlichkeit geben die Datenschutzbestimmungen des Telekommunikationsgesetzes in den §§ 91 - 107 TKG.[640] § 88 Abs. 3 Satz 2 TKG enthält ein grundsätzliches Zweckbindungsgebot für die dem Fernmeldegeheimnis unterliegenden Kenntnisse. Diese Zweckbindung darf gemäß § 88 Abs. 3 Satz 3 TKG durchbrochen werden, wenn es das Telekommunikationsgesetz selbst oder eine gesetzliche Vorschrift, die sich ausdrücklich auf Telekommunikationsvorgänge bezieht, vorsieht.

Ferner gibt es nur eine Möglichkeit, Eingriffe in das Fernmeldegeheimnis zu verhindern, wenn eine Zweckentfremdung – beispielsweise aufgrund einer Kontrollmaßnahme – erfolgen soll: Sie besteht generell in einer Einwilligung beider Ge-

[637] *Behling*, BB 2010, 892 (896); *Eckhardt*, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 4, lit. L, Rn. 68.
[638] *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, TKG, § 88 Rn. 6.; zur Vertraulichkeit des gesprochenen Wortes näher Kapitel 5.4 „Verbot des heimlichen Abhörens und Mitschneidens von Telefonaten".
[639] *Eckhardt*, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 4, lit. L, Rn. 73; zu den zivilrechtlichen Folgen des § 44 BDSG s. *Wybitul/Reuling*, CR 2010, 829 ff.
[640] *Bock*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 88 Rn. 26.

sprächsteilnehmer.[641] Zwar ist von einer Öffnungsklausel durch eine Einwilligung, wie sie ausdrücklich in § 4 Abs. 1 BDSG enthalten ist, keine Rede, jedoch wird die Einwilligung auch nicht explizit ausgeschlossen. Da schon die Möglichkeit existiert, auf das in Art. 10 GG verankerte Fernmeldegeheimnis zu verzichten, muss dies erst recht für die einfachgesetzliche Regelung gelten.[642]

In diesem Zusammenhang ist auf die Besonderheit hinzuweisen, dass die telekommunikationsrechtliche Einwilligung gemäß § 94 TKG auch elektronisch abgegeben werden kann.[643] Eine Voraussetzung dazu ist, dass die Einwilligung bewusst und eindeutig erklärt wird. Dies lässt sich beispielsweise durch eine qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG sicherstellen.[644] Eine weitere Anforderung besteht im Protokollierungserfordernis der Einwilligung. Ferner muss ihr Inhalt jederzeit abrufbar und die Einwilligung an sich für die Zukunft widerrufbar sein.

Als erwähnenswert gilt in diesem Zusammenhang das in § 95 Abs. 5 TKG manifestierte Kopplungsverbot: Hiernach darf die Erbringung von Telekommunikationsdiensten nicht davon abhängen, ob der Teilnehmer in die Verwendung seiner Daten für andere Zwecke einwilligt, wenn er einen anderen Zugang zu diesen Diensten nicht oder in nicht zumutbarer Weise erhalten kann. Was genau unter „anderen Zugang“ zu fassen ist, geht aus der Vorschrift nicht hervor. Grundsätzlich kommen diesbezüglich zwei verschiedene Interpretationsrichtungen in Frage: Erstens kann darunter zu verstehen sein, dass es ausreicht, die potenziellen Teilnehmer an Mitbewerber zu verweisen, wenn dies keine unzumutbaren Umstände erfordert. Die zweite denkbare Auslegung ergibt, dass der Anbieter selbst einen vergleichbaren TK-Dienst bereitzustellen hat, der ohne über die zur Erbringung des TK-Dienstes erforderlichen personenbezogenen Daten hinaus auskommt. Vor dem Hintergrund des Verbraucherschutzes ist der letztgenannten Alternative der Vorzug einzuräumen.[645]

[641] *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, TKG, § 88 Rn. 15; *Hanebeck/Neunhoeffer*, K&R 2006, 112 (114); *Löwisch*, DB 2009, 2782 (2783).
[642] *Mattl*, Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2008, 87 f.; *Hoss*, Internet- und E-Mail-Überwachung am Arbeitsplatz, 2009, 73.
[643] *Büttgen*, in: Beck’scher TKG-Kommentar, 3. Aufl. 2006, § 95 Rn. 18.
[644] *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 113.
[645] So auch *Büttgen*, in: Beck’scher TKG-Kommentar, 3. Aufl. 2006, § 95 Rn. 33.

5.1.1 Callcenter-Betreiber als Telekommunikationsanbieter gegenüber Mitarbeitern

Der Betreiber des Callcenters kann seinen Mitarbeitern erlauben, die Kommunikationseinrichtung auch zu privaten Zwecken in Anspruch zu nehmen, um etwa in den Pausenzeiten ausnahmsweise wichtige private Belange regeln zu können. Liegt eine diesbezügliche ausdrückliche Genehmigung vor, sind die Callcenter-Agenten an ihren konkreten Umfang gebunden. Eine pauschale Gestattung der privaten Inanspruchnahme reicht im Grundsatz soweit, dass alles erlaubt ist, was den betrieblichen Ablauf nicht stört, keine unzumutbaren Kosten verursacht und den ordnungsgemäßen Betrieb der TK-Anlage nicht gefährdet.[646]

Unter Umständen kann auch eine betriebliche Übung dazu führen, dass die Nutzung der callcenter-internen Kommunikationsanlage zu privaten Zwecken zulässig ist.[647] Eine dahingehende Betriebsübung stellt sich jedoch nur ein, wenn die praktizierte Privatnutzung für den Callcenter-Betreiber erkennbar war, von ihm geduldet wird und die Arbeitnehmer darauf vertrauen durften, dass auch zukünftig dieser Zustand herrschen wird.[648] Für das Entstehen einer betrieblichen Übung im Zusammenhang mit der privaten Nutzung der elektronischen Kommunikationssysteme ist grundsätzlich anzunehmen, dass sechs bis zwölf Monate hierfür ausreichen.[649] Im Streitfall hat der Arbeitnehmer zu beweisen, dass eine betriebliche Übung in Bezug auf die private Nutzungsmöglichkeit vorliegt.[650]

Damit das Führen von Privatgesprächen überhaupt gezielt funktioniert, muss der Callcenter-Agent die Möglichkeit besitzen, beispielsweise über die manuelle Eingabe von Telefonnummern nach außen zu telefonieren. Wenn das Frontend-System eine Outbound-Funktionalität umfasst, lässt sich dies technisch relativ einfach bewerkstelligen.

---

[646] Küttner/*Kreitner*, Personalbuch, 18. Aufl. 2011, Internet-/Telefonnutzung – Arbeitsrecht, Rn. 6; *Kramer*, NZA 2004, 457 (459).
[647] *Weißnicht*, MMR 2003, 448; *Beckschulze/Henkel*, DB 2001, 1491 (1492); *Fleischmann*, NZA 2008, 1397; a. A. *Koch*, NZA 2008, 911 ff.
[648] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 164; *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 3 Rn. 185; *Beckschulze/Henkel*, DB 2001, 1491 (1492); zu den verschiedenen Theorien der betrieblichen Übung *Waltermann*, RdA 2006, 257 ff. sowie *Thüsing*, NZA 2005, 718 ff.
[649] So *Barton*, NZA 2006, 460 (461); *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 3 Rn. 185; *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 164; in Bezug auf die private Kommunikation mittels Internet und E-Mail a. A. *Waltermann*, NZA 2007, 529 ff., der das Entstehen einer betrieblichen Übung aufgrund der Anwendung von Rechtsprechungsgrundsätzen zur betrieblichen Übung ablehnt.
[650] *Besgen/Prinz*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 1 Rn. 9.

Zunächst gilt es zu klären, wann eine dienstliche und wann eine private Nutzung der TK-Anlage durch die Callcenter-Mitarbeiter vorliegt, da diese Unterscheidung im Hinblick auf die rechtlichen Konsequenzen zwingend erforderlich ist.

Nach h. M. liegt eine dienstliche Nutzung vor, sobald die Inanspruchnahme dazu bestimmt ist, die Arbeit zu fördern. Ein eingetretener Erfolg ist dafür allerdings nicht ausschlaggebend, sodass allein auf die Absicht, die Arbeit voranzutreiben, abgestellt werden muss.[651]

Eine besondere Form stellen telefonisch abgewickelte Privatgespräche aus dienstlichem Anlass dar; sie gelten als Dienstgespräche. Wenn zum Beispiel ein Mitarbeiter seine Ehefrau anruft, um ihr mitzuteilen, dass er länger als geplant arbeiten müsse und deshalb später nach Hause komme, liegt ein solcher Fall vor.[652] Die Zulässigkeit dienstlich motivierter Privatanrufe resultiert aus der Fürsorgepflicht des Arbeitgebers.[653]

Für die Bestimmung der Privatnutzung ist eine Negativabgrenzung vorzunehmen; eine reine Privatnutzung liegt immer dann vor, wenn keine betriebliche Nutzung oder Privatnutzung aus betrieblichem Anlass gegeben ist.[654]

Bestehen Zweifel im Hinblick auf die Abgrenzung, kann auf die diesbezüglichen Grundsätze des Unfallversicherungsrechts und der Arbeitnehmerhaftung zurückgegriffen werden. In beiden Regelungsmaterien wird ein Ereignis vorausgesetzt, das im „ursächlichen und inneren Zusammenhang mit einer betrieblichen Tätigkeit“ steht.[655]

Ist es den Callcenter-Mitarbeitern aufgrund einer Erlaubnis oder Duldung gestattet, die betriebliche Kommunikationsanlage auch zu privaten Telefonaten zu nutzen, nimmt der Arbeitgeber im Hinblick auf private Telefongespräche die Stellung eines Diensteanbieters gemäß § 3 Nr. 6 TKG ein.[656] Dies hat zur Konsequenz, dass die Privattelefonie der Mitarbeiter anhand der Vorschriften des bereichsspezifischen

[651] *Ernst*, NZA 2002, 585 (588); *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 162; *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 3 Rn. 177; *ders.*, K&R 2000, 323 (324); *Weißnicht*, MMR 2003, 448; *Rath/Karner*, K&R 2007, 446 (449).
[652] *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 3 Rn. 178.
[653] *BAG* v. 27.5.1986, NJW 1987, 674; *Ernst*, NZA 2002, 585 (588).
[654] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 163; *Kramer*, NZA 2004, 457 (458).
[655] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 162; *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 3 Rn. 177; *BSG* v. 26.10.2004, BeckRS 2005, 40526; *BSG* v. 25.10.1989, NZA 1990, 409 ff.
[656] *Eckhardt*, DuD 2006, 365 (368); *Behling*, BB 2010, 892; *Hanebeck/Neunhoeffer*, K&R 2006, 112 (113).

Telekommunikationsgesetzes zu beurteilen ist. Sowohl die Mitarbeiter als auch deren private Gesprächspartner sind aufgrund der Erlaubnis zur Privatnutzung als „Dritte“ gemäß § 3 Nr. 10 TKG zu qualifizieren. Zwischen beiden Personengruppen und dem Callcenter-Betrieber entsteht im Fall der genehmigten privaten Inanspruchnahme der betrieblichen TK-Anlage ein TK-Nutzungsverhältnis.

Ungeachtet dessen, ob die Mitarbeiter das callcenter-interne Kommunikationssystem entgeltlich oder unentgeltlich zu privaten Zwecken nutzen dürfen, agieren sie in beiden Fällen nicht mehr als Teil des Unternehmens und ebenso wenig in Erfüllung ihrer arbeitsvertraglich geschuldeten Pflichten. Jedem Arbeitnehmer bleibt es vielmehr selbst überlassen, ob er vom TK-Nutzungsangebot des Arbeitgebers Gebrauch machen oder dies ablehnen will.[657]

Die Schutzfunktion des Fernmeldegeheimnisses gilt gemäß § 88 Abs. 2 Satz 1 TKG gegenüber dem Diensteanbieter, problembezogen gegenüber dem Callcenter-Betreiber und seinen Erfüllungsgehilfen.[658]

Damit es zu keiner „Ausstrahlungswirkung“ der Anwendbarkeit der aufgezeigten Vorschriften des Telekommunikationsgesetzes auf betrieblich oder dienstlich initiierte Telefonate im Callcenter kommt, ist Callcenter-Betreibern zu raten, die Privatnutzung der TK-Anlage technisch oder organisatorisch von ihrer Inanspruchnahme für das Arbeitsverhältnis klar abzugrenzen. Dies gelingt nur dann zweifelsfrei, wenn der Callcenter-Mitarbeiter bei Privattelefonaten beispielsweise eine bestimmte Nummer vorzuwählen hat, sodass die Privatnutzung für den Arbeitgeber erkennbar wird, oder wenn Regelungen bestehen, etwa dass die Privatnutzung ausschließlich in den Pausenzeiten erlaubt ist. Andernfalls liegt eine sogenannte Mischnutzung vor, bei der die betriebliche Kommunikation wie private behandelt werden muss; dies führte zur Unzulässigkeit der Anwendung von Verhaltens- oder Leistungskontrollen in Bezug auf die Mitarbeiter, da die gesamte Telekommunikation Schutz durch das Fernmeldegeheimnis genösse. Die Einräumung einer privaten Nutzungsmöglichkeit der Kommunikationsanlage ist im Callcenter-Bereich noch viel regelungsbedürftiger einzustufen als bei herkömmlichen Arbeitsverhältnissen, da der überwiegende Teil des „Arbeitsprodukts“ gerade im Telefonieren über die TK-Anlage besteht.

[657] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 161; *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004, § 4 Rn. 235 f.; *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 82.
[658] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 171 f.

Im Hinblick auf erlaubte private Telekommunikationsvorgänge durch Callcenter-Mitarbeiter lässt sich zusammenfassend festhalten, dass die gesamte Kommunikation – also sowohl die Gesprächsinhalte als auch die äußeren Umstände der Telefonate – durch das Fernmeldegeheimnis geschützt ist. Kenntnisse, die dem Fernmeldegeheimnis unterliegen, dürfen grundsätzlich nur für die Erbringung des Telekommunikationsdienstes und zum Schutz seiner technischen Systeme genutzt werden. Im Übrigen kommen für Zweckänderungen gesetzliche Erlaubnistatbestände in Betracht. Alternativ kann eine diesbezügliche Einwilligung eingeholt werden, die gleichermaßen vom Callcenter-Mitarbeiter und seinem Gesprächspartner zu erteilen ist. Es gelten die bereits aufgezeigten Grundsätze zur datenschutzrechtlichen Einwilligung aus § 4a BDSG und die zur elektronischen Form der Einwilligung für den Bereich der Telekommunikation aus § 94 TKG.

Bei der erlaubten Privatnutzung tritt das Bundesdatenschutzgesetz als lex generalis hinter die speziellen Normen des Telekommunikationsgesetzes zurück.

Betriebliche oder dienstliche Telekommunikation genießt keinen Schutz durch das Fernmeldegeheimnis. Die Callcenter-Mitarbeiter, die im Rahmen der Erfüllung ihrer Arbeitsaufgaben auf die Inanspruchnahme der TK-Anlage des Callcenters angewiesen sind, nehmen die Stellung eines Besitzdieners gemäß § 855 BGB ein; sie sind insoweit Teil der Organisation und nicht „Dritte“ im Sinne des § 3 Nr. 10 TKG.[659] Darüber hinaus liegt in Bezug auf die Mitarbeiter gerade kein „Angebot“ vor, bei dem sie nach Belieben entscheiden können, ob sie die betrieblichen oder dienstlichen Kommunikationsmittel einsetzen wollen oder nicht – im Rahmen ihres Beschäftigungsverhältnisses obliegt ihnen die Pflicht, die Techniken zu nutzen.[660]

5.1.2 Callcenter-Betreiber als Telekommunikationsanbieter gegenüber externen Gesprächspartnern

Die Privatnutzung der callcenter-internen TK-Anlage könnte grundsätzlich auch dadurch verwirklicht werden, dass vom Callcenter-Mitarbeiter ausgewählte externe Gesprächspartner, zum Beispiel Ehegatte oder Freunde, ihn über eine individuelle Telefonnummer gezielt im Callcenter anwählen können. Möglich wäre dies durch die Bereitstellung eines separaten Nummernkreises, der eigens der Durchführung von Privatgesprächen diente. Diese Form der privaten Nutzung der TK-Anlage des

[659] *Schönfeld/Strese/Flemming*, MMR-Beil. 2001, 8 (11); *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 159.
[660] *Höld*, Die Überwachung von Arbeitnehmern, 2006, 130; *Busse*, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, 2006, § 10 Rn. 23.

Callcenters dürfte allerdings aufgrund ihres erheblichen technischen – und damit auch finanziellen – Aufwands in der Praxis kaum anzutreffen sein. Aus Gründen der Vollständigkeit wird die Alternative zur oben aufgezeigten Privatnutzungsmöglichkeit dennoch kurz aufgegriffen.

Betrachtet man eine solche Konstellation, gelangt man zum Ergebnis, dass gemäß § 3 Nr. 10 TKG das „nachhaltige Angebot von Telekommunikation für Dritte“ hier gegeben ist. Die Gesprächspartner haben Kenntnis der jeweiligen Telefonnummer und bringen mit der Anwahl dieser zum Ausdruck, dass sie das Telekommunikationsangebot annehmen wollen. In der Konsequenz nimmt der Callcenter-Betreiber die Stellung eines Diensteanbieters gegenüber den externen Gesprächspartnern ein. Damit schützt das Fernmeldegeheimnis aus § 88 TKG auch dann die erlaubte private Telekommunikation zwischen den Callcenter-Mitarbeitern und deren Gesprächspartnern, wenn die Telefonate von den externen Gesprächsteilnehmern initiiert worden sind. Es wird insofern auf die bereits in Kapitel 5.1.1 „Callcenter-Betreiber als Telekommunikationsanbieter gegenüber Mitarbeitern“ aufgezeigten Grundsätze verwiesen.

5.2 Datenschutzvorschriften des Telekommunikationsgesetzes

Die telekommunikationsrechtlichen Datenschutzregelungen sind aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG abgeleitet und stellen eine Ausprägung des informationellen Selbstbestimmungsrechts dar; sie gelten für den Bereich der Telekommunikation im Verhältnis zwischen Privaten.[661]

Die Vorschriften über den Datenschutz im Telekommunikationsgesetz sind in den §§ 91 - 107 TKG geregelt und gemäß § 91 Abs. 1 Satz 1 TKG anzuwenden, wenn das Callcenter geschäftsmäßig Telekommunikationsdienste erbringt oder an deren Erbringung mitwirkt. Die personenbezogenen Daten der Teilnehmer und der Nutzer des Telekommunikationsdienstes sind geschützt. Als „Teilnehmer“ gilt nach § 3 Nr. 20 TKG sowohl jede natürliche als auch juristische Person, die mit dem Telekommunikationsdiensteanbieter einen Vertrag über die Erbringung von Telekommunikationsdiensten geschlossen hat. Im Gegensatz dazu ist unter „Nutzer“ gemäß § 3 Nr. 14 TKG jede natürliche Person zu verstehen, die aus privaten oder geschäftlichen Gründen einen Telekommunikationsdienst nutzt, ohne zwangsweise Teilneh-

[661] *Eckhardt*, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 4, lit. L, Rn. 3.

mer sein zu müssen. Eine vertragliche Beziehung zum Diensteanbieter muss also nicht bestehen.

An einem konkreten Beispiel lässt sich die Bedeutung der beiden Begriffe veranschaulichen: Der Callcenter-Betreiber ist gegenüber seinem Telekommunikationsdiensteanbieter Teilnehmer, da er mit diesem einen Vertrag über die Bereitstellung der Telekommunikationsinfrastruktur geschlossen hat. Die Callcenter-Mitarbeiter sind – bei der betrieblichen Nutzung der callcenter-internen TK-Anlage – im Verhältnis zum Telekommunikationsdiensteanbieter des Callcenter-Betriebs als Nutzer zu qualifizieren: Zwar nehmen sie den Telekommunikationsdienst in Anspruch, stehen jedoch in keiner vertraglichen Beziehung mit dem Telekommunikationsdiensteanbieter.

Für die Anwendbarkeit der Datenschutzregelungen des Telekommunikationsgesetzes ist gemäß § 3 Nr. 10 TKG ausschlaggebend, ob ein nachhaltiges Telekommunikationsangebot für Dritte mit oder ohne Gewinnerzielungsabsicht vorliegt. Wie aufgezeigt wurde, ist eine solche Situation bei einer erlaubten Privatnutzung der TK-Anlage durch Callcenter-Mitarbeiter gegeben.

Nachfolgend werden die im Zusammenhang mit Callcentern bedeutendsten telekommunikationsrechtlichen Datenschutzvorschriften kurz dargestellt.

5.2.1 Informationspflichten

§ 93 TKG regelt die telekommunikationsrechtlichen Informationspflichten: Nach § 93 Abs. 1 Satz 1 TKG hat der Diensteanbieter die Teilnehmer in allgemeiner Form über Art, Umfang, Ort sowie Zweck der Erhebung und Verwendung ihrer personenbezogenen Daten zu informieren. Dies muss bei Vertragsschluss geschehen. Zwar liegt bei einer durch den Callcenter-Betreiber gestatteten privaten Nutzungsmöglichkeit der TK-Anlage in der Regel kein eigenes Vertragsverhältnis über die Inanspruchnahme der betrieblichen Telefonanlage vor. Trotzdem hat eine diesbezügliche Information der Mitarbeiter zu erfolgen; sie kann beispielsweise mittels Betriebs- oder Dienstvereinbarung durchgeführt werden.

Die Benachrichtigungspflicht aus § 33 BDSG, wonach der Datenverarbeiter die Betroffenen über die Speicherung ihrer Daten, über deren Art und über die Zwecke ihrer Erhebung, Verarbeitung oder Nutzung zu benachrichtigen hat, findet in § 93

Abs. 1 Satz 3 TKG ihren Niederschlag.[662] Die Vorschrift sieht vor, dass auch die Nutzer, die in keinem Vertragsverhältnis zum Callcenter-Betreiber als Diensteanbieter stehen, allgemein zu informieren sind. Damit soll der Tatsache Rechnung getragen werden, dass nicht nur mit den Daten der Teilnehmer, also denen der Callcenter-Mitarbeiter, sondern auch mit denen der Nutzer (zum Beispiel Rufnummer) in Gestalt der privaten Gesprächspartner umgegangen werden muss.[663]

Nutzer müssen nicht individuell über den Umgang mit ihren Daten informiert werden; dies wäre allein aufgrund der technischen Struktur der Telekommunikation gar nicht möglich. Die allgemeine Information durch den Telekommunikationsdiensteanbieter kann beispielsweise mittels seines Internetauftritts stattfinden.[664] Diese Benachrichtigungspflicht mag für große Telekommunikationsdiensteanbieter weniger ein Problem darstellen, als für Arbeitgeber, die deshalb zu Telekommunikationsanbietern werden, weil sie die Privatnutzung ihrer organisationsinternen TK-Anlage genehmigen.

Praktisch entspricht die Unterrichtungspflicht im Hinblick auf die Teilnehmer einer Bringschuld des Diensteanbieters, während diese Verpflichtung hinsichtlich der Nutzer eher mit einer Holschuld derselben vergleichbar ist.[665] Der Auskunftsanspruch nach § 34 BDSG bleibt ferner unberührt.

Darüber hinaus existiert gemäß § 93 Abs. 3 TKG i. V. m. § 42a BDSG eine spezielle Informationspflicht bei Datenverlust.[666] Bei der Feststellung, dass gespeicherte Bestands- oder Verkehrsdaten unzulässig übermittelt wurden oder Dritten andersartig unzulässig zur Kenntnis gelangt sind, kann diese Informationspflicht ausgelöst werden. Weitere Voraussetzung ist die Befürchtung schwerwiegender negativer Konsequenzen für die Rechte oder schützenswerten Interessen des betroffenen Nutzers.

5.2.2 Umgang mit verschiedenen Datenarten

Das Telekommunikationsgesetz differenziert drei verschiedene Datenarten. Hierzu zählen:

[662] *Büttgen*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 93 Rn. 7.
[663] *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, TKG, § 93 Rn. 9.
[664] *Büttgen*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 93 Rn. 54.
[665] *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, TKG, § 93 Rn. 9.
[666] S. dazu Kapitel 3.1.2.2 „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten".

- „Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“ als Bestandsdaten gemäß § 3 Nr. 3 TKG;
- „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet und genutzt werden“ als Verkehrsdaten gemäß § 3 Nr. 30 TKG;
- „Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben“ als Standortdaten gemäß § 3 Nr. 19 TKG.

Die Zulässigkeit des Umgangs mit den aufgeführten Arten von Daten richtet sich nach den §§ 95 ff. TKG.

Mittels Telekommunikation übertragene Inhalte, also die Gespräche, werden von der Regelungsebene des Telekommunikationsgesetzes nicht erfasst.

5.2.2.1 Bestandsdaten

Bestandsdaten gemäß § 3 Nr. 3 TKG dürfen nach § 95 Abs. 1 Satz 1 TKG durch den Diensteanbieter erhoben und verwendet werden, wenn sie für die Begründung, inhaltliche Gestaltung, Modifikation oder Beendigung eines Vertrags über Telekommunikationsdienste erforderlich sind.

Bestandsdaten sind dauerhaft gespeichert und ermöglichen die Telekommunikation im Rahmen der vertraglichen Beziehung. Namentlich handelt es sich um persönliche Angaben wie Anschrift, Name und Kontonummer sowie Telefon- oder Anschlussnummer.

Zwischen dem Arbeitgeber und seinen Beschäftigten besteht jedoch regelmäßig kein spezielles Vertragsverhältnis in Bezug auf die Inanspruchnahme der TK-Anlage; deshalb sind die Daten aus dem Arbeitsvertrag den Bestandsdaten der Telekommunikation gleichzusetzen.[667]

[667] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 251 f.

5.2.2.2 Verkehrsdaten

Zum Herstellen und Aufrechterhalten einer Telekommunikationsverbindung werden Verkehrsdaten benötigt.[668] Verkehrsdaten, die bei der erlaubten privaten Inanspruchnahme der TK-Anlage anfallen, darf der Callcenter-Betreiber als Diensteanbieter für verschiedene Zwecke verwenden.

In § 96 Abs. 1 Nr. 1 - 5 TKG sind unterschiedliche Arten von Verkehrsdaten aufgezählt. Zu ihnen gehören zum Beispiel die Anschlusskennungen, Beginn und Ende der Verbindung sowie übermitteltes Datenvolumen.

§ 96 Abs. 2 Satz 2 TKG sieht vor, dass gespeicherte Verkehrsdaten nach Beendigung der Telekommunikation grundsätzlich sofort zu löschen sind. Die Löschung muss dann nicht unverzüglich erfolgen, wenn die Daten für die in Satz 1 aufgezählten Zwecke benötigt werden. Solche Zwecke sind etwa die

- Entgeltabrechnung gemäß § 97 TKG,
- Erstellung eines Einzelverbindungsnachweises gemäß § 99 TKG oder
- Aufdeckung von Störungen oder Fehlern in der TK-Anlage gemäß § 100 TKG.

Existiert zwischen dem Callcenter-Betreiber und seinen Mitarbeitern beispielsweise die Vereinbarung, dass die TK-Anlage zu privaten Zwecken bei eigener Kostentragung genutzt werden darf, so ist der Datenumgang unter den Voraussetzungen des § 97 TKG zulässig.

5.2.2.3 Standortdaten

Standortdaten spielen in Bezug auf die Callcenter-Mitarbeiter keine Rolle, da die Mitarbeiter private Nutzungsvorgänge der betrieblichen TK-Anlage ausschließlich an ihrem Arbeitsplatz durchführen können. Überdies stellen die Mitarbeiter eine geschlossene Benutzergruppe dar und sind somit keine Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten für die Öffentlichkeit gemäß § 98 Abs. 1 Satz 1 TKG.

[668] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 253.

5.2.3 Datenumgang bei Störung und Missbrauch der TK-Anlage

Dem Diensteanbieter ist es – soweit erforderlich – gemäß § 100 Abs. 1 TKG ausnahmsweise gestattet, zur Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern an TK-Anlagen die Bestands- und Verkehrsdaten zu erheben und zu verwenden.

Zudem ist unter weiteren Voraussetzungen der Umgang mit Bestands- und Verkehrsdaten zulässig, wenn dies zur Verhinderung von Leistungserschleichungen oder anderen rechtswidrigen Inanspruchnahmen der TK-Netze und -Dienste erforderlich ist. Hierzu kann der Diensteanbieter den höchstens sechs Monate alten Gesamtbestand der angefallenen Verkehrsdaten heranziehen.

5.2.4 Technische Schutzmaßnahmen

Die telekommunikationsrechtliche Erweiterung und Konkretisierung des allgemeinen § 9 BDSG verkörpert § 109 TKG:[669] Liegt gegenüber dem Callcenter-Betreiber ein TK-Nutzungsverhältnis vor, so hat dieser nach § 109 Abs. 1 Nr. 1 und Nr. 2 TKG die Pflicht, technische und sonstige Maßnahmen zu treffen, die das Fernmeldegeheimnis, die personenbezogenen Daten sowie die Telekommunikations- und Datenverarbeitungssysteme schützen.

§ 109 Abs. 2 TKG bestimmt weitergehend für Unternehmen, die TK-Dienste für die Öffentlichkeit anbieten, dass diese adäquate Schutzvorkehrungen gegen Katastrophen, äußere Angriffe und erhebliche Beeinträchtigungen von Kommunikationsnetzen zu treffen haben. Nach § 109 Abs. 2 TKG hat derjenige, der TK-Dienste für die Öffentlichkeit bereitstellt, einen Sicherheitsbeauftragten zu bestellen und ein Sicherheitskonzept zu entwickeln. Abs. 2 und Abs. 3 gelten ausdrücklich nur für die öffentliche Bereitstellung von TK-Diensten, jedoch nicht für den Betrieb von sogenannten Corporate Networks. Bei einer zulässigen Privatnutzung der betrieblichen Kommunikationsanlage durch Callcenter-Mitarbeiter müssen demzufolge keine entsprechenden Vorkehrungen getroffen werden.[670]

[669] *Eckhardt*, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 1, lit. B, Rn. 93; *Bock*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 109 Rn. 10 f.
[670] BT-Drs. 15/2316, 92; *Bock*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 109 Rn. 31.

5.3 Verbot der Rufnummerunterdrückung

Das Gesetz zur Bekämpfung unerlaubter Telefonwerbung befasst sich unter anderem mit unerlaubten Werbeanrufen[671] (sogenannte Cold Calls). Im Telekommunikationsgesetz wurde die Pflicht zur Rufnummerübertragung des Werbenden im Rahmen von Werbeanrufen verankert; Verstöße sollen mit einer Geldbuße geahndet werden können.[672]

Gemäß § 102 Abs. 1 TKG müssen der Anrufende sowie der Angerufene die Möglichkeit besitzen, die Rufnummeranzeige unentgeltlich und mühelos zu deaktivieren, falls der Telekommunikationsanbieter die Übermittlung der Rufnummer des Anrufenden anbietet. Ferner ist zu gewährleisten, dass der Angerufene den Anrufer kostenfrei und auf einfache Art abweisen kann, wenn dieser seine Telefonnummer unterdrückt. Das Recht auf Privatsphäre wird durch die Möglichkeit des Anrufs mit unterdrückter Rufnummer gewahrt.[673]

§ 102 Abs. 2 TKG beinhaltet eine Ausnahme von der grundsätzlich freien Entscheidung, ob die Telefonnummer des Anrufers übertragen werden soll oder nicht: Diese betrifft zu Werbezwecken Anrufende und enthält das für sie geltende Verbot, die Nummer zu verbergen. Insofern wird durch diese Vorschrift der ausdrückliche Wille des Gesetzgebers deutlich, die Rufnummerunterdrückung im Bereich der Telefonwerbung gesetzlich zu verbieten.[674] Werden Werbeanrufe ohne die vorherige Einwilligung des Angerufenen – und somit unzulässig – durchgeführt, soll die Pflicht zur Rufnummerübertragung die Identifizierung des Anrufers ermöglichen.[675]

Ursprünglich war vom Rechtsausschuss vorgesehen[676], dass beauftragte Callcenter zwischen der Anzeige der eigenen Rufnummer oder derjenigen des Auftraggebers wählen können.[677] Diese Abweichung von § 66j Abs. 2 Satz 1 TKG wurde durch den anfänglich vorgesehenen Satz 2 des § 102 Abs. 2 TKG erlaubt. Die Option konnte letztendlich nicht umgesetzt werden. Der Hauptgrund liegt in der Schwierigkeit, den tatsächlichen Anrufer zu ermitteln, wenn die Übertragung der Rufnummer eines (angeblichen) Auftraggebers erfolgt. Diese Ermittlungstätigkeit wäre im Übrigen äußerst unpraktikabel.[678]

---

[671] Dazu Kapitel 3.2.1 „Verbot von Werbeanrufen ohne Einwilligung“.
[672] *Hecker*, K&R 2009, 601; BT-Drs. 16/10734, 1.
[673] BT-Drs. 16/10734, 14.
[674] *Hecker*, K&R 2009, 601 (605).
[675] BT-Drs. 16/10734, 15; *von Wallenberg*, BB 2009, 1768 (1769).
[676] S. BT-Drs. 16/12406, 6.
[677] *Ditscheid/Ufer*, MMR 2009, 367 (370); *Hecker*, K&R 2009, 601 (605).
[678] *Hecker*, K&R 2009, 601 (605).

§ 149 Abs. 1 Nr. 17c TKG bestimmt, dass unerlaubte Telefonanrufe zu werbenden Zwecken mit verborgener Rufnummer eine Ordnungswidrigkeit darstellen. Bei Verstößen gegen die Pflicht zur Rufnummeranzeige können gemäß § 149 Abs. 2 Satz 1 TKG Bußgelder bis zur Höhe von 10.000 Euro verhängt werden. Die Notwendigkeit zur Anzeige der Rufnummer stellt eine gesetzliche Nebenpflicht dar, ähnlich wie die Auskunfts-, Mitteilungs- oder Meldepflicht. Die Verfolgung von Ordnungswidrigkeiten in diesem Zusammenhang obliegt der Bundesnetzagentur. Damit diese ihre Ermittlungen aufnehmen kann, ist sie auf Angaben des Verbrauchers zum Anruf angewiesen (etwa Datum, Uhrzeit und werbendes Unternehmen).[679]

5.4 Verbot des heimlichen Abhörens und Mitschneidens von Telefonaten

§ 201 StGB stellt unter anderem das unbefugte Abhören mit einem Abhörgerät und das unbefugte Aufzeichnen des nichtöffentlich gesprochenen Wortes unter Strafe. Im gesprochenen Wort offenbart sich ein bedeutender Teil der menschlichen Persönlichkeit. Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG umfasst die Befugnis des Sprechers selbst zu bestimmen, ob sein gesprochenes Wort lediglich dem Gesprächspartner, Dritten oder sogar der Öffentlichkeit zur Kenntnisnahme bestimmt sein soll.[680] Eine „nichtöffentliche" Äußerung liegt vor, wenn sich die Äußerung nicht an die Allgemeinheit richtet und von Außenstehenden nicht oder nicht ohne Weiteres vernommen werden kann;[681] dies trifft insbesondere auf Telefongespräche zu. Die Vorschrift dient dem Schutz der Vertraulichkeit des gesprochenen Wortes. Geschützt ist der Mensch in seiner Privat- und Vertraulichkeitssphäre, in welcher die Unbefangenheit der menschlichen Kommunikation gewährleistet sein soll.[682]

Nach § 201 Abs. 2 Nr. 1 StGB ist das unbefugte Abhören des nicht zu seiner Kenntnis bestimmten nichtöffentlich gesprochenen Wortes anderer Personen mithilfe eines Abhörgeräts als Straftat zu qualifizieren. Das Belauschen eines Gesprächs, zum Beispiel durch Horchen an der Tür, ohne Zuhilfenahme technischer Hilfsmittel, ist nicht strafbar.[683] Als „Abhörgerät" gelten technische Einrichtungen, etwa Mikrofone, Minisender, Vorrichtungen zum Anzapfen von Telefonleitungen. Irrele-

[679] BT-Drs. 16/10734, 15 f.; Anmerkung: Beim Verweis auf „17a" innerhalb lit. b handelt es sich offenbar um ein redaktionelles Versehen in der Gesetzesbegründung. Korrekt wäre stattdessen der Verweis auf lit. c.
[680] *Kläver*, DuD 2003, 228 (229 f.).
[681] *Wessels/Hettinger*, Strafrecht. Besonderer Teil 1, 32. Aufl. 2008, § 12 Rn. 527; *Baumeister*, ZUM 2000, 114.
[682] *Ernst*, NJW 2004, 1277 (1278).
[683] MüKo-StGB/*Graf*, Band 3, § 201 Rn. 27.

vant ist, ob ihr Besitz zulässig ist oder nicht. Keine Abhörgeräte im Sinne der Vorschrift sollen laut h. M. in Literatur und Rechtsprechung demgegenüber – vollkommen pauschal – herkömmliche Mithöreinrichtungen, wie Zweithörer, Zweitapparat oder eingebauter Lautsprecher, darstellen.[684] Die wesentliche Begründung solle darin liegen, dass derartige Mithöreinrichtungen im Geschäftsleben üblich seien und auch im Privatbereich mit dem Mithören gerechnet werden müsse.[685] Diese Argumentation überzeugt aus folgenden Gründen im Grundsatz nicht: Schließt eine Person beispielsweise ein herkömmliches Analogtelefon heimlich mittels Telefonadapter an die Verteilerdose eines Telefonanschlusses an und hört ein Telefonat ohne Kenntnis der beiden Gesprächsteilnehmer mit, so solle dies nicht strafbar sein, da kein Abhörgerät zum Einsatz gelange. Die Möglichkeit des „Dual Use" von zugelassenen Geräten, das heißt deren Einsatz zu einem anderen Verwendungszweck als ursprünglich vorgesehen, bleibt dabei vollkommen unberücksichtigt. Ausschlaggebend müsste jedoch in erster Linie der Zweck sein, zu dem eine Einrichtung, die das Mithören ermöglicht, konkret benutzt wird. So ist es einleuchtend, dass ein Telefon mit eingebautem Lautsprecher bei einer normalen Verwendung keine Abhöreinrichtung darstellt.[686] Wird ein solches aber in irgendeiner Form zum Belauschen genutzt, müsste es ohne jeden Zweifel als Abhörgerät eingestuft werden.

Als Rechtfertigung zum Mithören kommen insbesondere eine gesetzliche Erlaubnis, allgemeine Rechtfertigungsgründe sowie die Einwilligung der betroffenen Gesprächspartner in Betracht.[687] Teilweise wird vertreten, dass bereits eine mutmaßliche Einwilligung ausreichen könne;[688] diese kann im Rahmen von geschäftlichen Gepflogenheiten, etwa bei der telefonischen Abwicklung von Bankgeschäften, Relevanz erlangen.[689] Allerdings darf die mutmaßliche Einwilligung des Kunden in Bezug auf das Mithören eines Dritten im Bereich der Callcenter-Dienstleistungen nicht grundsätzlich unterstellt werden. Exakt diese Fragestellung greift der § 32i Abs. 2 Satz 2 Nr. 2 BDSG-E auf: Eine Kenntnisnahme der Gesprächsinhalte zum Zwecke der Leistungs- oder Verhaltenskontrolle der Callcenter-Mitarbeiter darf

[684] *Wessels/Hettinger*, Strafrecht. Besonderer Teil 1, 32. Aufl. 2008, § 12 Rn. 541 f.; *Rengier*, Strafrecht. Besonderer Teil II, 10. Aufl. 2009, § 31 Rn. 5; *Joecks*, Strafgesetzbuch. Studienkommentar, 8. Aufl. 2009, § 201 Rn. 10 m. w. N.; *BGH* v. 17.2.1982, NJW 1982, 1397 ff.; *BGH* v. 8.10.1993, NJW 1994, 596 ff.; a. A. MüKo-StGB/*Graf*, Band 3, § 201 Rn. 31 f.

[685] *Joecks*, Strafgesetzbuch. Studienkommentar, 8. Aufl. 2009, § 201 Rn. 10; *BGH* v. 17.2.1982, NJW 1982, 1397 ff.; zum heimlichen Mithörenlassen von Telefongesprächen zwischen Arbeitnehmer und Arbeitgeber *BAG* v. 29.10.1997, NZA 1998, 307; zum Abhören eines Dienstgesprächs durch den Arbeitgeber *BVerfG* v. 19.12.1991, NJW 1992, 815.

[686] Insoweit vollkommen zutreffend MüKo-StGB/*Graf*, Band 3, § 201 Rn. 31 f., der ebenso auf den konkreten Verwendungszweck der Vorrichtung abstellt.

[687] NK-StGB-*Kargl*, § 201 Rn. 22 ff.

[688] So etwa *Rengier*, Strafrecht. Besonderer Teil II, 10. Aufl. 2009, § 31 Rn. 7.

[689] *Wessels/Hettinger*, Strafrecht. Besonderer Teil 1, 32. Aufl. 2008, § 12 Rn. 533.

unter anderem nur unter der Voraussetzung stattfinden, dass die Kunden über eventuell durchgeführte Mithörmaßnahmen informiert wurden und darin eingewilligt haben. Reichte bereits eine mutmaßliche Einwilligung aus, wäre keine ausdrückliche Forderung durch die Vorschrift notwendig gewesen.

Gemäß § 201 Abs. 1 Nr. 1 StGB macht sich strafbar, wer unbefugt das nichtöffentlich gesprochene Wort einer anderen Person auf einen Tonträger aufnimmt. Die Aufzeichnung des gesprochenen Wortes auf einen Tonträger ist erfüllt, wenn dadurch die akustische Wiedergabe ermöglicht wird. Als Tonträger kann beispielsweise eine Kassette, eine DVD oder ein Mikrochip dienen. Der Zweck der Vorschrift des § 201 Abs. 1 Nr. 1 StGB besteht darin, eine Verdinglichung des gesprochenen Wortes durch unbefugte Mitschnitte zu unterbinden.[690]

Allgemein entfällt der Straftatbestand, wenn der Sprechende über den Mitschnitt informiert wurde und ferner seine wirksame Einwilligung erteilt hat.[691] Dies gilt auch für rein geschäftliche Telefonate, weil auch bei ihnen aus der Spontaneität heraus formulierte Gedanken mit der Möglichkeit der jederzeitigen Abrufbarkeit und Wiederholbarkeit objektiviert werden und damit einen erheblichen Eingriff in das Recht zur Selbstbestimmung über das gesprochene Wort darstellen.[692] Darüber hinaus können die bei der Fragestellung des Mithörens bereits genannten Rechtsfertigungsgründe unter Umständen zum Tragen kommen.

Übertragen auf die Situation im Callcenter bedeutet dies, dass grundsätzlich eine Einwilligung der Kunden in die Vorgänge des Mithörens sowie des Aufzeichnens der Telefonate durch den Callcenter-Betreiber oder den in seinem Auftrag Handelnden, beispielsweise den Coach, vorliegen muss, um der Strafbarkeit zu entgehen. Mit dem Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes[693] versucht der Gesetzgeber unter anderem, dem Kontrollinteresse des Callcenter-Betreibers in Bezug auf das Verhalten oder die Leistung seiner Mitarbeiter gerecht zu werden: Im Hinblick auf die Callcenter-Agenten ist es gemäß § 32i Abs. 2 Satz 2 BDSG-E zulässig, Gesprächsinhalte zu genannten Zwecken ohne Kenntnis der Mitarbeiter im Einzelfall stichprobenhaft oder anlassbezogen zu erheben, zu verarbei-

[690] HK-GS/*Tag*, StGB, § 201 Rn. 7; str. in Bezug auf die Frage, ob die Aufnahme heimlich erfolgen müsse (befürwortend etwa HK-GS/*Tag*, StGB, § 201 Rn. 7 m. w. N.; ablehnend NK-StGB-*Kargl*, § 201 Rn. 10; *Lackner/Kühl*, StGB, § 201 Rn. 3a m. w. N.; *OLG Thüringen* v. 24.4.1995, NStZ 1995, 502).
[691] HK-GS/*Tag*, StGB, § 201 Rn. 7; differenzierend im Hinblick auf mutmaßliche Einwilligungen *Kramer*, NJW 1990, 1760 (1762); *Lüderssen*, wistra 2006, 441 (446), der ausschließlich die ausdrückliche Einwilligung als ausreichend erachtet.
[692] *BGH* v. 13.10.1987, NJW 1988, 1016 (1017).
[693] S. BT-Drs. 17/4230.

ten oder zu nutzen. Einschränkend gilt es zu berücksichtigen, dass die Mitarbeiter im Vorfeld über die in einem eingegrenzten Zeitraum eventuell stattfindende Kontrolle informiert wurden. Ferner sind die Kenntnis der Kontrollmaßnahmen sowie das diesbezügliche Einverständnis durch Kunden erforderlich. Darüber hinaus müssen die Mitarbeiter nachträglich unverzüglich darüber unterrichtet werden, dass eine Erhebung, Verarbeitung oder Nutzung dieser Inhaltsdaten durch den Arbeitgeber erfolgt ist.[694]

Im Übrigen ergibt sich gemäß § 201 Abs. 1 Nr. 2 StGB eine Strafbarkeit, wenn unbefugt hergestellte Gesprächsmitschnitte gebraucht oder Dritten zugänglich gemacht werden. Exemplarisch lassen sich das Kopieren und Abspielen einer solchen Aufnahme sowie ihr Aushändigen an andere Personen ins Feld führen.[695] Wenn der Betreiber des Callcenters derart aufgezeichnete Gespräche beispielsweise zum Zwecke der Evaluation der Telefongespräche zwischen seinen Mitarbeitern und Kunden anhört, ist die Strafbarkeit gegeben.

Ferner macht sich gemäß § 201 Abs. 2 Satz 1 Nr. 2 StGB strafbar, wer das ohne Befugnis aufgezeichnete oder abgehörte nichtöffentlich gesprochene Wort eines anderen öffentlich macht. Satz 2 enthält eine hierauf bezogene Bagatellklausel, die bewirkt, dass lediglich belanglose Äußerungen (etwa über die Wettervorhersage) nicht von der Tatbestandsmäßigkeit erfasst werden.[696]

Wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter eine oben genannte Straftat begeht, wird gemäß § 201 Abs. 3 StGB mit einer Freiheitsstrafe von bis zu fünf Jahren oder einer Geldstrafe bestraft. Diese Strafverschärfung bezieht sich auch auf bestimmte Dienstleistungen, die Callcenter anbieten können; so fällt die Gesundheitsberatung darunter.

Aufgrund der Tatsache, dass die heutzutage im Callcenter eingesetzte TK-Infrastruktur nicht mehr auf Analogtechnik beruht, sondern digitale Übertragungsverfahren (VoIP) zum Einsatz gelangen, ist die Einschlägigkeit des § 202b StGB zu prüfen. Die Vorschrift wurde durch Art. 1 Nr. 3 des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 7.8.2007 in das Strafgesetzbuch

[694] BT-Drs. 17/4230, 9.
[695] *Lackner/Kühl*, StGB, § 201 Rn. 4b; zur Frage, ob die Aufnahme überhaupt unbefugt erfolgt sein muss („monistische vs. dualistische Auffassung") *Wölfl*, JURA 2003, 742 ff.
[696] *Lackner/Kühl*, StGB, § 201 Rn. 7 f.; BT-Drs. 11/7414, 4.

eingefügt.[697] Zweck des Gesetzes war, dem Missbrauch der sich rasant fortentwickelnden Informationstechnologie zu begegnen.[698]

§ 202b StGB stellt das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübertragung sowie aus einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Zuhilfenahme technischer Mittel unter Strafe. Die Vorschrift erfasst sämtliche nichtöffentlichen elektronischen Datenübertragungen, zum Beispiel E-Mail, Fax und Telefon.[699] Sie soll einen allgemeinen Schutz übermittelter Daten gewährleisten.[700] Unter „Daten" in diesem Sinne sind gemäß § 202b i. V. m. § 202a Abs. 2 StGB solche Daten zu fassen, die magnetisch, elektronisch oder anderweitig nicht unmittelbar wahrnehmbar übermittelt werden oder gespeichert sind.

Allerdings kommt § 202b StGB eine Lückenfüllungsfunktion zu, wenn beispielsweise die Voraussetzungen des § 201 StGB nicht erfüllt sind;[701] die Vorschrift enthält eine entsprechende Subsidiaritätsklausel. Die Gesetzesbegründung bezeichnet die Regelung ausdrücklich als „elektronisches Pendant zu dem Abhören und Aufzeichnen von Telefongesprächen".[702]

Im Ergebnis lässt sich festhalten, dass das unbefugte Mithören und Mitschneiden von Telefonaten bereits von § 201 StGB erfasst wird – unabhängig von der eingesetzten Übertragungstechnik. Insoweit hat der § 202b StGB diesbezüglich keine Relevanz. Dasselbe gilt im Übrigen für § 202a StGB, der das unbefugte Verschaffen von Daten unter Umgehung einer besonderen Zugangssicherung unter Strafe stellt, wenn die Daten nicht für denjenigen bestimmt sind, der sie sich verschafft. Bereits mangels existierender Zugangssicherung – konkret wäre eine verschlüsselte Telekommunikationsverbindung zwischen dem Callcenter-Mitarbeiter und seinem Gesprächspartner notwendig – scheidet die Norm aus.

[697] NK-StGB-*Kargl*, § 202b Rn. 1; s. dazu *Schumann*, NStZ 2007, 675 ff.
[698] BT-Drs. 16/3656, 1.
[699] NK-StGB-*Kargl*, § 202b Rn. 4.
[700] *Gröseling/Höfinger*, MMR 2007, 549 (552).
[701] HK-GS/*Tag*, StGB, § 202b Rn. 7; *Vassilaki*, CR 2008, 131 (132); *Schultz*, MIR 2006, Dok. 180, Rn. 19.
[702] BT-Drs. 16/3656, 11.

6 Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit

6.1 Verpflichtung der Mitarbeiter auf das Datengeheimnis

Gemäß § 5 BDSG ist sämtlichen Mitarbeitern, die personenbezogene Daten verarbeiten, der unbefugte Umgang mit diesen Daten verboten. Ein unbefugtes Handeln liegt bereits dann vor, wenn Mitarbeiter unternehmensinterne Zugriffsbefugnisse überschreiten, selbst wenn der konkrete Datenverarbeitungsvorgang an sich von der Stelle zulässig vollzogen werden dürfte.[703] Diejenigen Beschäftigten bei nichtöffentlichen Stellen und öffentlichen Stellen des Bundes, die in Datenverarbeitungsprozesse involviert sind – also in der Regel auch alle Callcenter-Agenten –, müssen bei Aufnahme ihrer Beschäftigung zur Einhaltung des Datengeheimnisses verpflichtet werden.[704] Diese Verpflichtung ist auch durch sämtliche Landesdatenschutzgesetze vorgesehen.

Das Geheimnis gilt nach Beendigung des Beschäftigungsverhältnisses weiter. Selbst Auftragsdatenverarbeiter sind gemäß § 11 Abs. 4 Satz 1 BDSG dieser Verpflichtung zu unterwerfen.[705] Dem Datengeheimnis unterliegen grundsätzlich sämtliche Beschäftigte, die mit der personenbezogenen Datenverarbeitung in Verbindung stehen. Es kommt nicht darauf an, wie das Beschäftigungsverhältnis konkret ausgestaltet ist, das heißt etwa auch arbeitnehmerähnliche Personen, Werkstudenten, Aushilfen und Teilzeitbeschäftigte müssen das Datengeheimnis beachten, sofern sie in entsprechende Prozesse mit eingebunden sind. Dasselbe gilt für die Mitglieder des Betriebs- und Personalrats, die zwar als unabhängige Gremien tätig, jedoch trotzdem ein Teil der verantwortlichen Stelle sind.[706]

Die betroffenen Mitarbeiter sind adäquat zu unterweisen. Die Belehrung setzt sich aus mehreren Komponenten zusammen: Erstens muss eine hinreichende Information dahingehend erfolgen, was die Pflicht zur Wahrung des Datengeheimnisses konkret und tätigkeitsspezifisch beinhaltet; hierbei soll eine möglichst detaillierte Unterrichtung mit Hinweisen zur praktischen Umsetzung stattfinden.[707] Es ist auf drohende Schadenersatzforderungen sowie auf mögliche Sanktionen arbeits-, dienst-

[703] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 5 Rn. 6; *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 5 Rn. 4.
[704] Küttner/*Griese*, Personalbuch, 18. Aufl. 2011, Datenschutz – Arbeitsrecht – Organisatorische Vorkehrungen des Arbeitgebers, Rn. 20.
[705] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 5 Rn. 1; Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 25.
[706] Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 14 ff.
[707] Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 28.

und strafrechtlicher Natur hinzuweisen, die aus einem Verstoß gegen das Datengeheimnis resultieren können.[708] Zweitens ist die Aufforderung, das Datengeheimnis stets gewissenhaft zu wahren, erforderlich.[709] Zu Beweiszwecken gilt es als ratsam, die Durchführung der Aufklärung durch Unterschrift der Mitarbeiter bestätigen zu lassen.[710] Für die unternehmerische Praxis bietet es sich an, das unterschriebene Exemplar im Original in die Personalakte mit aufzunehmen und eine Kopie dem Beschäftigten auszuhändigen.[711]

Bei Verstößen gegen das Datengeheimnis können neben arbeitsrechtlichen Maßnahmen – etwa Kündigungen in gravierenden Fällen – auch Bußgelder und Strafen für die betreffenden Mitarbeiter in Betracht kommen.[712] Ordnungswidrigkeiten liegen vor, wenn die Verletzung des Datengeheimnisses gleichzeitig eine in § 43 Abs. 2 BDSG aufgezählte Handlung darstellt.[713] Eine Strafbarkeit kann sich insbesondere aus § 44 BDSG und §§ 203 sowie 206 StGB ergeben.[714]

Vom Datengeheimnis aus § 5 Satz 1 BDSG unberührt bleiben andere gesetzlich verankerte Berufs- oder Amtsgeheimnisse; diese gelten nebeneinander.[715]

Das Bundesdatenschutzgesetz gibt nicht vor, wer die Verpflichtung vorzunehmen hat. Daher kommen vorrangig die Personalabteilung oder der Datenschutzbeauftragte dafür in Frage.[716]

[708] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 5 Rn. 6.
[709] Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 28.
[710] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 5 Rn. 11 f.; in Bezug auf die Wirksamkeit des Datengeheimnisses ist die Unterschrift des Mitarbeiters nicht als konstitutive Voraussetzung zu werten; das Datengeheimnis gilt sogar dann, wenn der Mitarbeiter seine Unterschrift verweigert. Nur die Aufklärung durch den Arbeitgeber oder den betrieblichen Datenschutzbeauftragten muss stattgefunden haben, Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 29.
[711] Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 28.
[712] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 5 Rn. 3 f.
[713] Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 33.
[714] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 5 Rn. 3; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 5 Rn. 2; Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 34 f.; zu den zivilrechtlichen Folgen des § 44 BDSG s. *Wybitul/Reuling*, CR 2010, 829 ff.
[715] Simitis/*Ehmann*, BDSG, 7. Aufl. 2011, § 5 Rn. 7 f.; *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 5 Rn. 1.
[716] *Runge*, DuD 1993, 321 (322); zum innerorganisatorischen Datenschutzbeauftragten ausführlich Kapitel 7.1.1 „Beauftragter für Datenschutz“.

6.2 Notwendige Schutzmaßnahmen nach § 9 BDSG

Aus § 9 BDSG resultiert für öffentliche und nichtöffentliche Callcenter-Betriebe die Verpflichtung, technische und organisatorische Vorkehrungen zu treffen, die ein hohes Maß an Datensicherheit gewährleisten. Die in der Anlage zu der Vorschrift aufgeführten Schutzmaßnahmen konkretisieren die notwendigen Erfordernisse, wobei die Bestimmungen der Anlage nur für automatisierte Datenverarbeitungsprozesse gelten. Durch das Wort „insbesondere“ in Satz 2 der Anlage wird deutlich, dass der Maßnahmenkatalog nicht abschließend ist. Im Vordergrund steht zwar zunächst die Sicherheit der Daten, jedoch dienen die Maßnahmen primär dem Datenschutz; es kommt zu einer „Überschneidung“ der Begriffe. Werden Datenverlust, -diebstahl und -verfälschung verhindert, trägt dies auch zur Wahrung der Persönlichkeitsrechte von Betroffenen bei. Dabei gilt es zu berücksichtigen, dass nur insoweit Handlungsbedarf besteht, als die Maßnahmen verhältnismäßig in Bezug auf den angestrebten Zweck ausfallen.[717] Bei der Bestimmung der Erforderlichkeit muss gemäß Anlage zu § 9 BDSG auch die Art der zu schützenden personenbezogenen Daten oder Datenkategorien herangezogen werden. Die Schutzwürdigkeit hoch sensitiver personenbezogener Informationen, wie Sozialdaten, ist wesentlich höher als bei einfachen Adressangaben.[718]

Um stets ein hohes Niveau an Datenschutz und -sicherheit gewährleisten zu können, müssen die organisationsinternen Datenverarbeitungsprozesse einer regelmäßig stattfindenden Risikoanalyse unterzogen werden.[719] Wesentliche Kriterien stellen in diesem Zusammenhang die drei allgemeinen Schutzziele der IT-Sicherheit dar; dies sind Vertraulichkeit, Integrität und Verfügbarkeit.[720] Die durchzuführende Risikoanalyse ist eine systematische Überprüfung der Informationstechnik im Hinblick auf Ursachen und Folgen der Gefährdungen. Hochrelevant sind dabei Fragen nach der Art der verarbeiteten Daten und dem Verarbeitungsverfahren, woraus sich die Gefährdung ergibt, sowie Fragen, welche Schäden potenziell entstehen und welche Auswirkungen aus Schäden resultieren können.[721]

[717] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 1 ff.
[718] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 9 Rn. 18; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 9; *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 2; *Duisberg/Picot*, CR 2009, 823 (825).
[719] *Schmidl*, NJW 2010, 476; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 9.
[720] *Schmidl*, NJW 2010, 476 (477); *Schill/Springer*, Verteilte Systeme, 2007, 124; zu den Schutzzielen der IT-Sicherheit ausführlich *Bedner/Ackermann*, DuD 2010, 323 ff., die die drei Oberziele der IT-Sicherheit zu weiteren Schutzzielen konkretisieren.
[721] *Ernestus*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.2 Rn. 31.

Die Schutzpflichten erstrecken sich ferner auf den personellen Aspekt: Zwar richtet sich die Pflicht zur Einleitung adäquater Schutzvorkehrungen an die Unternehmensleitung, dennoch müssen vorrangig Mitarbeiter, die alltäglich mit der IT-Einrichtung des Unternehmens arbeiten, die IT-sicherheitsrelevanten Vorgaben einhalten und umsetzen; andernfalls können arbeitsrechtliche Sanktionen drohen.[722] Die Mitarbeiter sind auf Einhaltung des Datengeheimnisses[723] gemäß § 5 BDSG zu verpflichten. Dem Datenschutzbeauftragten obliegt nach § 4g Abs. 1 Satz 3 Nr. 2 BDSG die Aufgabe, die mit der personenbezogenen Datenverarbeitung betrauten Mitarbeiter auf die Beachtung des Datenschutzes hin zu sensibilisieren.[724]

Auch im Auftrag für andere Unternehmen tätige Datenverarbeiter (sogenannte Auftragsdatenverarbeiter[725] gemäß § 11 BDSG) müssen die Voraussetzungen des § 9 BDSG und dessen Anlage erfüllen. Eine solche Auftraggeber-/Auftragnehmerkonstellation kann beispielsweise dann gegeben sein, wenn sich ein Unternehmen bei der Erbringung telefonischer Dienstleistungen eines externen Callcenters bedient.

Satz 1 der Anlage zu § 9 BDSG hebt eine den aufgeführten Verpflichtungen der Anlage übergeordnete Kontrollfunktion hervor: Es handelt sich hierbei um die Organisationskontrolle, die notwendige organisatorische Rahmenbedingungen schaffen soll, um sämtliche anderen Forderungen zu erfüllen. Sie bezweckt die eindeutige innerorganisatorische Festlegung von Verantwortlichkeiten und Berechtigungen.[726] Dem einzelnen Mitarbeiter darf nur insoweit der Zugriff auf personenbezogene Daten erlaubt sein, als er ihn zur Erledigung seiner Arbeitsaufgabe benötigt.[727] Diese Forderung wird durch das systeminterne Rechtemanagement erfüllt.

Nachfolgend werden die in der Anlage zu § 9 BDSG enthaltenen technischen und organisatorischen Maßnahmen kurz aufgezeigt.[728] Wer solche Vorkehrungen im Zusammenhang mit dem Gesprächsmanagement-System treffen muss, ist ausschließlich abhängig davon, wie die konkrete Systemarchitektur rechtlich und geografisch gestaltet wird. Die Entscheidung darüber kann nur einzelfallbezogen ge-

[722] *Trappehl/Schmidl*, NZA 2009, 985 ff.
[723] Dazu ausführlich Kapitel 6.1 „Verpflichtung der Mitarbeiter auf das Datengeheimnis".
[724] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 9 Rn. 22.
[725] Dazu ausführlich Kapitel 3.2.2 „Regelungen beim Outsourcing von Callcenter-Dienstleistungen".
[726] *Heibey*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.5 Rn. 37.
[727] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 24.
[728] Zu den notwendigen technischen und organisatorischen Maßnahmen in Bezug auf Telefonanlagen ausführlich *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 190 ff.; *Hammer/Roßnagel*, DuD 1990, 394 ff.

troffen werden. Der einfachste Fall liegt vor, wenn das gesamte Gesprächsmanagement-System im Callcenter-Betrieb implementiert wird.

Ergänzend ist anzuführen, dass sämtliche personenbezogenen Daten, die ausschließlich zur Sicherstellung eines ordnungsgemäßen Betriebs von IT-Systemen, zur Datenschutzkontrolle sowie zur Datensicherung gespeichert werden, der strengen Zweckbindung des § 31 BDSG unterliegen. Die entsprechende Vorschrift für den öffentlichen Bereich auf Bundesebene findet sich in § 14 Abs. 4 BDSG. Einige Datenschutzgesetze der Länder enthalten wortgetreue oder ähnliche Regelungen. Die Verwendung dieser Daten ist nur für die genannten Zwecke zulässig. Werden zum Beispiel Protokolle über den Zutritt zu Räumen angefertigt – und soll die Protokollierung ausschließlich[729] der Zutrittskontrolle dienen –, liegt die strikte Zweckbindung vor.[730] Aufgrund des den Daten innewohnenden Kontrollpotenzials in Bezug auf das Verhalten oder die Leistung der Mitarbeiter sind mit technischen Mitteln erstellte Zutrittsprotokolle nach § 87 Abs. 1 Nr. 6 BetrVG oder § 75 Abs. 3 Nr. 17 BPersVG oder nach den entsprechenden landesgesetzlichen Regelungen mitbestimmungspflichtig, wenn eine Auswertung grundsätzlich möglich ist.[731]

6.2.1 Zutrittskontrolle

Unbefugte Personen dürfen keinen Zutritt zu Datenverarbeitungsanlagen haben, die personenbezogene Daten verarbeiten oder nutzen. Der Begriff „Zutritt“ ist in diesem Kontext ausschließlich räumlich zu verstehen.[732] Die Berechtigung zum Zutritt zu Räumen, in denen Datenverarbeitungssysteme stehen, lässt sich durch verschiedene Maßnahmen kontrollieren; dazu zählen

- Ausweisüberprüfung,[733]
- biometrische Authentifizierungsverfahren,[734]
- Schließanlage und
- Kennwortschutz.

[729] Nicht unzulässig wäre aber beispielsweise, die Zutrittsprotokolle auch zur Arbeitszeiterfassung zu nutzen, wenn beide Zwecke im Vorfeld festgelegt wurden (so auch *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 31 Rn. 5).
[730] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 31 Rn. 1 ff.
[731] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 31 Rn. 1.
[732] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 6; ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 9 Rn. 3.
[733] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 6.
[734] *von Stechow*, Datenschutz durch Technik, 2005 ,75; dazu ausführlich *Hornung/Steidle*, AuR 2005, 201 ff.; *Tillenburg*, DuD 2011, 197 ff.

Durch weitere Vorkehrungen, wie die Installation von Überwachungseinrichtungen[735] oder Alarmanlagen oder die Anwendung des Vier-Augen-Prinzips beim Betreten der Räume, erhöht sich das Sicherheitsniveau.[736]

Einer besonderen Regelung bedarf die Frage, wie die Zutrittsberechtigungen von beispielsweise Wartungspersonal, Hausmeister oder Reinigungskräften ausgestaltet sein sollen.[737] Darüber hinaus ist festzulegen, wie in Notfallsituationen verfahren werden soll.[738] Unter Umständen ist auch die Zutrittsmöglichkeit von (potenziellen) Kunden regelungsbedürftig. Dies kann etwa bei einem Outsourcing-Callcenter oder einem Unternehmen, auf das die Datenhaltung eines anderen Unternehmens ausgelagert wurde, notwendig sein: Nach § 11 Abs. 2 Satz 1 BDSG muss der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen. Aus diesem Erfordernis leitet sich regelmäßig die Verpflichtung für den Auftraggeber ab, auch die Räumlichkeiten zu begutachten, in denen die Datenverarbeitungsanlagen untergebracht sind.[739]

6.2.2 Zugangskontrolle

Mittels der Zugangskontrolle soll sichergestellt sein, dass nur Berechtigte Zugang zu den Datenverarbeitungsanlagen haben. Im Gegensatz zum Zutritt handelt es sich hierbei nicht um den körperlichen Einlass, sondern um die technische und organisatorische Möglichkeit der Nutzung des Datenverarbeitungssystems.[740] Unter den Begriff der Nutzung sind sämtliche Einflussnahmen auf den Verarbeitungsvorgang selbst mittels Datenverarbeitung zu fassen.[741]

Die Zugangskontrolle ist insbesondere für Service-Rechenzentren relevant, die für andere Unternehmen Datenverarbeitungsprozesse vornehmen. Sie kann vornehmlich durch technische und programmtechnische Maßnahmen realisiert werden: Die Vergabe von Passwörtern sowie deren Protokollierung stellen geeignete Vorkeh-

[735] Solche Vorkehrungen werfen unter Umständen weitergehende datenschutzrechtliche Fragen auf.
[736] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 9 Rn. 59.
[737] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 9 Rn. 4.
[738] *Roth*, ITRB 2010, 60 (61).
[739] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 9 Rn. 67 ff.
[740] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 23 ff.; *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 9 Rn. 70.
[741] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 7.

rungen dar.[742] Außerdem können biometrische Authentifizierungsverfahren adäquate Sicherungsmittel darstellen. Auch eine Firewall dient zur Abwehr von Angriffen auf das Verarbeitungssystem. Satz 3 der Anlage zu § 9 BDSG fordert überdies ausdrücklich dem Stand der Technik entsprechende Verschlüsselungsverfahren.

6.2.3 Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Nutzung des Systems berechtigten Personen – also etwa die Callcenter-Agenten – nur auf solche Daten zugreifen können, für die sie eine Zugriffsberechtigung besitzen.[743] Die Mitarbeit in verschiedenen Kampagnen kann eine temporäre Freischaltung unterschiedlicher Datenbankbereiche erfordern. Die Zugriffsmöglichkeit auf die jeweiligen Datenfelder lässt sich am einfachsten mit einer Passwortabfrage beschränken. Das Berechtigungskonzept sollte möglichst fein und individuell festlegbar sein.[744] Außerdem ist der Zugriff auf das unabdingbar notwendige Mindestmaß zu limitieren.[745] Nicht nur die Eingrenzung auf Datenbereichsebene, sondern auch auf bestimmte Nutzungshandlungen muss dabei in Erwägung gezogen werden. So können beispielsweise gewisse Mitarbeitergruppen mit einem Zugriffsrecht, das nur das Lesen erlaubt, ausgestattet werden.[746]

Darüber hinaus beinhaltet diese Kontrollfunktion einen weiteren Aspekt, namentlich die Speicherkontrolle.[747] Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.[748] Zur Umsetzung der Zugriffskontrolle dienen gemäß Satz 3 der Anlage zu § 9 BDSG insbesondere dem Stand der Technik entsprechende Verschlüsselungsverfahren.

---

[742] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 9 Rn. 75 f.; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 23.
[743] *Federrath/Pfitzmann*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.2 Rn. 33; *von Stechow*, Datenschutz durch Technik, 2005, 76.
[744] *Hahn*, DuD 2003, 605 (607).
[745] *Hammer/Roßnagel*, DuD 1990, 394 (400).
[746] *Roth*, ITRB 2010, 60 (61).
[747] Im BDSG 90 war die Speicherkontrolle eine in der Anlage zu § 9 BDSG separat aufgeführte Sicherungsmaßnahme.
[748] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 24; *Heibey*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.5 Rn. 45.

6.2.4 Weitergabekontrolle

Bei ihrer elektronischen Übertragung, ihrem Transport sowie ihrer Speicherung dürfen personenbezogene Daten von Unbefugten nicht gelesen, kopiert, verändert oder entfernt werden können. Unbefugt handelt, wer außerhalb seiner ihm übertragenen Kompetenzen und Aufgaben agiert.[749] Überdies muss überprüf- und feststellbar sein, an wen Übermittlungen personenbezogener Daten durch das Verarbeitungssystem vorgesehen sind.

Ein konkreter Schritt, der dem Schutz der Daten im Rahmen des Übermittlungsvorgangs dient, ist nach Satz 3 der Anlage zu § 9 BDSG die Anwendung von Verschlüsselungsverfahren. Zusätzlichen Schutz bietet die Nutzung von VPN-gesicherten Übertragungswegen.[750] Übermittlungsprotokolle dienen dazu, die Empfänger der Daten bei Übertragungsprozessen zu ermitteln.[751] Die Datenträger sollten gekennzeichnet und der gesamte Bestand katalogisiert werden. Bei der Entnahme von Datenträgern ist eine Registrierung durchzuführen, die mindestens das Datum, den Zeitpunkt und die Person, die das Medium mitnimmt, umfasst.[752]

6.2.5 Eingabekontrolle

Die Nachvollziehbarkeit aller durchgeführten Aktionen innerhalb des Verarbeitungssystems muss durch die Eingabekontrolle umgesetzt sein. Anhand dieser Maßnahme soll detailliert ermittelt werden können, welcher Benutzer wann welchen Vorgang getätigt hat. Somit lassen sich sämtliche Veränderungen, etwa die Erstellung, Erweiterung und Löschung von Daten, feststellen und einem Mitarbeiter zuordnen.[753] Voraussetzung dafür ist allerdings, dass jeder einzelne Nutzer eindeutig identifizierbar ist.[754] Erfolgt eine Authentisierung der Nutzer auf Grundlage eines nutzerindividuellen Passworts, liegt die notwendige Identifizierbarkeit vor. Technisch lässt sich die Überprüfbarkeit der Nutzungsvorgänge durch die Einrichtung von Protokollierungsverfahren realisieren.[755]

---

[749] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 25.
[750] *Roth*, ITRB 2010, 60 (61 f.).
[751] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 9 Rn. 5; a. A. *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 12, der grundsätzlich keine Übermittlungsprotokolle für erforderlich hält.
[752] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 9 Rn. 5.
[753] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 26.
[754] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 12.
[755] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 26.

Die Mitarbeiter im Callcenter können nach verschiedenen Kategorien differenziert werden, die – abhängig von ihrer Arbeitsaufgabe – jeweils über bestimmte Rechte im Gesprächsmanagement-System verfügen müssen. Eine solche Segmentierung führt zur Vereinfachung des Rechtemanagements.[756] So besitzen etwa sämtliche Callcenter-Agenten dieselben Rechte. Dass beispielsweise dem Teamleiter und dem Trainer weitergehende Rechte zuzugestehen sind, versteht sich von selbst. Wichtig in diesem Zusammenhang ist nur, dass jede Aktion am System einer Person eindeutig zurechenbar ist.

6.2.6 Auftragskontrolle

Die Auftragskontrolle muss in engem Zusammenhang mit den Forderungen des § 11 BDSG gesehen werden. Direkter Adressat der Regelung ist der Auftragnehmer, mittelbar wird jedoch auch der Auftraggeber in die Pflicht genommen.[757] Verantwortlich für die Einhaltung der Datenschutzvorschriften bleibt gemäß § 11 Abs. 1 Satz 1 BDSG der Auftraggeber selbst. Darüber hinaus hat er beispielsweise den Auftragausführenden sorgfältig auszuwählen und eine detaillierte schriftliche Festlegung zu treffen, wie das Auftragsverhältnis ausgestaltet sein soll. § 11 Abs. 2 BDSG enthält überdies eine nicht abschließende Aufzählung von inhaltlichen Bestandteilen der Auftragsvergabe.

Durch die Auftragskontrolle ist ausdrücklich gefordert, dass im Auftrag verarbeitete personenbezogene Daten nur den Weisungen des Auftraggebers entsprechend verarbeitet werden können. In der Konsequenz hat das auslagernde Unternehmen hinreichend konkrete und präzise Anweisungen zu erteilen. Außerdem gilt es, eine klare Kompetenzverteilung zwischen dem Auftraggeber und Auftragnehmer vorzunehmen.[758]

6.2.7 Verfügbarkeitskontrolle

Die Forderung im Rahmen der Verfügbarkeitskontrolle besteht im Schutz personenbezogener Daten vor zufälligem Verlust oder Zerstörung. Hauptsächlich Gefahren durch höhere Gewalt soll damit begegnet werden.[759] Die regelmäßige Anferti-

[756] *Schill/Springer*, Verteilte Systeme, 2007, 136.
[757] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 27.
[758] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 9 Rn. 7.
[759] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 28.

gung von Sicherungskopien, deren Aufbewahrung andernorts und unter besonderem Schutz erfolgt, stellt eine mögliche Verfahrensweise dar.[760]

In Abhängigkeit verschiedener Faktoren, darunter auch die Wichtigkeit und Menge der zu sichernden Daten, sind bei der Erstellung eines Datensicherungskonzepts hauptsächlich folgende Aspekte zu betrachten:

- Zeitpunkt und Zeitintervall der Sicherungen,
- Zuständigkeits- und Verantwortlichkeitsregelungen,
- Anzahl der aufzubewahrenden Generationen,
- Umfang der jeweiligen Datensicherungen sowie
- Dokumentation der Sicherungen.[761]

Die in der CRM-Datenbank gespeicherten Kundendaten bilden einen wichtigen Grundpfeiler für die Funktionsfähigkeit des Gesprächsmanagement-Systems. Diese Daten sollten regelmäßig adäquat gesichert werden.

6.2.8 Datentrennung

Der im Datenschutzrecht bedeutsame Grundsatz der Zweckbindung kommt auch durch die Forderung nach Datentrennung zum Ausdruck: Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.[762] Dies gilt nicht für Systeme, die zulässige Zweckänderungen oder Zusammenführungen von Daten von vorneherein vorsehen.[763]

Die Umsetzung der Datentrennung hat jedoch nicht derart zu erfolgen, dass die Daten auf unterschiedlichen Datenträgern gespeichert werden müssen. Sie kann softwareseitig etwa mittels Benutzerrechteverwaltung und Datenseparierung realisiert sein.[764] Auch eine Einschränkung dahingehend, dass nur bestimmte Anwendungen auf ausgewählte Daten zugreifen können, ist denkbar.[765]

---

[760] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 14.
[761] *BSI*, IT-Grundschutz-Kataloge (abrufbar unter: https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m06/m06032.html).
[762] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 29.
[763] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 9 Rn. 15.
[764] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rn. 29.
[765] *Roth*, ITRB 2010, 60 (63).

7 Datenschutzkontrolle

Jedem Betroffenen, dessen personenbezogene Daten verarbeitet werden, stehen verschiedene Informations- und Mitwirkungsrechte zu, wie die auf Auskunft und Berichtigung. Insofern besitzt bereits der Einzelne Möglichkeiten, selbst den Umgang mit seinen Daten zu kontrollieren. Da dies jedoch nur in einem begrenzten Umfang möglich ist, und oftmals die Wahrnehmung der angesprochenen Rechte bereits an ihrer Unkenntnis scheitert, bedarf es übergeordneter Institutionen, die die Wahrung des informationellen Selbstbestimmungsrechts der Betroffenen sicherstellen.

Eine institutionalisierte Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften durch organisationseigene und -fremde Einrichtungen ist deshalb so wichtig, weil sie die Betroffenen in Ausübung ihrer Rechte unterstützen und selbst vorbeugend über die Beachtung des Datenschutzes wachen.[766]

Nachstehend werden die existierenden Überwachungsorgane, differenziert nach organisationsinterner Kontrolle und -externer Kontrolle, näher beleuchtet.

7.1 Interne Kontrollorgane

7.1.1 Beauftragter für Datenschutz

Aus § 4f BDSG resultiert bei Vorliegen bestimmter Voraussetzungen die Pflicht zur Bestellung eines Datenschutzbeauftragten. Verpflichtet werden aufgrund dieser Vorschrift sämtliche öffentlichen Stellen des Bundes, wenn sie personenbezogene Daten automatisiert verarbeiten. Der behördliche Beauftragte kann gemäß § 4f Abs. 1 Satz 5 BDSG auch für mehrere Bereiche, zum Beispiel Dienststellen, gleichzeitig verantwortlich sein.[767] Für öffentliche Stellen der Landesverwaltung ist das Erfordernis der Bestellung durch die Landesdatenschutzgesetze unterschiedlich geregelt.[768]

Die Notwendigkeit zur Ernennung eines Beauftragten für Datenschutz besteht bei nichtöffentlichen Stellen in der Regel erst, wenn dort mehr als neun Personen mit

[766] *Heil*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.1 Rn. 1.
[767] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4f Rn. 1 ff.
[768] Eine freiwillige Bestellung ist etwa durch § 10a Abs. 1 Satz 1 HmbDSG oder § 10 Abs. 1 Satz 1 LDSG vorgesehen, während die Bestellung durch § 5 Abs. 1 Satz 1 HDSG zwingend durchgeführt werden muss.

automatisierten Verarbeitungsvorgängen befasst sind.[769] Da die Zahl der im Callcenter-Betrieb Beschäftigten im Regelfall neun übersteigen wird, ist die Bestellung eines Datenschutzbeauftragten für nichtöffentliche Callcenter normalerweise verpflichtend. Das Gesprächsmanagement-System erfüllt die Tatbestandsvoraussetzungen der automatisierten Datenverarbeitung ohne jeden Zweifel.

Gemäß § 4f Abs. 1 Satz 6 BDSG ist die Einsetzung eines Beauftragten für Datenschutz – unabhängig von der Mitarbeiterzahl – obligatorisch, wenn beispielsweise automatisierte Verfahren eingeführt werden, die der Vorabkontrolle unterliegen, oder eine automatisierte Verarbeitung zur Markt- und Meinungsforschung stattfindet.[770]

Eine solche innerbehördliche oder -betriebliche Selbstkontrolle durch die Person des Datenschutzbeauftragten soll insbesondere der Entlastung staatlicher Aufsichtsorgane dienen.[771] Der Beauftragte für Datenschutz sorgt in der Behörde oder im Betrieb für die Umsetzung und Einhaltung der Bestimmungen des Bundesdatenschutzgesetzes sowie weiterer datenschutzrechtlicher Vorschriften.

Damit auch in nichtöffentlichen Organisationen, die nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet sind, die Ausführung der in § 4g Abs. 1 und 2 BDSG verankerten Tätigkeiten erfolgt, müssen die Unternehmensleitungen gemäß § 4g Abs. 2a BDSG entsprechende Maßnahmen einleiten. Somit wird die Geschäftsleitung faktisch zum Beauftragten für den Datenschutz.[772]

Aus Gründen der Vollständigkeit wird darauf hingewiesen, dass für die obersten Bundesbehörden, für den Präsidenten des Bundeseisenbahnvermögens und für bestimmte bundesunmittelbare Anstalten, Stiftungen sowie Körperschaften des öffentlichen Rechts (zum Beispiel Bundesagentur für Arbeit und Deutsche Bundesbank) § 18 Abs. 1 BDSG vorsieht, dass sie selbst die Kontrolle über die Einhaltung des Datenschutzes ausüben. Diese Stellen müssen dafür sorgen, dass sowohl die allgemeinen als auch die bereichsspezifischen Regelungen zum Datenschutz eingehalten werden.[773] Dazu dient auch die Einsetzung eines Datenschutzbeauftragten.[774]

[769] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4f Rn. 9.
[770] *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 12 Rn. 590.
[771] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 1; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4f Rn. 1; *Klug*, RDV 2001, 12 (13); *Petri*, RDV 2003, 267 (269).
[772] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 4g Rn. 1.
[773] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 18 Rn. 1.
[774] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 18 Rn. 4.

Dem organisationsinternen Datenschutzbeauftragten kommt hinsichtlich der datenschutzgerechten Gestaltung der Prozesse im Callcenter die größte praktische Bedeutung zu. Die Darstellung seiner Aufgaben, Befugnisse und Pflichten erfolgt daher ausführlicher als die bei den übrigen Kontrollorganen.

7.1.1.1 Aufgaben

Das Aufgabenfeld des Beauftragten für Datenschutz ist in § 4g BDSG festgelegt. Seine Hauptfunktion besteht darin, die Vorschriften des Bundesdatenschutzgesetzes dahingehend zu konkretisieren, dass sie auf die unternehmensindividuellen Gegebenheiten angewendet werden können.[775] § 4g Abs. 1 Satz 1 BDSG bestimmt, dass der Datenschutzbeauftragte auf die Einhaltung des Bundesdatenschutzgesetzes sowie anderer datenschutzrechtlicher Vorschriften hinwirkt. Die Norm enthält zwar einzelne konkrete Verpflichtungen, jedoch ist dieser Katalog nicht als abschließend zu betrachten. Differenzieren lassen sich die mit der Vorschrift umfassten Aufgaben in Kontroll-, Beratungs- und Schulungstätigkeiten.[776] Bestehen Zweifel bei der Ausübung seiner Funktionen, kann der Datenschutzbeauftragte die für die verantwortliche Stelle zuständige Aufsichtsbehörde konsultieren und von ihr Beratung sowie Unterstützung gemäß § 38 Abs. 1 Satz 2 BDSG in Anspruch nehmen.

Damit eine adäquate Aufgabenerfüllung des Datenschutzbeauftragten gewährleistet ist, muss er insbesondere zwei Voraussetzungen erfüllen: Er hat einerseits ausreichende Fachkunde zu besitzen und andererseits Zuverlässigkeit vorzuweisen.[777] Das erforderliche Maß an datenschutzrechtlicher Qualifikation kann nicht pauschal angegeben werden, sondern bestimmt sich hauptsächlich abhängig von Faktoren wie

- Umfang der jeweiligen Datenverarbeitungsprozesse,
- Schutzwürdigkeit der personenbezogenen Daten[778] sowie
- Größe und Struktur des Unternehmens.[779]

Das notwendige Fachwissen bezieht sich primär auf die nachfolgend aufgeführten Kompetenzbereiche:

[775] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4g Rn. 5.
[776] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 16 ff.
[777] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 4f Rn. 3.
[778] *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 10; *Gola/Klug*, NJW 2007, 118 (120).
[779] *Gola/Klug*, NJW 2007, 118 (120).

- allgemeine EDV-Kenntnisse,
- fundiertes Wissen im allgemeinen und bereichsspezifischen Datenschutzrecht,
- Kenntnis der datenschutzrelevanten Vorschriften des Betriebsverfassungsgesetzes,[780]
- Verständnis komplexer betriebswirtschaftlicher Zusammenhänge,
- Kenntnis aktueller Techniken und Prozesse der automatisierten Datenverarbeitung,[781]
- pädagogisch-didaktische Fähigkeiten,[782]
- psychologisches Einfühlungsvermögen[783] sowie
- Sozial- und Methodenkompetenz.[784]

Die für die Aufgabenerfüllung unabdingbare Zuverlässigkeit lässt sich nur schwer operationalisieren; abzustellen ist bei ihrer Bestimmung auf charakterliche Eigenschaften, wie

- Gewissenhaftigkeit,
- Loyalität und
- Verschwiegenheit.

Jedenfalls wird die notwendige Zuverlässigkeit nicht gegeben sein, wenn die Person zuvor durch irgendein Verhalten aufgefallen ist, welches das Vertrauen zu ihr erschüttert hat.[785]

7.1.1.1.1 Kontrolle

Ganz allgemein hat der Beauftragte für Datenschutz eine weitreichende Kontrollfunktion inne, die sich auf sämtliche personenbezogenen Verarbeitungsprozesse innerhalb der Organisation bezieht. Von seiner Überwachung betroffen sind nicht lediglich groß angelegte Datenverarbeitungsvorgänge in Großrechenanlagen, sondern vielmehr auch die einzelnen Bedienplätze mit ihrer IT- und TK-Anbindung, an denen autonom oder dezentral Daten verarbeitet werden.[786] Dazu zählen die Ar-

[780] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 113.
[781] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4f Rn. 20.
[782] *Abel*, MMR 2002, 289 (291).
[783] *Simitis*, NJW 1998, 2395 (2396).
[784] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 114.
[785] *Abel*, MMR 2002, 289 (291).
[786] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 48 ff.

beitsplätze der Callcenter-Agenten mit ihrem jeweiligen Computersystem, insbesondere dem Frontend-System.

Weitere grundlegende Aufgaben des Datenschutzbeauftragten sind die Erfüllung der in der Anlage zu § 9 BDSG genannten Anforderungen sowie primär die Sicherstellung, dass

- sich die Vorgänge des Erhebens, Verarbeitens oder Nutzens von personenbezogenen Daten zulässig vollziehen,
- eine angemessene Auskunft und Benachrichtigung der Betroffenen erfolgen und
- die Berichtigung, Sperrung und Löschung vorschriftsmäßig umgesetzt werden.[787]

Die datenschutz- und datensicherheitsbezogene Kontrolle von IT-Systemen muss alle Komponenten mit einschließen; zu nennen sind angeschlossene Datenbank-Systeme, Betriebssystemsoftware, Hardwarebestandteile auf Client- und Serverebene sowie Aspekte der Vernetzung.[788]

Durch § 4d BDSG ist grundsätzlich eine Meldepflicht für automatisierte Datenverarbeitungsverfahren vorgeschrieben. Die Meldung muss gemäß § 4d Abs. 1 BDSG gegenüber der zuständigen Aufsichtsbehörde oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erfolgen. § 4d Abs. 2 BDSG sieht vor, dass diese Meldung unter anderem entfallen kann, wenn das Callcenter über einen Beauftragten für Datenschutz verfügt;[789] davon ist normalerweise auszugehen. In diesem Fall obliegt dem Callcenter aus § 4g Abs. 2 Satz 1 BDSG die Verpflichtung, dem Beauftragten für Datenschutz eine Übersicht sowohl über die in § 4e Satz 1 Nr. 1 - 9 BDSG aufgeführten Angaben als auch über die Personen mit Zugriffsberechtigung bereitzustellen. Der Datenschutzbeauftragte muss sich diese Informationen nicht etwa bei den einzelnen Abteilungen beschaffen, sondern die Organisation hat die erforderlichen Fakten zur Verfügung zu stellen.[790]

Der Datenschutzbeauftragte führt auf der Grundlage dieser Informationen das Verfahrensverzeichnis. § 4e BDSG enthält die zwingenden Inhalte eines solchen Ver-

[787] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 4g Rn. 25.
[788] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 54.
[789] *Schild*, DuD 2001, 282 f.; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4d Rn. 6 f.; *Pahlen-Brandt*, DuD 2007, 24 (25); *Gola/Klug*, NJW 2007, 118 (122).
[790] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4g Rn. 60; *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 26; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4g Rn. 23.

zeichnisses; so sind zum Beispiel die Anschrift der verantwortlichen Stelle, die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung sowie die vorgesehenen Löschungsfristen in das Register mit aufzunehmen. Wichtig in diesem Zusammenhang ist, dass den mit aufgenommenen Angaben eine ausreichende Aussagekraft innewohnt.[791]

Gemäß § 4g Abs. 2 Satz 2 BDSG hat der Datenschutzbeauftragte das Verfahrensverzeichnis auf Anfrage jedermann verfügbar zu machen. Wie dies konkret geschieht, bleibt ihm selbst überlassen. So ist die Anfertigung von Kopien in Papierform gleichermaßen denkbar wie die Einstellung des Registers ins Internet.[792] Darüber hinaus bedarf das Verfahrensverzeichnis einer stetigen Aktualisierung, das heißt neue oder sich ändernde Verfahren sind unverzüglich zu melden.[793]

Durch § 4d Abs. 5 BDSG ist für Datenverarbeitungen, die ein besonderes Risiko für die Rechte und Freiheiten der Betroffenen in sich bergen, grundsätzlich eine Vorabkontrolle[794] vorgesehen. Sie beinhaltet die datenschutzrechtliche Prüfung der Prozesse im Vorfeld der Verarbeitung. Auch die Durchführung der Vorabkontrolle fällt gemäß § 4d Abs. 6 Satz 1 BDSG in den Zuständigkeitsbereich des Beauftragten für Datenschutz.

Insbesondere die automatisierte Verarbeitung besonderer Arten personenbezogener Daten ist unter die genannten risikoreichen Vorgänge zu fassen. Gleiches gilt für Datenverarbeitungen, die die Persönlichkeit des Betroffenen – einschließlich seiner Leistungen, Fähigkeiten und seines Verhaltens – bewerten sollen. So sind die automatisierte Erstellung von Verbraucherprofilen und umfassende personenbezogene Data-Mining-Analysen, wie sie auch im Rahmen des Gesprächsmanagement-Systems vorgesehen sein können, als risikobehaftete Verfahren im Sinne der Vorschrift einzustufen.[795] Gerade für diese Anwendungszwecke werden jedoch ohnehin regelmäßig Einwilligungen der Kunden notwendig sein, was gleichzeitig zur Entbehrlichkeit der diesbezüglichen Prüfung im Vorfeld der Verarbeitung führt.[796] Der Vorabkontrolle bedarf es auch dann nicht, wenn eine gesetzliche Verpflichtung zur

[791] Zum Spannungsverhältnis zwischen erforderlichem Konkretisierungsgrad und zulässiger Abstraktheit des Verfahrensverzeichnisses, einschließlich ausformuliertem Beispiel, s. *Petri*, RDV 2003, 267 ff.
[792] *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 26.
[793] *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 26; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4g Rn. 61.
[794] Zum Komplex Vorabkontrolle s. ausführlich *Klug*, RDV 2001, 12 ff.
[795] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4d Rn. 13.
[796] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4d Rn. 13; *Gola/Klug*, NJW 2007, 118 (122).

Durchführung von Datenverarbeitungsprozessen, die besondere Risiken aufweisen, existiert, oder ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis mit dem Betroffenen den Umgang mit den personenbezogenen Daten rechtfertigt.

Unabhängig vom konkreten Einsatzfeld des Callcenters, welches das Gesprächsmanagement-System nutzt, sollten dem Datenschutzbeauftragten die vorgesehenen Verfahren zur Prüfung der Notwendigkeit der Vorabkontrolle vorgelegt werden. Die Verantwortung für die Zulässigkeit der durchgeführten automatisierten Datenverarbeitungsprozesse liegt letztendlich bei der Leitung der verantwortlichen Stelle.[797]

Die Kontrollfunktion des Datenschutzbeauftragten erstreckt sich jedoch nicht auf die Datenverarbeitungsprozesse der Beschäftigtenvertretung: Der Betriebsrat ist in der Erfüllung seiner Aufgaben grundsätzlich unabhängig vom Arbeitgeber, während der Beauftragte für Datenschutz von der Unternehmensleitung – in der Regel ohne direkte Einflussmöglichkeit des Betriebsrats – ernannt wird. Jeder Arbeitgeber hat somit faktisch die Möglichkeit, eine ihm wohlgefällige Person als Datenschutzbeauftragten auszusuchen.[798] Wenn der Arbeitgeber über den Beauftragten für Datenschutz nun Einblick in Informationen des Betriebsrats hätte, die ihm im Normalfall unzugänglich wären, führte dies zu einem massiven Informationsungleichgewicht und Konfliktpotenzial; mögliche Strategien des Betriebsrats wären dem Arbeitgeber frühzeitig bekannt und der Betriebsrat wäre deshalb in seiner faktischen Handlungsfähigkeit als Interessenvertretung gravierend behindert.[799]

7.1.1.1.2 Beratung

Eine weitere zentrale Aufgabe des Datenschutzbeauftragten besteht in der Beratung verschiedener Zielgruppen; diese setzen sich primär aus der Leitung des Callcenters und den Callcenter-Agenten zusammen. Da der innerorganisatorische Datenschutzbeauftragte selbst keine rechtliche Möglichkeit besitzt, datenschutzrechtliche Maßnahmen durchzusetzen, hat die Beratung der Geschäfts- oder Behördenleitung große

[797] So auch *Engelien-Schulz*, RDV 2003, 270 (273).
[798] Kritisch zur Wirksamkeit von Kontrollen durch innerbetriebliche oder -behördliche Datenschutzbeauftragte *Pahlen-Brandt*, DuD 2007, 24 ff.; zum Interessenkonflikt, wenn der innerbetriebliche Datenschutzbeauftragte gleichzeitig Mitarbeiter in der Revisionsabteilung sein soll, *Ernst*, NJOZ 2010, 2443 ff.
[799] *Wagner*, BB 1993, 1729 ff.

Bedeutung hinsichtlich der Einflussnahme auf die Gestaltung des Datenschutzes innerhalb des Callcenters.[800]

Die Spannweite der Beratungsfunktion schließt alle Bereiche, Anlagen und Tätigkeiten mit ein, die im Zusammenhang mit personenbezogenen Datenverarbeitungsvorgängen stehen. So kann eine Veränderung in der Organisation eines Callcenters einen Rückgriff auf den Sachverstand des Datenschutzbeauftragten erfordern, da zum Beispiel Zugriffsberechtigungen geändert werden müssen. Auch bei der Aufstellung interner Datenschutzrichtlinien und diesbezüglicher Verhaltensanweisungen ist eine Beteiligung des Datenschutzbeauftragten in der Regel überaus sinnvoll.[801]

Wenn Verstöße gegen den praktizierten Datenschutz oder Schwachstellen in demselben festgestellt werden, ist eine konstruktive Lösungsfindung, idealerweise unter Beteiligung sämtlicher Betroffenen, durchzuführen.[802] Die Beratungsleistung soll sich jedoch nicht nur auf die Behebung von Problemen erstrecken, sondern vielmehr auch vorausschauend auf ein hohes Niveau an Datenschutz abzielen. Aus diesem Grund sollte der Datenschutzbeauftragte der Organisation bereits in der Planungsphase beispielsweise bei der Einführung neuer Datenverarbeitungssysteme hinzugezogen werden. Er hat dann im Vorfeld des Wirkbetriebs die Möglichkeit, Anforderungen an das System zu definieren, die den datenschutzrechtlichen Zielsetzungen am besten gerecht werden.[803]

Durch § 4f Abs. 5 Satz 2 BDSG kommt für zum Beispiel Beschäftigte des Callcenters die Möglichkeit zum Ausdruck, den Beauftragten für Datenschutz nach Rat zu fragen. Hiernach können sich Betroffene zu jeder Zeit an ihn wenden. Der Datenschutzbeauftragte sollte in diesem Zusammenhang Offenheit gegenüber Anregungen und Kritik zeigen.[804]

7.1.1.1.3 Schulung

In § 4g Abs. 1 Satz 4 Nr. 2 BDSG ist die Schulungsverantwortung des Datenschutzbeauftragten gesetzlich manifestiert. Er hat die mit der personenbezogenen

[800] *Braun-Lüdicke*, Der Konzerndatenschutzbeauftragte, 2008, 54 f.
[801] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 31 ff.
[802] *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 17.
[803] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 24 f.
[804] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 39.

Datenverarbeitung Beschäftigten auf die Einhaltung der datenschutzrechtlichen Vorschriften und Erfordernisse hin zu sensibilisieren. Idealerweise werden dazu Mitarbeiter zu Beschäftigtengruppen zusammengefasst, um somit eine speziell auf ihre Tätigkeit ausgerichtete datenschutzrechtliche Schulung anzubieten.[805] Dabei muss der bereits vorhandene datenschutzrechtliche Kenntnisstand der Mitarbeiter bei der Planung von Bildungsmaßnahmen Berücksichtigung finden.

Durch die Qualifizierung sollen die Mitarbeiter mit den wesentlichen Vorschriften vertraut gemacht werden und ein Grundverständnis für den Stellenwert des Datenschutzes erlangen. Den Beschäftigten muss unter anderem vermittelt werden,

- wann Daten automatisiert oder nichtautomatisiert in oder aus Dateien verarbeitet, genutzt oder dafür erhoben werden,
- dass bei Vorliegen bestimmter Voraussetzungen ein Benachrichtigungsanspruch des Betroffenen besteht, wenn erstmals eine personenbezogene Datenspeicherung erfolgt,
- dass Betroffenen grundsätzlich ein Auskunftsanspruch zusteht und
- dass der Beauftragte für Datenschutz in allen Fragen des Datenschutzes erster Ansprechpartner für die Mitarbeiter ist.[806]

Im Rahmen seiner Aufgabenausführung steht es dem Datenschutzbeauftragten frei, insbesondere die Methoden und Arbeitsmittel zur Mitarbeiterschulung selbst zu bestimmen.[807] In Frage kommen dabei je nach Kontext:

- Qualifizierung im Rahmen von Veranstaltungen der Personalentwicklung (Aus-, Fort- und Weiterbildung),
- Durchführen abteilungs- oder mitarbeitergruppenspezifischer Vorträge,
- Verteilen von Merkblättern und Informationsbroschüren,
- Anbringen von Aushängen am Schwarzen Brett,
- Informationsbereitstellung über organisationsinterne Kommunikationsmedien (wie Intranet, Unternehmenszeitschrift),
- regelmäßige Tätigkeitsberichterstattung in Mitarbeiterversammlungen.[808]

[805] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 4g Rn. 12; *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 40 f.; *Schierbaum*, Der Personalrat 2001, 454 (458).
[806] *Schaffland/Wiltfang*, BDSG, Stand: April 2011, § 4g Rn. 15.
[807] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4g Rn. 20.
[808] *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 23.

Der Beauftragte für Datenschutz muss die jeweilige Qualifizierungsmaßnahme nicht selbst durchführen; dazu kann er sich beispielsweise eines externen Beraters bedienen. Besonders bei großen Unternehmen ist eine umfangreiche Mitarbeiterschulung, die an die Person des innerbetrieblichen Datenschutzbeauftragten gebunden wäre, aus kapazitativen Gründen nicht möglich.[809] Die Organisation hat die für die Schulungsmaßnahme erforderlichen Räume, Materialien und Finanzmittel bereitzustellen.[810]

In diesem Zusammenhang wird darauf hingewiesen, dass der Datenschutzbeauftragte die Verpflichtung der Mitarbeiter auf das Datengeheimnis[811] vornehmen darf.[812] Ob dies im jeweils konkreten Fall sinnvoll erscheint, muss im Einzelfall entschieden werden. Oftmals wird es aus praktischen Gründen die Personalabteilung sein, die beim Einstellungsgespräch mit neuen Mitarbeitern die Verpflichtung vornimmt. So lässt sich die unterschriebene Erklärung des Mitarbeiters sofort in die Personalakte mit aufnehmen.[813]

7.1.1.2 Auswahl und Bestellung

Grundsätzlich kann entweder eine unternehmensinterne Person oder ein externer Beauftragter die Funktion des Datenschutzbeauftragten ausüben.[814] Pauschal ist keiner der beiden Varianten der Vorzug zu geben – die Entscheidung darüber bedarf stets einer einzelfallabhängigen Prüfung. So wird ein externer Dienstleister, der oftmals mehrere Unternehmen gleichzeitig betreut, über einen tendenziell großen Erfahrungsschatz verfügen, wohingegen insbesondere bei kleinen Unternehmen der Vorteil eines unternehmensinternen Mitarbeiters darin gesehen werden kann, dass er mit den internen Strukturen bestens vertraut ist.[815] Weitergehend kann der Datenschutzbeauftragte seine Tätigkeit hauptamtlich oder nur nebenamtlich ausführen. Dadurch ist eine gewisse Flexibilität gegeben, die sowohl für kleine und mittelständische Unternehmen als auch für Großunternehmen ausreichend Spielraum lässt, die jeweils ideale Lösung zu finden.[816]

[809] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 45.
[810] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4g Rn. 20.
[811] Dazu ausführlich Kapitel 6.1 „Verpflichtung der Mitarbeiter auf das Datengeheimnis".
[812] *Runge*, DuD 1993, 321 (322).
[813] *Kinast*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 5 Rn. 27.
[814] ErfK/*Wank*, BDSG, 11. Aufl. 2011, § 4f Rn. 3.
[815] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4f Rn. 17 f.
[816] *Braun-Lüdicke*, Der Konzerndatenschutzbeauftragte, 2008, 38.

Der Beauftragte ist gemäß § 4f Abs. 1 Satz 1 BDSG schriftlich[817] zu bestellen. Die vorgeschriebene Schriftform nach § 126 BGB macht es erforderlich, dass das Formular zur Ernennung von einem Vertreter der verantwortlichen Stelle und dem zukünftigen Datenschutzbeauftragten eigenhändig unterschrieben wird.[818] Die geforderte Schriftform hat konstitutiven Charakter; wird sie nicht eingehalten, ist die Bestellung unwirksam. Die Nichtbeachtung des Schriftformerfordernisses ist nach § 43 Abs. 1 Nr. 2 und Abs. 3 BDSG bußgeldbewehrt und kann darüber hinaus Schadenersatzansprüche auslösen.[819]

7.1.1.3 Position in der Organisation

In § 4f Abs. 3 Satz 1 und 2 BDSG wird festgeschrieben, dass der Beauftragte für Datenschutz dem Leiter der Organisation direkt zu unterstellen und in Ausübung seiner Tätigkeit weisungsfrei ist. Seine Einordnung in der Organisation wird damit klar vorgegeben und ermöglicht die direkte Kommunikation mit der Leitung. Überdies bildet die Weisungsungebundenheit das zentrale Merkmal seiner Unabhängigkeit; der Callcenter-Betreiber kann dem Datenschutzbeauftragten nicht vorschreiben, wie er seine Aufgaben zu erfüllen hat.[820]

§ 4f Abs. 3 Satz 3 BDSG enthält ein Benachteiligungsverbot für den Datenschutzbeauftragten. Diesbezügliche Benachteiligungen können zum Beispiel im Erschweren der organisationsinternen Kommunikation oder im Ausschluss von Vergünstigungen bestehen.[821] Die Beendigung des Auftragsverhältnisses des Datenschutzbeauftragten kann sich hauptsächlich aus der Abberufung, dem Wegfall der Bestellpflicht und der Amtsniederlegung ergeben. Der Datenschutzbeauftragte genießt durch § 4f Abs. 3 Satz 5 BDSG dasselbe Niveau an Kündigungsschutz wie vergleichbare Funktionsträger. Die Kündigung seines Arbeitsverhältnisses ist grundsätzlich unzulässig; nur wenn Tatsachen vorliegen, die den Callcenter-Betreiber zu einer Kündigung aus wichtigem Grund – ohne die Einhaltung einer Kündigungsfrist – legitimieren, darf sie erfolgen.[822]

---

[817] Der Anhang enthält in Anlage 1 ein Musterschreiben zur Bestellung eines Datenschutzbeauftragten.
[818] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4f Rn. 57; *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 220.
[819] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4f Rn. 59.
[820] Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4f Rn. 121 f .
[821] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 122; unzutreffend *Scheja*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 4f Rn. 83, der die Gültigkeit des Benachteiligungsverbots lediglich auf interne Datenschutzbeauftragte (also Personen, die gleichzeitig Mitarbeiter der jeweiligen Organisation sind) beschränkt sieht.
[822] *Scheja*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 4f Rn. 48.

Ergänzend sei erwähnt, dass der Beauftragte für Datenschutz eine verantwortungsvolle Aufgabe wahrnimmt, die bei falscher oder unsachgemäßer Ausführung zu gravierenden Konsequenzen für die von den Datenverarbeitungen Betroffenen, für das Callcenter und für ihn selbst führen kann.[823]

7.1.2 Beschäftigtenvertretung

Die Beschäftigtenvertretung in Gestalt des Betriebs- oder Personalrats hat allgemein zur Aufgabe, die Interessen der Beschäftigten zu vertreten und ihrem Schutz zu dienen. Insbesondere durch § 75 Abs. 2 BetrVG findet der Schutzauftrag des Betriebsrats sowie des Arbeitgebers im Hinblick auf die Sicherstellung des Arbeitnehmerpersönlichkeitsrechts ausdrücklich Erwähnung. Eine im Wortlaut nach äquivalente Vorschrift existiert im Personalvertretungsrecht zwar nicht, dennoch umfassen § 68 Abs. 1 Nr. 2 BPersVG sowie die entsprechenden Bestimmungen der Landespersonalvertretungsgesetze auch den Schutz der informationellen Selbstbestimmung der Beschäftigten.[824]

Die zunehmende Technisierung der Unternehmen und öffentlichen Stellen, einhergehend mit der umfassenden Ausstattung der einzelnen Arbeitsplätze mit Informationstechnik, führt zu einem steigenden Gefährdungsgrad in Bezug auf das Persönlichkeitsrecht der Mitarbeiter. Aus diesem Grund ist es notwendig, bei der automatisierten Verarbeitung von Beschäftigtendaten ausreichenden Schutz des informationellen Selbstbestimmungsrechts der Mitarbeiter zu gewährleisten.[825] Dies gilt besonders für Callcenter, wo im Regelfall ein Höchstmaß an informationstechnischen Arbeitsmitteln genutzt wird.

Zwischen den Aufgabenfeldern der Beschäftigtenvertretung und des Datenschutzbeauftragten der Organisation besteht eine unmittelbare Verzahnung im Hinblick auf die Überwachung der Einhaltung des Datenschutzes.[826] Die Überschneidung der Zuständigkeitsbereiche führte in der Praxis in einigen Fragen zu unklaren Verhältnissen: Insbesondere die Frage nach einer gegenseitigen Kontrollmöglichkeit stand

[823] Zur Haftung von Datenschutzbeauftragten ausführlich *Helfrich*, CR 1992, 456 ff.; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 4g Rn. 97 ff.
[824] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 247; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 842; zu den Gemeinsamkeiten und strukturellen Unterschieden des Betriebsverfassungsrechts gegenüber dem Personalvertretungsrecht überblicksartig *Richardi*, Der Personalrat 1993, 49 ff.
[825] *Gliss/Kramer*, Arbeitnehmerdatenschutz, 2006, 55.
[826] *Schierbaum*, Der Personalrat 2001, 454 (461).

im Vordergrund der Diskussion.[827] Das *BAG* kam zu dem Ergebnis, dass eine Kontrollbefugnis des betrieblichen Datenschutzbeauftragten hinsichtlich der Datenverarbeitung durch Betriebsräte nicht besteht.[828] Der Hauptgrund liegt darin, dass die Unabhängigkeit des Betriebsrats durch die Person des Datenschutzbeauftragten, die vom Arbeitgeber selbst ausgesucht wird, gefährdet ist. Die Autonomie der Interessenvertretung hat eine spezielle Regelung zur Grundlage, die nach § 1 Abs. 3 Satz 1 BDSG den datenschutzrechtlichen Vorschriften vorgeht.[829]

Im umgekehrten Fall, also hinsichtlich des Kontrollrechts des Betriebsrats gegenüber dem Datenschutzbeauftragten, liegt eine ähnliche Situation vor: Der Betriebsrat darf lediglich feststellen, ob der Datenschutzbeauftragte seine Aufgaben weisungsfrei und ordnungsgemäß auszuüben vermag, um seiner Kontrollfunktion angemessen nachzukommen.[830] Spezifische Kontroll- und Weisungsrechte gegenüber dem Datenschutzbeauftragten besitzt er jedoch nicht.[831]

Auch Akzeptanzprobleme seitens der Beschäftigtenvertretung im Hinblick auf die Bestellung des Datenschutzbeauftragten stellen eine Schwierigkeit dar. Weder der Betriebsrat noch der Personalrat einer öffentlichen Stelle des Bundes verfügt im Grundsatz[832] über ein diesbezügliches Mitwirkungsrecht. Lediglich einzelne Landespersonalvertretungsgesetze[833] sehen ausdrücklich ein Mitbestimmungsrecht vor.[834]

Um potenzielle Konflikte bereits im Vorfeld einzudämmen, sollte der Betriebsrat bei der Bestellung des Datenschutzbeauftragten beteiligt werden.[835] Im Idealfall ist darüber hinaus eine Zusammenarbeit der beiden Kontrollinstanzen Betriebsrat und Datenschutzbeauftragter anzustreben. Eine solche Kooperation kann zu Effizienzgewinnen bei der Kontrolle und zur Vermeidung redundanter Arbeitsschritte führen.

---

[827] Ausführlich zu diesem Spannungsverhältnis *Wagner*, BB 1993, 1729 ff.
[828] *Eckert*, DStR 1998, 1691.
[829] *BAG* v. 11.11.1997, NZA 1998, 385; zu den Konsequenzen des Judikats des *BAG* siehe *Simitis*, NJW 1998, 2395 ff.; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 686.
[830] *Fitting et al.*, HK BetrVG, § 80 Rn. 7; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 688.
[831] *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 688.
[832] Etwas anderes ergibt sich beispielsweise bei einem Sachverhalt, der nach § 99 BetrVG mitbestimmungspflichtig ist.
[833] So etwa § 79 Abs. 3 Nr. 2 LPVG und § 66 Nr. 6 PersVG.
[834] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 224 ff.
[835] *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 12 Rn. 597 ff.

7.1.2.1 Aufgaben im Rahmen der Datenschutzkontrolle

Gemäß § 80 Abs. 1 Nr. 1 BetrVG zählt zu den allgemeinen Aufgaben des Betriebsrats unter anderem die Überwachung, ob die zu Gunsten der Beschäftigten wirkenden Gesetze, Verordnungen, Unfallverhütungsvorschriften sowie Tarifverträge und Betriebsvereinbarungen eingehalten werden. Die entsprechende bundespersonalvertretungsrechtliche Vorschrift, die zusätzlich die Kontrolle der Einhaltung von Verwaltungsanordnungen umfasst, findet sich in § 68 Abs. 1 Nr. 2 BPersVG. Auch in den jeweiligen Landesgesetzen ist eine diesbezügliche Regelung enthalten. Das Bundesdatenschutzgesetz stellt ein solches, die Beschäftigten schützendes Gesetz dar, sofern Daten von Beschäftigten betroffen sind.[836] Dadurch kommt es zu einer doppelten Kontrolle der Einhaltung des Datenschutzes in der Organisation, nämlich durch den Datenschutzbeauftragten sowie durch die Beschäftigtenvertretung.[837]

Das Überwachungsrecht des Kollektivorgans besteht selbst dann, wenn der Arbeitgeber im Rahmen einer Auftragsdatenverarbeitung Beschäftigtendaten bei einem Dritten verarbeiten lässt. Durch eine entsprechende Vertragsgestaltung muss mit dem Serviceunternehmen vereinbart werden, dass die Beschäftigtenvertretung auch dort ihre Überwachungsfunktion ausüben kann.[838]

Zur Aufgabendurchführung steht der Beschäftigtenvertretung aus § 80 Abs. 2 Satz 1 BetrVG, § 68 Abs. 2 BPersVG sowie den entsprechenden landesgesetzlichen Regelungen ein Informationsrecht zu. Sie ist zur Wahrnehmung ihrer Rechte umfassend und rechtzeitig zu unterrichten. Rechtzeitig ist die Information dann erteilt, wenn der Betriebsrat vor einer Entscheidung noch die Möglichkeit besitzt, sich mit den Einzelheiten und potenziellen Auswirkungen der vorgesehenen Maßnahme vertraut zu machen sowie Gegenargumente einzubringen.[839] Umfassend bedeutet, dass sämtliche zur Beurteilung des Sachverhalts notwendigen Informationen mitgeteilt werden müssen. Die Unterrichtung kann grundsätzlich mündlich erfolgen, bei komplexen Sachverhalten ist die Überlassung schriftlicher Unterlagen praktisch unumgänglich.[840] Erst die lückenlose Kenntnis aller Umstände gibt dem Kollektivorgan die

[836] *Fitting et al.*, HK BetrVG, § 80 Rn. 7; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 13 Rn. 630; *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 251; *Schierbaum*, Der Personalrat 2001, 454 (459).
[837] *Thüsing*, in: Richardi (Hrsg.), Kommentar zum Betriebsverfassungsgesetz, 12. Aufl. 2010, § 80 Rn. 8.
[838] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 251; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 13 Rn. 631.
[839] *Kruse*, Der Personalrat 1993, 64 (68); *Schierbaum*, Der Personalrat 2001, 454 (459); *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 13 Rn. 636; *Gola/Wronka*, NZA 1991, 790 (793).
[840] *Thüsing*, in: Richardi (Hrsg.), Kommentar zum Betriebsverfassungsgesetz, 12. Aufl. 2010, § 80 Rn. 52.

Möglichkeit zu beurteilen, inwieweit ein technisches System zur Feststellung von Verhalten oder Leistung der Mitarbeiter objektiv geeignet ist. Auch darüber, ob ausreichende Datensicherheitsmaßnahmen vom Arbeitgeber getroffen wurden, ist die Beschäftigtenvertretung zu unterrichten.[841]

Neben der allgemeinen Unterrichtungspflicht des Arbeitgebers hat die Beschäftigtenvertretung darüber hinaus das Recht, selbst Maßnahmen zur Informationsbeschaffung zu betreiben; dazu sind beispielsweise Betriebsbegehungen und Interviews mit Mitarbeitern denkbar.[842] Im öffentlichen Bereich besteht dieses Überwachungsrecht ebenso[843], wenngleich der Dienststellenleiter in gewissen Fällen, etwa wenn die Kontrolle eine erhebliche Störung des Betriebsablaufs hervorriefe, der Kontrollmaßnahme widersprechen kann.[844] Trotzdem muss der Personalrat ein grundsätzlich gleich gelagertes Überwachungsrecht wie der Betriebsrat besitzen, das auch die Besuchsmöglichkeit einzelner Arbeitsplätze umfasst, da dieses Recht ansonsten ins Leere liefe.[845]

Nach § 80 Abs. 3 BetrVG kann der Betriebsrat zur Durchführung seiner Aufgaben Sachverständige[846] hinzuziehen, soweit dies zur Aufgabenerfüllung notwendig erscheint. Dazu ist mit dem Arbeitgeber eine vorherige Vereinbarung zu treffen. Der Arbeitgeber wird die Inanspruchnahme eines Experten dann nicht verwehren können, wenn ein vernünftiger und seine Tätigkeit gewissenhaft ausführender Betriebsrat auf die Hilfe des Sachverständigen angewiesen ist.[847] Erst dann, wenn der Betriebsrat über verschiedene Möglichkeiten – etwa mittels Studium von Fachliteratur – versucht hat, sich selbst sachkundig zu machen, und trotz dieser Versuche Informationslücken bestehen, soll die Zuziehung eines fachkundigen Dritten als legitim angesehen werden können.[848] Nach § 80 Abs. 2 Satz 3 BetrVG kann der Betriebsrat

[841] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 252.
[842] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 252 f.; *BAG* v. 8.2.1977, AP Nr. 10 zu § 80 BetrVG 1972.
[843] Grundsätzlich lassen sich betriebsverfassungsrechtliche Aussagen auf das Personalvertretungsrecht übertragen; in einzelnen Fällen – so etwa beim Recht, Beschäftigte an ihrem Arbeitsplatz aufzusuchen – kommt es zu Beurteilungsdiskrepanzen durch die Entscheidungen der Verwaltungsgerichte, *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 839.
[844] So *BVerwG* v. 9.3.1990, NJW 1990, 2483.
[845] *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 844; *Kruse*, Der Personalrat 1993, 64 (70); um dieser Rechtsunsicherheit entgegenzuwirken, lautet § 68 Abs. 4 LPVG ausdrücklich: „Der Vorsitzende oder ein beauftragtes Mitglied der Personalvertretung hat jederzeit das Recht, nach vorheriger Unterrichtung des Leiters der Dienststelle, die Dienststelle zu begehen und, sofern die Beschäftigten zustimmen, diese an ihrem Arbeitsplatz aufzusuchen, wenn zwingende dienstliche Gründe nicht entgegenstehen".
[846] Zum Begriff des Sachverständigen *Pflüger*, NZA 1988, 45 ff.
[847] *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 13 Rn. 644; *Pflüger*, NZA 1988, 45 (46).
[848] *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 13 Rn. 645.

auch sachkundige Beschäftigte der Organisation befragen; dies wird jedoch in vielen Fällen zu keinen objektiven Antworten führen, da Mitarbeiter zum Beispiel aus Loyalitätsgründen nicht wahrheitsgemäß Auskünfte erteilen.[849] Obwohl im Personalvertretungsrecht nicht ausdrücklich erwähnt, kann auch der Personalrat grundsätzlich die Hinzuziehung von Sachverständigen verlangen. Auch in einem solchen Fall müssen zuvor sämtliche anderweitigen Informationsquellen ausgeschöpft sein.[850]

7.1.2.2 Befugnisse

Falls der Betriebsrat durch den Arbeitgeber begangene Verstöße gegen das Datenschutzrecht feststellt, kann er sich an die zuständige Aufsichtsbehörde nach § 38 BDSG wenden.[851] Ähnliches gilt für den Personalrat, der die Möglichkeit hat, die für seine öffentliche Stelle zuständige Kontrollinstanz zu konsultieren. Für öffentliche Stellen des Bundes stellt dies der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit dar, öffentliche Landeseinrichtungen können sich dem Landesdatenschutzbeauftragten des jeweiligen Bundeslandes anvertrauen.

Der Betriebsrat besitzt in bestimmten Fällen Unterrichtungs- und Beratungsrechte aus § 90 BetrVG. Nach § 90 Abs. 1 Nr. 2 BetrVG ist der Arbeitgeber verpflichtet, den Betriebsrat über die Planung technischer Anlagen zu informieren. Unter den Begriff der technischen Anlage fallen sämtliche Geräte, Maschinen und Hilfsmittel, welche unmittelbar oder mittelbar dem Arbeitsablauf dienen, diesen ermöglichen oder erleichtern.[852] Das Gesprächsmanagement-System dient zwar in erster Linie der Gesprächsoptimierung, muss aber – damit dieses Ziel überhaupt erreicht werden kann – dem Callcenter-Agenten erleichterten und schnelleren Zugang zu relevanten Informationen bieten; insoweit verkörpert das System eine technische Anlage im Sinne der Vorschrift. Dieselbe Unterrichtungspflicht gilt gemäß § 90 Abs. 1 Nr. 3 BetrVG in Bezug auf Arbeitsabläufe sowie Arbeitsverfahren; dazu zählt zum Beispiel die Arbeit an Geräten zur automatisierten Datenerfassung mit einem Bildschirm. Das Spracherkennungsmodul realisiert eine automatisierte Datenerhebung und das Frontend-System besteht unter anderem aus einem Bildschirm. Die Information hat rechtzeitig und unter Vorlage sämtlicher relevanten Unterlagen zu erfol-

[849] So auch *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 646.
[850] *BVerwG* v. 8.11.1989, CR 1990, 783; *Gräfl*, in: Richardi/Dörner/Weber (Hrsg.), Kommentar zum Personalvertretungsrecht, 3. Aufl. 2008, § 68 Rn. 71; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 845; *Vogelgesang*, CR 1992, 405 (409).
[851] *Auernhammer*, DuD 1992, 621; *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 15 Rn. 645.
[852] BeckOK/*Werner*, BetrVG, Ed. 20, Stand: 1. Juni 2011, § 90 Rn. 3.

gen.[853] Beide Mitwirkungsrechte weisen zwar keine direkten Bezüge zum Datenschutz auf, dennoch können sie im Zusammenhang mit der geplanten Einführung des Gesprächsmanagement-Systems im Callcenter zu beachten sein. § 90 Abs. 2 BetrVG enthält die Vorgabe, rechtzeitig mit dem Betriebsrat über die intendierten Maßnahmen und potenziellen Auswirkungen zu beraten, sodass dieser Bedenken sowie Vorschläge vorbringen und damit auf die Planung des Arbeitgebers einwirken kann.

Das Kollektivorgan besitzt überdies das Recht, mit dem Arbeitgeber über bestimmte Maßnahmen zu verhandeln. Als bedeutendste Instrumente sind die Mitbestimmungsregelungen aus § 87 Abs. 1 Nr. 6 BetrVG oder § 75 Abs. 3 Nr. 17 BPersVG und deren landesrechtliche Entsprechungen zu benennen.[854]

7.2 Externe Kontrollorgane

Generell sieht der Gesetzgeber für Tätigkeiten, von denen potenziell Gefahren für den Einzelnen oder die Allgemeinheit ausgehen, staatliche Kontrollen vor – so auch für den Bereich des Datenschutzes.[855] Die externe Kontrolle der Ausführung des Bundesdatenschutzgesetzes und – eingeschränkt – weiterer datenschutzrechtlicher Vorschriften bei nichtöffentlichen Stellen obliegt gemäß § 38 BDSG den Aufsichtsbehörden.[856] Für öffentliche Stellen des Bundes ist gemäß § 24 Abs. 1 BDSG der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständige Kontrollinstanz. In allen Bundesländern existieren Landesdatenschutzbeauftragte, welche die Einhaltung des Datenschutzes in den Stellen der Landesverwaltung überwachen.

Gemäß § 38 Abs. 6 BDSG bestimmen die Landesregierungen oder die von ihnen dazu ermächtigten Stellen die Aufsichtsbehörden. Da die Kontrollstellen hinsichtlich des Datenschutzes für den nichtöffentlichen Bereich in Deutschland generell der staatlichen Aufsicht unterlagen, wurde durch die EU-Kommission ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Der *EuGH* entschied, dass die Bundesrepublik Deutschland gegen Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG verstößt, da die Aufsichtsbehörden staatlicher Aufsicht un-

[853] *Annuß*, in: Richardi (Hrsg.), Kommentar zum Betriebsverfassungsgesetz, 12. Aufl. 2010, § 90 Rn. 19 ff.
[854] *Däubler*, Gläserne Belegschaften?, 5. Aufl. 2010, § 13 Rn. 628; dazu ausführlich Kapitel 4.1.1.2.1 „Erlaubnis aus einer Betriebs- oder Dienstvereinbarung“.
[855] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 1.
[856] *Auernhammer*, DuD 1992, 621; *Herb*, ZUM 2004, 530 (531).

terstellt sind und damit das Erfordernis, ihre Aufgabe „in völliger Unabhängigkeit" wahrzunehmen, falsch umgesetzt wird.[857] Als Reaktion auf das *EuGH*-Urteil wurde der Großteil der Aufsichtsbehörden in den Ländern zwischenzeitlich in die Dienststelle des jeweiligen Landesdatenschutzbeauftragten integriert. Dadurch soll der europäischen Vorgabe entsprochen werden.

Die aktuelle Fassung des Bundesdatenschutzgesetzes differenziert einerseits nach der Kontrolle des nichtöffentlichen Bereichs durch Aufsichtsbehörden und andererseits nach der Aufsicht über öffentliche Stellen des Bundes durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Zwar wurde bereits, wie oben dargestellt, eine Vielzahl der Aufsichtsbehörden in die Dienststelle des jeweiligen Landesdatenschutzbeauftragten mit aufgenommen. Dennoch gebietet sich die separate Darstellung der beiden Kontrollstellen, da zumindest Bayern bei der Umsetzung des *EuGH*-Urteils einen Sonderweg beschreitet: Hier wurde eine eigenständige und damit unabhängige Behörde, namentlich das Landesamt für Datenschutzaufsicht, geschaffen. Abgesehen davon bleiben auch bei einer organisatorischen Zusammenführung der Aufsichtsbehörden mit dem jeweiligen Landesdatenschutzbeauftragten die Aufgaben und Befugnisse der Kontrolle der öffentlichen und die der Kontrolle der nichtöffentlichen Stellen weiterhin getrennt und beruhen auf unterschiedlichen Rechtsgrundlagen.

7.2.1 Aufsichtsbehörden

Die Stellung, Aufgaben und Kompetenzen der Aufsichtsbehörden sind in § 38 BDSG geregelt.[858] Wie die Kontrolle konkret ausgestaltet sein soll, ist durch § 38 BDSG nicht ausdrücklich vorgegeben. Insofern steht es der Aufsichtsbehörde nach pflichtgemäßem Ermessen grundsätzlich frei, zu entscheiden, wann, auf welche Weise, in welchem Umfang und in welchen zeitlichen Abständen verantwortliche Stellen – das heißt auch Callcenter – überprüft werden. Häufig wird die Aufsichtsbehörde aufgrund einer Beschwerde von Betroffenen, im Zusammenhang mit Callcentern etwa von Kunden, tätig.[859]

[857] *EuGH* v. 9.3.2010, RDV 2010, 121 ff. = MMR 2010, 352 ff. m. Anm. *Petri/Tinnefeld* = EuZW 2010, 296 ff. m. Anm. *Roßnagel*; s. zu dieser Diskussion auch *Petri/Tinnefeld*, MMR 2010, 157 ff.; *Bull*, EuZW 2010, 488 ff.; *Schild*, DuD 2010, 549 ff.; zum „Berliner Modell" *Garstka*, DuD 2000, 289 ff.
[858] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 1.
[859] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 10.

Nachfolgend werden die Aufgaben und Befugnisse der Aufsichtsbehörden, deren Kontrolle Callcenter-Betriebe im nichtöffentlichen Bereich unterliegen, kurz dargestellt.

7.2.1.1 Aufgaben

Die jeweils zuständige Aufsichtsbehörde unterstützt und berät betriebliche und behördliche Datenschutzbeauftragte auf deren Wunsch hin gemäß §§ 4g Abs. 1 Satz 2 und 4d Abs. 6 Satz 3 BDSG sowie die datenverarbeitende Stelle selbst.[860] Die Fremdkontrolle durch die Aufsichtsbehörde und die organisationsinterne Kontrolle durch den Datenschutzbeauftragten ergänzen sich somit. Die Aufsichtsbehörden arbeiten nach dem sogenannten Kooperationsprinzip. Dieses Prinzip hat zum Ziel, die Sicherstellung bestimmter Allgemeininteressen, wie die des Datenschutzes, nicht als alleinige Aufgabe des Staates zu sehen, sondern vielmehr Wirtschaftsakteure im Rahmen einer Selbstüberwachung in den Prozess mit einzubeziehen.[861] Aufgrund der ausgeprägten Problemkenntnis der Aufsichtsbehörde kann sie typische Datenschutzprobleme leicht identifizieren und durch präventives Einschreiten auf die Einhaltung des Datenschutzes in der Organisation hinwirken.[862]

Eine bedeutende Aufgabe von Aufsichtsbehörden besteht darüber hinaus in der Erstellung von Tätigkeitsberichten, die in der Regel als Bundestags- oder Landtagsdrucksachen veröffentlicht werden. Sie dienen der Offenlegung von Schwierigkeiten der Exekutive bei der Umsetzung der Datenschutzvorschriften sowie dazu, die Öffentlichkeit in Bezug auf die Wichtigkeit des Datenschutzes zu sensibilisieren.[863] Die Veröffentlichung dieser Berichte erfolgt nach § 38 Abs. 1 Satz 7 BDSG regelmäßig im Turnus von spätestens zwei Jahren.

Zum Schutz seiner Rechte und Freiheiten beim Umgang mit seinen personenbezogenen Daten kann sich jedermann nach § 38 Abs. 1 Satz 8 unter Verweis auf § 21 BDSG an die zuständige Aufsichtsbehörde wenden.[864] Die von Betroffenen an die Aufsichtsbehörde herangetragenen Eingaben müssen von ihr im Rahmen ihres Aufgaben- und Kompetenzbereichs bearbeitet werden.[865] Nicht in ihren Verantwort-

[860] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 13.
[861] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 1 ff.
[862] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 13.
[863] *Petri/Tinnefeld*, MMR 2010, 157 (158).
[864] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 22.
[865] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 58 ff.

lichkeitsbereich fallende Beschwerden hat sie an die zuständigen Stellen weiterzuleiten.[866]

Überdies fungiert die Aufsichtsbehörde als Registrierstelle für die nach § 4d BDSG meldepflichtigen automatisierten Datenverarbeitungen. Der Grund liegt darin, dass die Verarbeitungen mit ihren Zweckbestimmungen transparent gemacht werden sollen, damit eine datenschutzrechtliche Zulässigkeitsprüfung vollzogen werden kann. Die Offenlegung der Prozesse dient sowohl den Bürgern, die sich gemäß § 38 Abs. 2 Satz 2 BDSG über diesbezügliche Verarbeitungen erkundigen können, als auch der Aufsichtsbehörde selbst, für die die Registereintragungen im Wesentlichen den Ausgangspunkt ihrer Kontrolltätigkeit darstellen. Von anlasslosen oder -bezogenen Überprüfungen können jedoch ebenso nicht meldepflichtige Stellen betroffen sein, da Kontrollen nicht von der Registereintragung abhängen.[867] Falls ein organisationsinterner Datenschutzbeauftragter im Callcenter existiert, ist eine diesbezügliche Meldung an die Aufsichtsbehörde gemäß § 4d Abs. 2 BDSG grundsätzlich nicht erforderlich, da der Datenschutzbeauftragte nach § 4g Abs. 2 BDSG ein solches Verzeichnis selbst zu führen hat. § 4d Abs. 3 BDSG enthält eine weitere Ausnahme von der Meldepflicht.

7.2.1.2 Befugnisse

Im Rahmen ihres Aufgabengebiets verfügt die Aufsichtsbehörde über spezielle Befugnisse, damit sie ihre Tätigkeit adäquat ausführen kann.

Der Aufsichtsbehörde steht gemäß § 38 Abs. 3 BDSG ein umfangreiches Auskunftsrecht zu. Nach diesem haben die kontrollierten Callcenter und deren Leitungspersonen alle zur Aufgabenerfüllung der Behörde notwendigen Auskünfte unverzüglich zu erteilen. Die gegenüber der Aufsichtsbehörde getätigten Angaben müssen vollständig und wahrheitsgemäß sein und können sich auch auf die Aufdeckung von Datenquellen beziehen. Zur Kostenerstattung ist die Aufsichtsbehörde nicht verpflichtet.[868] Ein Auskunftsverweigerungsrecht besteht allerdings in den Fällen, in denen sich der Auskunftspflichtige selbst oder einen Angehörigen im Sinne des § 383 Abs. 1 Nr. 1 - 3 ZPO der Gefahr einer Strafverfolgung oder Belangung aufgrund einer Ordnungswidrigkeit aussetzen würde. Kommt das der Überprüfung unterliegende Callcenter seiner Auskunftspflicht nicht sachgerecht nach, droht ein Bußgeldverfahren gemäß § 43 Abs. 1 Nr. 10 BDSG. Überdies ist die

[866] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 38 Rn. 2.
[867] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 46.
[868] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 25 ff.

Durchsetzung der Auskunftsverpflichtung mit Mitteln des Verwaltungszwangs, etwa Zwangsgeld oder Ersatzvornahme, möglich.[869]

Darüber hinaus besitzt die Aufsichtsbehörde das Recht, Prüfbesuche vor Ort durchzuführen. Eine vorherige Ankündigung ist hierfür nicht erforderlich. Die Grundstücke und Geschäftsräume dürfen zu den branchenüblichen Geschäftszeiten betreten werden.[870] Die Befugnis zur Ausführung der Prüfbesuche umfasst ferner Besichtigungsrechte, die sich gemäß § 38 Abs. 4 Satz 2 BDSG auf die Geschäftsunterlagen, das Register nach § 4g Abs. 2 Satz 1 BDSG, die gespeicherten personenbezogenen Daten sowie die Datenverarbeitungsprogramme erstrecken. Dazu dürfen auch Notizen und Kopien der Unterlagen angefertigt werden. Die kontrollierte Stelle ist zur Duldung der Maßnahme verpflichtet. Daraus können unter Umständen bestimmte Mitwirkungspflichten, wie das Zugänglichmachen von Räumen und Heraussuchen von Unterlagen, resultieren. Kooperiert das Callcenter nicht oder nicht angemessen mit der Behörde, kann sie ihre Rechte durch Mittel des Verwaltungszwangs durchsetzen; außerdem droht ein Bußgeldverfahren nach § 43 Abs. 1 Nr. 10 BDSG.[871]

Gemäß § 38 Abs. 5 Satz 1 BDSG besitzt die Aufsichtsbehörde die Befugnis, die Beseitigung festgestellter Verstöße beim Umgang mit personenbezogenen Daten sowie die Beseitigung technischer oder organisatorischer Mängel anzuordnen.[872] Dies betrifft beispielsweise die vom Callcenter zu treffenden Maßnahmen nach § 9 BDSG nebst Anlage. Wird im Rahmen des Kontrollverfahrens etwa eine unzureichende Zutrittssicherung zu den Datenverarbeitungsanlagen festgestellt, kann die Aufsichtsbehörde die Implementierung einer sicheren Zutrittskontrollmaßnahme anordnen.[873] Vor einer Anordnung muss die datenverarbeitende Stelle nach Maßgabe des jeweiligen Landesverwaltungsverfahrensgesetzes angehört werden.[874] Die Zuwiderhandlung einer Anordnung nach § 43 Abs. 1 Nr. 11 BDSG ist bußgeldbewehrt.

Liegen nach § 38 Abs. 5 Satz 2 BDSG schwerwiegende Verstöße oder Mängel der genannten Art vor – hauptsächlich dann, wenn damit eine besondere Gefährdung des Persönlichkeitsrechts der Betroffenen einhergeht –, kann die Aufsichtsbehörde die Erhebung, Verarbeitung oder Nutzung von Daten oder die Anwendung der Datenverarbeitungsverfahren verbieten. Voraussetzung dafür ist allerdings, dass die

[869] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 78.
[870] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 72 ff.
[871] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 30 ff.
[872] *Kühling/Bohnen*, JZ 2010, 600 (606), die die Befugniserweiterung der Aufsichtsbehörden begrüßen.
[873] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 89.
[874] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 38.

erkannten und beanstandeten Mängel trotz Verhängung eines Zwangsgeldes nicht in angemessener Frist beseitigt wurden. Was die Bestimmung der Länge des Zeitraums anbelangt, können keine konkreten Vorgaben gemacht werden. Sie ist einzelfallabhängig und unter Abwägung der potenziellen Gefahren für das Persönlichkeitsrecht der Betroffenen einerseits und der aus der Maßnahme für das Callcenter resultierenden Konsequenzen andererseits zu vollziehen. Bei erheblichen Verstößen kann eine Frist von nur wenigen Tagen durchaus legitim sein.[875] Der Aufsichtsbehörde stehen bei festgestellten Datenschutzverstößen gemäß § 38 Abs. 1 Satz 6 BDSG umfassende Befugnisse zu, die ihr erlauben, die Betroffenen darüber zu informieren, die Verstöße zur Verfolgung oder Ahndung bei den zuständigen Stellen zu melden sowie bei Vorliegen gravierender Übertretungen gewerberechtliche Maßnahmen über die Gewerbeaufsichtsbehörde einzuleiten.

Die Aufsichtsbehörde verfügt sogar über die Befugnis, den organisationsinternen Datenschutzbeauftragten abzuberufen. Mit diesem Recht sollte jedoch generell sehr vorsichtig umgegangen werden: So kann die fehlende Fachkunde etwa durch entsprechende Schulungsmaßnahmen behoben werden. Es ist durchaus möglich, dass der Arbeitgeber seine Unterstützungspflicht nach § 4f Abs. 5 BDSG nicht adäquat ausgeübt hat, indem er dem Datenschutzbeauftragten nicht die erforderliche Zeit oder die notwendigen finanziellen Mittel bereitgestellt hat; in solchen Fällen trifft den Datenschutzbeauftragten keine Schuld.[876] Das Verfahren der Abberufung besteht in einem Verwaltungsakt, der sich gegen die verantwortliche Stelle selbst richtet. Dennoch können sowohl die Stelle als auch der Datenschutzbeauftragte Widerspruch einlegen. Erlangt der Verwaltungsakt Bestandskraft, endet nicht automatisch die Bestellung des Datenschutzbeauftragten. Vielmehr hat die Leitung der Organisation nun den Widerruf der Bestellung auszusprechen.[877]

Aus Gründen der Vollständigkeit wird angeführt, dass neben den Kontrollen, die durch das Bundesdatenschutzgesetz vorgesehen sind, nach § 38 Abs. 7 BDSG auch solche nach der Gewerbeordnung stattfinden können. Derselbe datenschutzrechtliche Sachverhalt wird in diesem Fall von zwei verschiedenen Aufsichtsbehörden nebeneinander beurteilt.[878] Bei Vorliegen schwerwiegender Verstöße ist es gemäß § 35 GewO möglich, dass die weitere gewerbliche Tätigkeit eingeschränkt oder untersagt wird.[879] Übermittlungen personenbezogener Daten zwischen den Aufsichtsbehörden untereinander zu Aufsichtszwecken sind zulässig. Damit wird die Wahr-

[875] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 39.
[876] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 40 f.
[877] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 38 Rn. 28.
[878] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 38 Rn. 49.
[879] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 38 Rn. 36.

scheinlichkeit redundanter Arbeitsschritte verschiedener Aufsichtsbehörden minimiert und eine breite Informationsgrundlage geschaffen.

7.2.2 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit sowie Landesbeauftragte für den Datenschutz

Für Callcenter, die von öffentlichen Stellen des Bundes oder eines Landes betrieben werden, stellen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit oder der jeweilige Landesbeauftragte für den Datenschutz die zuständigen Organe zur Fremdkontrolle dar.

Das Bundesdatenschutzgesetz enthält mit den §§ 22 - 26 BDSG einen eigenen Unterabschnitt, dessen Regelungen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit betreffen. Die einzelnen Landesdatenschutzgesetze beinhalten jeweils entsprechende Vorschriften zu den Landesdatenschutzbeauftragten. Das Aufgabenfeld, die Befugnisse sowie die Rechtsstellung der Landesbeauftragten für den Datenschutz sind vergleichbar mit denen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.[880] Auf die eigenständige Darstellung wird aufgrund der Vergleichbarkeit verzichtet.[881]

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bekleidet gemäß § 22 Abs. 4 Satz 1 BDSG ein öffentlich-rechtliches Amt spezieller Art: Er ist weder Beamter noch Angestellter und nimmt daher eine rechtliche Sonderposition ein. In seiner Amtsausübung handelt er nach § 22 Abs. 4 Satz 2 BDSG unabhängig und nur dem Gesetz unterworfen. Seine Unabhängigkeit ist mit der eines Richters zu vergleichen.[882] Niemand kann ihm eine Weisung erteilen, die im Zusammenhang mit der Ausübung seines Amts steht. Diese Unabhängigkeit reicht jedoch nicht soweit, dass seine materielle Bindung ans Gesetz überwunden würde.[883]

Gemäß § 22 Abs. 4 Satz 3 BDSG untersteht der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit einer Rechtsaufsicht, die durch die Bundesregierung ausgeübt wird. Diese Aufsicht dient als Korrektiv für Maßnahmen und Ent-

[880] *Garstka/Gill*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.2 Rn. 11; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 22 Rn. 14.
[881] Eine rechtsvergleichende Übersicht über zentrale Gesichtspunkte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und der Datenschutzbeauftragten der einzelnen Länder liefert *Niese*, DuD 1994, 635 ff.
[882] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 22 Rn. 8 f.
[883] *Bizer*, DuD 2000, 673.

scheidungen, die unmittelbare Rechtswirkung entfalten und rechtswidrig sind.[884] Verweigert der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beispielsweise die Annahme einer Eingabe nach § 21 BDSG, stellt dies einen diesbezüglichen Verstoß dar.[885]

Eingerichtet ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit seiner Dienststelle gemäß § 22 Abs. 5 BDSG beim Bundesinnenministerium; es handelt sich dabei um eine Angliederung einer Behörde bei einer anderen.[886] Das Bundesinnenministerium übt die Dienstaufsicht über den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit aus.

Seine zentralen Aufgaben und Befugnisse sind nachfolgend kurz dargelegt.

7.2.2.1 Aufgaben

Die Hauptaufgabe des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit besteht gemäß § 24 Abs. 1 Satz 1 BDSG in der Kontrolle der Einhaltung der Datenschutzvorschriften bei öffentlichen Stellen des Bundes. Aus § 11 Abs. 4 Nr. 1b BDSG erstreckt sich seine Kontrollfunktion darüber hinaus auf nichtöffentliche Einrichtungen, die Daten im Auftrag für öffentliche Stellen des Bundes verarbeiten.[887] Er kann Callcenter, die genannte Voraussetzungen erfüllen, stichprobenweise oder in regelmäßigen Abständen – beides auch ohne vorhergehende Ankündigung – überprüfen.[888]

Das Ergebnis einer abgeschlossenen Kontrolle ist der öffentlichen Organisation nach § 24 Abs. 5 BDSG mitzuteilen. Mit diesem Bericht können Vorschläge zum Abstellen der festgestellten Mängel und zur Verbesserung des Datenschutzes einhergehen.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat dem Bundestag gemäß § 26 Abs. 1 Satz 1 BDSG im regelmäßigen Turnus von zwei Jahren Bericht zu erstatten. In diesem legt er Rechenschaft über seine Tätigkeit ab und präsentiert wichtige Ergebnisse aus seiner Kontrollfunktion. Darüber hinaus zählt gemäß § 26 Abs. 1 Satz 2 BDSG zu seinen Aufgaben, den Bundestag sowie die Öf-

[884] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 22 Rn. 10.
[885] Mit weiteren Beispielen *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 22 Rn. 11.
[886] *Heil*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.1 Rn. 34.
[887] Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 24 Rn. 5.
[888] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 24 Rn. 4.

fentlichkeit über wesentliche Entwicklungen des Datenschutzes aufzuklären. Zu solchen Entwicklungen gehören insbesondere Technologien und deren Anwendung, die Praxis im Umgang mit personenbezogenen Daten sowie potenzielle Auswirkungen und Risiken für Betroffene.[889]

Durch § 26 Abs. 3 BDSG ist die Möglichkeit der Beratung der Bundesregierung und öffentlicher Stellen des Bundes in datenschutzrechtlichen Fragestellungen vorgesehen. Weitergehend kann ihnen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Empfehlungen aussprechen, die auf die Verbesserung des Datenschutzes abzielen. Die Ratgeberfunktion beschränkt sich jedoch nicht nur auf die genannten Adressaten, sondern erstreckt sich grundsätzlich auf sämtliche anderen Stellen, besonders auf Betroffene. Ziel ist die Verwirklichung einer proaktiven Beratung, die der Entstehung von Konflikten entgegenwirkt.[890]

Überdies fällt die Erstellung von Gutachten und Berichten gemäß § 26 Abs. 2 Satz 1 BDSG in den Aufgabenbereich des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Er hat diese Gutachten und Berichte auf Anforderung der Bundesregierung oder des Bundestages anzufertigen.

Bestehen Hinweise auf datenschutzrelevante Vorgänge und Angelegenheiten bei öffentlichen Organisationen, sieht § 26 Abs. 2 Satz 2 BDSG deren Untersuchung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vor. Eine diesbezügliche Begutachtung kommt insbesondere aufgrund eines Ersuchens des Bundestages, der Bundesregierung, des Innenausschusses oder des Petitionsausschusses in Betracht. Falls derartige Vorgänge öffentlich bekannt werden, muss der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit von Amts wegen tätig werden.[891]

In § 26 Abs. 4 BDSG kommt das Kooperationsprinzip zum Ausdruck: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit fördert die Zusammenarbeit mit den Datenschutzbeauftragten der Länder. Ebenso soll er das Zusammenspiel mit den Aufsichtsbehörden nach § 38 BDSG sowie mit den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union intensivieren.

Gemäß § 21 Satz 1 BDSG verfügt jeder über das Recht, sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden, wenn er befürchtet, dass seine Rechte durch den Datenumgang bei öffentlichen Stellen des

[889] Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 26 Rn. 3 ff.
[890] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 26 Rn. 7 f.
[891] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 26 Rn. 5.

Bundes verletzt wurden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist dann verpflichtet, die Anrufung entgegenzunehmen und sie zu bearbeiten. Überdies besteht eine Aufklärungspflicht gegenüber der ihn anrufenden Person.[892]

7.2.2.2 Befugnisse

Dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit steht aus § 23 Abs. 4 BDSG ein Zeugnisverweigerungsrecht in Bezug auf die ihm in seiner amtlichen Funktion anvertrauten Informationen zu. Der Petent muss darauf vertrauen können, sich – ohne nachteilige Konsequenzen befürchten zu müssen – an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden zu können.[893] Überdies unterliegt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit der Verschwiegenheitspflicht gemäß § 23 Abs. 5 BDSG, die ihn grundsätzlich daran bindet, über sämtliche ihm amtlich zur Kenntnis gelangte Angelegenheiten Verschwiegenheit zu bewahren.

Dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Mitarbeitern seiner Dienststelle stehen aus § 24 Abs. 4 BDSG im Rahmen der Kontrollen prinzipiell die Befugnisse zu, insbesondere sämtliche relevanten Unterlagen einzusehen und jederzeit die Diensträume der kontrollierten Organisation zu betreten. Die kontrollierte Stelle hat sie bei ihrer Tätigkeit zu unterstützen.[894]

Beanstandungen gemäß § 25 BDSG sind die schärfsten Sanktionsmittel, die dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Verfügung stehen. Sie können sich auf einen Verstoß gegen konkrete Datenschutzbestimmungen beziehen, jedoch auch auf sonstige, etwa organisatorische, Mängel beim Umgang mit personenbezogenen Daten.[895] Eine Beanstandung sollte erst dann in Betracht gezogen werden, wenn die nach § 24 BDSG vorgesehenen Maßnahmen der Beratung und Empfehlung nicht ausreichen.[896] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit fordert anhand einer Beanstandung, welche die Darlegung des Verstoßes enthält, die datenverarbeitende Stelle unter Frist-

[892] *Grittmann*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 21 Rn. 10.
[893] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 23 Rn. 4; Simitis/*Dammann*, BDSG, 7. Aufl. 2011, § 23 Rn. 14 ff.
[894] *D/K/W/W*, BDSG, 3. Aufl. 2010, § 24 Rn. 10 ff.
[895] *Heil*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.1 Rn. 56; *Giesen*, RDV 1998, 15 (18).
[896] *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Ergänzungslieferung 2010, BDSG, § 25 Rn. 1.

setzung auf, eine Stellungnahme abzugeben.[897] In der Stellungnahme der kontrollierten Stelle sind gemäß § 25 Abs. 3 Satz 1 BDSG die Maßnahmen mit aufzunehmen, die zur Mängelbeseitigung ergriffen wurden.

Betrachtet man die insgesamt relativ schwachen Durchsetzungsmöglichkeiten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie die der Landesdatenschutzbeauftragten, gelangt man zu dem Schluss, dass ihnen eher die Funktion eines Beraters als die eines Kontrolleurs obliegt.[898] Sie können zwar Verstöße beanstanden, besitzen jedoch keine Befugnis zur Anordnung, die Übertretung und deren Konsequenzen zu beseitigen.[899]

[897] *Heil*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.1 Rn. 56; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 25 Rn. 5.
[898] *Mester*, Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, 2008, 204.
[899] *Bull*, EuZW 2010, 488 (493); *Garstka*, Informationelle Selbstbestimmung und Datenschutz, 62 (abrufbar unter: www.bpb.de/files/YRPN3Y.pdf).

8 Technische, organisatorische und rechtliche Gestaltungsvorschläge

Die vorstehenden Kapitel stellen den rechtlichen Rahmen dar, den es bei der Einführung und beim Betrieb des Gesprächsmanagement-Systems einzuhalten gilt. Das Datenschutzrecht bietet durch seine grundlegenden Anforderungen ein Schutzkonzept, das gewährleistet, dass Betroffene ihr informationelles Selbstbestimmungsrecht wahrnehmen können.

Im Folgenden werden anhand wesentlicher Datenschutzprinzipien und darüber hinaus weiterer bedeutender datenschutzrechtlicher Forderungen konkrete technische und organisatorische Vorschläge für die Gestaltung des Systems abgeleitet, um das ideale Maß an Datenschutz zu verwirklichen. Dieses optimale zu gewährleistende Datenschutzniveau stellt keine feste Größe dar, sondern muss einzelfallabhängig, unter Berücksichtigung des Gesamtkontexts des Systemeinsatzes bestimmt werden. Wesentliche Einflussgrößen sind das Einsatzgebiet, in dem das System zur Anwendung gelangt, und die Intensität der (potenziellen) Datenverarbeitungsprozesse, insbesondere im Rahmen des Data-Minings. Ziel soll nicht sein, allein das maximale Maß an Datenschutz zu erreichen. Der Aufwand (beispielsweise Kosten, Ressourcenverbrauch) muss in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

Technische Entwicklungen[900] vollziehen sich nicht im „luftleeren Raum“, sondern weisen eine Vielzahl von Berührungspunkten mit hauptsächlich sozialen, ethischen und rechtlichen Fragestellungen auf. Ein solches Geflecht führt zwangsläufig zu Interdependenzen zwischen Technik und den mit ihr verknüpften Feldern – so auch zwischen Technik und Recht.

Allgemein betrachtet bergen technische Neuerungen sowohl potenzielle Chancen als auch potenzielle Risiken. Die Ungewissheit über zukünftige neue Möglichkeiten und Gefahren durch die Nutzung der jeweiligen Technik ist in ihrer Entwicklungsphase besonders groß: In diesem Stadium steht meist ausschließlich ihre Funktionsfähigkeit im Fokus. Mögliche Chancen und Risiken der Technik werden selten intensiv reflektiert; eine umfassende Suche nach alternativen Lösungen und Gestaltungsvarianten findet oftmals nicht statt.[901] Der Entscheidungsprozess in Bezug auf die Entwicklung einer bestimmten Technik ist jedoch nur dann als verantwortungs-

[900] Die nachfolgenden Ausführungen zur rechtsadäquaten Technikgestaltung hat der Verfasser im Rahmen seiner Mitarbeit im Forschungsprojekt „Einsatz der RFID-Technologie als Innovation für eine ressourcenoptimierte und datenschutzgerechte Kreislauf- und Entsorgungswirtschaft“ erarbeitet. Sie wurden zwischenzeitlich in *Urban et al.*, RFID zur Weiterentwicklung der Kreislaufwirtschaft: datenschutzgerecht Ressourcen schonen, 2011, 31 ff., veröffentlicht.

[901] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 55.

voll zu bezeichnen, wenn im Vorfeld des Technikeinsatzes denkbare Chancen und Risiken erkannt, abgeschätzt und bewertet werden.[902]

Neuartige technische Anwendungen können neue Verhaltensweisen ermöglichen und hervorrufen, die unter Umständen Anpassungen rechtlicher Regelungen erfordern.[903] Neben demokratischen Willensbildungsprozessen nehmen technische Entwicklungen erheblichen Einfluss auf die Rechtsfortbildung.[904] Denkbar ist allerdings ferner, dass der bereits bestehende Rechtsrahmen durch die Anwendung der Technik verwirklicht oder sogar umgangen wird. Rechtliche Rahmensetzungen, die entweder aus Anreizen oder Restriktionen bestehen können, haben ihrerseits Auswirkungen auf die Planung sowie Ausgestaltung technischer Anlagen und Systeme. Letztendlich bestimmen sie mit über die Entstehung oder Verhinderung der jeweiligen Technik.[905] Allerdings kann auch die Technik selbst dazu beitragen, dass rechtliche Ziele realisiert und Schutzzwecke erfüllt werden. So ist überall dort, wo technische Vorkehrungen vor Missbrauch schützen, die Rechtsdurchsetzung durch Polizei und Gerichte gar nicht mehr notwendig. Vereinfacht ausgedrückt bedeutet dies: Alles, was technisch nicht möglich ist oder durch Technik verhindert wird, muss nicht verboten und schließlich auch nicht überwacht werden. Es lässt sich leicht gegen Rechtsnormen verstoßen, technische Begrenzungen können demgegenüber nicht ohne Weiteres umgangen werden. Die ideale Ausgestaltung eines technischen Systems enthält einen Systemschutz, der gewährleistet, dass die Durchsetzung rechtlicher Anforderungen quasi von selbst – durch ihren normalen Gebrauch – erfolgt.[906] Insofern kann die rechtsadäquate Technikgestaltung zur Minimierung des Kontrollaufwands sowie der daraus resultierenden Sanktionsverfahren führen.[907]

Grundsätzlich bestehen zwei Möglichkeiten, das Spannungsverhältnis zwischen Technik und Recht zu lösen: Erstens lässt sich die zu entwickelnde Technik nach Maßgabe des geltenden Rechts gestalten und zweitens kommt eine technikadäquate Anpassung der Rechtsordnung in Betracht.[908]

Wird abgewartet, bis schließlich negative Folgen aus der Verwendung einer Technik resultieren, ist oftmals „das Kind bereits in den Brunnen gefallen“, weil Korrek-

[902] *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993, 105.
[903] *Hornung*, Die digitale Identität, 2005, 87.
[904] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 55.
[905] *Hornung*, Die digitale Identität, 2005, 87.
[906] *Roßnagel*, in: Klumpp/Kubicek/Roßnagel (Hrsg.), next generation information society?, 2003, 428 f.
[907] *Roßnagel*, in: Klumpp/Kubicek/Roßnagel (Hrsg.), next generation information society?, 2003, 428 f.; *ders.*, DuD 1999, 253 (255).
[908] *Roßnagel et al.*, Digitalisierung der Grundrechte?, 1990, 5 f.

turen am Recht zu spät kämen.[909] Eine Vielzahl technischer Innovationen machte somit die ständige Anpassung des Rechts[910] notwendig. Dies impliziert, dass eine abwartende Haltung zu einem chronischen Vollzugsdefizit der jeweils geltenden Rechtsnormen führt.[911] Als Problem erweist sich in diesem Zusammenhang ferner, dass sich die Verwendung einer einmal etablierten Technik praktisch kaum mehr rückgängig machen lässt und sich daraus Sachzwänge ergeben.[912]

Soll vermieden werden, die Rechtsordnung ständig im Nachhinein korrigieren zu müssen, um auf unbeabsichtigte Auswirkungen der Technik zu reagieren, sind bereits in der Phase der Technikentwicklung denkbare Folgen für die Rechte der Gesellschaftsmitglieder zu berücksichtigen. Nur so lässt sich die Technik derart gestalten, dass sie zur Gewährleistung und Entfaltung dieser Rechte beiträgt.[913] Der schlechteste Fall wäre derjenige, bei dem sich eine Technik bereits etabliert hat, die aber aufgrund ihrer negativen sozialen Auswirkungen verboten werden müsste.[914] Die zentrale Frage in diesem Kontext hat folglich zu lauten: Wie ist die Technik auszugestalten, damit sie zur Erhaltung der gesellschaftlichen Ordnung sowie zur Erreichung ihrer Entwicklungsziele führt?[915] Die Antwort darauf liegt im Vollzug einer aktiv angelegten rechtsadäquaten Technikgestaltung, die gegebenenfalls ergänzend durch eine Rechtsänderung ermöglicht wird.

Zusammenfassend lässt sich festhalten, dass generell die Integration datenschutzfreundlicher Mechanismen in Produkte, Dienste und Verfahren in zweierlei Hinsicht vorteilhaft ist: Zum einen sind Datenschutztechniken im Gegensatz zum Datenschutzrecht global wirksam. Zum anderen bietet das Technik produzierende Gewerbe signifikant schnellere Reaktionszeiten als der eher träge Gesetzgebungsapparat.[916]

Im Hinblick auf die Entwicklung des Gesprächsmanagement-Systems ist es also richtig, schon im Vorfeld seines Einsatzes zu prüfen, inwieweit rechtliche Vorgaben eingehalten werden müssen und können. Die technische Realisierung des Systems soll sich in erster Linie an diese Vorgaben halten. Erst dann, wenn die Möglichkeiten der rechtsadäquaten Gestaltung der Technik an ihre Grenzen stoßen, etwa da-

[909] *Roßnagel et al.*, Digitalisierung der Grundrechte?, 1990, 6.
[910] So machte etwa das Aufkommen neuer Vertriebsformen die nachträgliche Anpassung des Bürgerlichen Gesetzbuches (§§ 312, 312a - f BGB) erforderlich.
[911] *Hornung*, Die digitale Identität, 2005, 88.
[912] *Roßnagel et al.*, Digitalisierung der Grundrechte?, 1990, 5 f.; *Roßnagel*, KJ 1990, 267 (288).
[913] *Schwenke*, Individualisierung und Datenschutz, 2006, 8.
[914] *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 56.
[915] *Roßnagel et al.*, Digitalisierung der Grundrechte?, 1990, 259 f.
[916] *Roßnagel*, MMR 2003, 693 (694).

durch, dass sich eine technische Lösung nicht realisieren lässt, ist durch Fortentwicklung des Rechts dafür Sorge zu tragen, dass ein größtmöglicher Schutz der Rechte der Gesellschaftsmitglieder gewährleistet ist.

8.1 Technische und organisatorische Ansätze zur Erhöhung des Datenschutzniveaus

Nachfolgend werden Gestaltungsvorschläge sowohl in Bezug auf die Technik als auch im Hinblick auf die Organisation von Callcentern dargestellt, die das Datenschutzniveau positiv beeinflussen, ohne das Funktionieren des Gesprächsmanagement-Systems zu verhindern.

8.1.1 Rechtmäßigkeit des Umgangs mit personenbezogenen Daten

Das Kriterium der Rechtmäßigkeit stellt die grundlegendste Anforderung an den Datenumgang dar. Dessen Legitimation kann sich gemäß § 4 Abs. 1 BDSG aus dem Datenschutzrecht, einer anderen Rechtsvorschrift oder einer Einwilligung des Betroffenen ergeben. Insbesondere die individuelle Einwilligung sichert in der Regel größtmögliche Selbstbestimmung im Hinblick auf den Datenumgang, soweit die Entscheidungsfreiheit beim Betroffenen liegt. Die individuelle Zustimmung kommt primär dann in Betracht, wenn keine (ausreichenden) gesetzlichen Erlaubnistatbestände existieren, die den Umgang mit den personenbezogenen Daten rechtfertigen.[917]

Idealerweise sollte die Einverständniserklärung im Rahmen eines Einwilligungsmanagements nach unterschiedlichen Verarbeitungserlaubnissen differenzieren. Konkret bedeutet dies, dass der Kunde beispielsweise die verschiedenen vorgesehenen Datenverarbeitungsprozesse sowie die dazugehörigen Zwecke einzeln zur Verarbeitung freigeben kann. So vermögen die Kunden individuell zuzustimmen, mit welcher konkreten Datenverarbeitung sie einverstanden sind und mit welcher nicht.[918]

Technisch kann ein solches Einwilligungsmanagement gegenüber Kunden dadurch realisiert werden, dass dem eigentlichen Gespräch mit einem Callcenter-Mitarbeiter entsprechende Bandansagen vorgeschaltet sind, auf welche die Kunden mittels

[917] Eine Ausweitung der Verarbeitungsbefugnisse mittels datenschutzrechtlicher Einwilligung kommt bei öffentlichen Callcenter-Betrieben nur in sehr engen Grenzen in Frage. S. dazu Kapitel 3.1.1.2 “Zulässigkeitsalternativen im öffentlichen Bereich”.
[918] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 96 f.

Sprachdialogsystem (IVR) oder Tonwahlverfahren (DTMF) reagieren müssen. Dies stärkte das informationelle Selbstbestimmungsrecht der Kunden erheblich. Beim Erstkontakt zum Kunden kann hinsichtlich der Form der Einwilligung auf die Ausnahmevorschrift des § 4a Abs. 1 Satz 3 BDSG zurückgegriffen werden. Haben bereits Kontakte zu einem bestimmten Kunden bestanden, sollte die Einwilligung in der grundsätzlich geforderten Schriftform erfolgen.

Da gerade im Zusammenhang mit Callcenter-Dienstleistungen der Umgang mit personenbezogenen Daten von Kunden in der großen Masse oftmals unumgänglich ist, lässt sich eine Einwilligung in den Datenumgang für bestimmte Fälle kaum anders praktikabel organisieren, als durch die Verwendung von Formularverträgen. Die differenzierende Einwilligungserklärung kann in diesem Zusammenhang mittels Kästchen zum Ankreuzen umgesetzt werden. Für derartige Formulareinwilligungen sind die Voraussetzungen für Allgemeine Geschäftsbedingungen nach §§ 305 ff. BGB zu beachten.[919]

Die Legitimation des Datenumgangs mittels Einwilligung ist insoweit problematisch, als die Einwilligung individuell eingeholt werden muss und vom Einverständnis der Kunden abhängt. Falls Kunden die Einwilligung beschränken oder sogar verweigern, kann sich dies derart auswirken, dass die Performance des Gesprächsmanagement-Systems eingeschränkt oder überhaupt nicht genutzt werden kann. Generell gestaltet sich die Rechtfertigung für den Umgang mit personenbezogenen Daten einfacher, wenn sich der Datenumgang auf eine Vertragsbeziehung stützen lässt.[920]

8.1.2 Zweckbindung der erhobenen personenbezogenen Daten

Das Datenschutzrecht enthält das grundsätzliche Erfordernis, dass personenbezogene Daten nur zu vorab festgelegten Zwecken erhoben, verarbeitet oder genutzt werden dürfen. Dies dient insbesondere der Vorbeugung von Datenmissbrauch.[921] Die Kunden müssen ihr informationelles Selbstbestimmungsrecht wahrnehmen können, indem sie grundsätzlich darüber im Bilde sind, wer was, wann und unter welchen Umständen über sie weiß.[922]

[919] S. dazu Kapitel 3.1.1.1.3 „Erlaubnis aus einer Einwilligung“.
[920] S. dazu Kapitel 3.1.1.1.1.1 „Erlaubnis aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG“.
[921] So *BVerfG* v. 15.12.1983, NJW 1984, 419; *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 75.
[922] *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 75.

Die Kunden sind über die vorgesehenen Zwecke des Umgangs mit ihren personenbezogenen Daten in Kenntnis zu setzen. Der Umgang mit den Daten darf sich nach Festlegung des Zwecks nur innerhalb dieser Zweckbestimmung vollziehen. Eine geplante Zweckänderung erfordert im Regelfall eine entsprechende Erlaubnis. Dieser zentrale Grundsatz im Datenschutzrecht kommt in § 28 Abs. 1 Satz 2 und § 4 Abs. 3 Satz 1 Nr. 2 BDSG zum Ausdruck.[923]

Im Wirtschaftsleben fällt allgemein der Datenverarbeitung zur Erfüllung eigener Geschäftszwecke eine bedeutende Rolle zu, wenn gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG die personenbezogene Datenverarbeitung im Rahmen eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erfolgt; die personenbezogene Verarbeitung der Daten muss dabei zur Erfüllung des Schuldverhältnisses jedoch erforderlich sein.[924] Zu denken ist hierbei etwa an die notwendige Kenntnis der Adressdaten von Kunden, damit der Versand einer Ware auf dem Postweg möglich wird. So plausibel die Erforderlichkeit der Verwendung der personenbezogenen Daten zur Auftragsabwicklung in diesem Beispiel auch ist, so fraglich ist sie allerdings in Bezug darauf, ob Kundendaten im CRM-System gespeichert und nach nahezu sämtlichen denkbaren Kriterien ausgewertet werden dürfen.

Der Zweckbindungsgrundsatz hat gravierende Auswirkungen auf die Zulässigkeit des Umgangs mit den personenbezogenen Daten, die für die volle Funktionalität des Gesprächsmanagement-Systems notwendig sind. Sollen beispielsweise der Aufbau einer Kundendatenbank vorangetrieben und in diesem Zusammenhang anfallende Daten im Telefonat mit den im CRM-System bereits verfügbaren Daten verknüpft werden, muss der festzulegende Zweck der Datenverarbeitung genau diesen Vorgängen entsprechen. Weitergehende Absichten dürfen mit den Daten nicht verfolgt werden. Darüber hinaus ist der Kunde im Vorfeld über die vorgesehenen Datenverarbeitungsvorgänge sowie deren Zwecke aufzuklären.

Eine pauschale Grenzziehung, wann und mit welcher Zielsetzung welche Daten aufbereitet, ausgewertet, mit welchen weiteren Daten verknüpft und zu neuen verdichtet werden dürfen, lässt sich nicht vornehmen, sondern muss für jeden Einzelfall bestimmt werden. Reichen vordefinierte Abfragen im CRM-System zur Erfüllung des angestrebten Zwecks aus, so dürfen keine extensiven Data-Mining-Methoden zur Anwendung gelangen, deren Ergebnisse vollkommen ungewiss sind.

[923] *Bizer*, DuD 2007, 350 (352 f.); *Simitis*, NJW 1998, 2473 (2478), fordert schärfere Anforderungen an die Präzisierung von Zweckbestimmungen durch datenverarbeitende Stellen.
[924] *Bizer*, DuD 2007, 350 (352).

Zweckbegrenzung und -bindung sind primär durch eine entsprechende Systemgestaltung und den Systemdatenschutz sicherzustellen.[925] Die konkrete Umsetzung dieser grundlegenden Prinzipien des Datenschutzes erfolgt im Gesprächsmanagement-System anhand eines feingranularen Rechtemanagements. Das Rechtemanagement erlaubt es, von den standardmäßig eingerichteten Benutzerrollen mit dazugehörigen Rechten abzuweichen und einen betriebs- oder dienststellenspezifischen Zuschnitt zu erzeugen.

Durch das Rechtemanagement lässt sich – vereinfacht ausgedrückt – sicherstellen, dass jeder Callcenter-Mitarbeiter nur diejenigen personenbezogenen Daten der Kunden einsehen, verändern oder entfernen kann, die zum Zwecke der Erledigung seiner jeweiligen Aufgabe benötigt werden. Eine technische Zweckbegrenzung wird zum Beispiel dadurch umgesetzt, dass die im CRM-System gespeicherten personenbezogenen Daten an die jeweilige Kampagne geknüpft sind; die Zusammenführung sämtlicher Kundendaten aus allen Kampagnen ist nicht möglich.

Auch im Hinblick auf die Callcenter-Mitarbeiter wird die Einhaltung der Zweckbindung der erhobenen Daten über die Mitarbeiter durch ein spezifisches Rechtemanagement gewährleistet. So existieren unterschiedliche Benutzerrollen, die – analog zum Rechtemanagement aufseiten der Kunden – jeweils mit Rechten verschiedenen Umfangs ausgestattet sind. Die konkrete Rechtevergabe ist auf die zur Ausführung des jeweiligen Aufgabenbereichs erforderlichen Befugnisse zugeschnitten.

Unterscheiden lassen sich die vordefinierten Benutzerrollen beispielsweise nach

- Callcenter-Agenten,
- Qualitätsprüfer,
- Teamleiter,
- Geschäftsführung und
- Administrator.

Das dargestellte Rechtemanagement mit den verschiedenen Benutzerrollen bietet eine adäquate Grundlage für die Einhaltung des Grundsatzes der Zweckbindung.

[925] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 71.

8.1.3 Erforderlichkeit des Umgangs mit personenbezogenen Daten

Erforderlichkeit liegt beim Umgang mit personenbezogenen Daten nur dann vor, wenn er für die Erfüllung des zulässigen Zwecks unentbehrlich ist.[926] Eignet sich ein Datum zwar zur Erfüllung der angestrebten Aufgabe oder ist es für sie zweckdienlich, liegt noch nicht die notwendige Erforderlichkeit vor. Die Geeignetheit des Datums allein stellt lediglich die notwendige, nicht jedoch die hinreichende Bedingung zum Vorliegen der Erforderlichkeit dar.[927]

Aufgrund des Erforderlichkeitsgrundsatzes muss für jeden Zweck geprüft werden, ob zu seiner Erreichung tatsächlich der vorgesehene Umfang an personenbezogenen Daten notwendig ist, oder ob die Datenverarbeitung auch mit weniger personenbezogenen Daten auskäme. Sollte Letzteres der Fall sein, muss eine entsprechende Reduzierung der von der Verarbeitung erfassten Daten erfolgen.

Die Erforderlichkeit des Datenumgangs bezieht sich auf ein bestimmtes technisches System sowie einen gegebenen Datenverarbeitungsprozess. Sie verkörpert eine normative Zweck-Mittel-Beziehung. Die Grundlage für einen zulässigen Zweck der personenbezogenen Datenverarbeitung bildet ihre Legitimation, die sich etwa aus einer Einwilligung, einem Vertrag oder einem vertragsähnlichen Vertrauensverhältnis ergeben kann.[928]

Um dem Prinzip der Erforderlichkeit zu genügen, ist der Umgang mit den personenbezogenen Daten unter Einhaltung der nachfolgend aufgeführten Forderungen zu vollziehen:

- Nur die zur Erreichung des festgelegten Zwecks unverzichtbaren Daten dürfen erhoben, verarbeitet oder genutzt werden. Beispielsweise ist die Speicherung von personenbezogenen Daten auf Vorrat zur Verwendung für sich potenziell zukünftig ergebende Zwecke verboten. Diese Forderung stellt gerade im Hinblick auf die CRM-Datenbank und vorgesehene Methoden des Data-Minings eine Einschränkung dar.
- Im Rahmen der Datenverarbeitung dürfen personenbezogene Daten ausschließlich in denjenigen Phasen verwendet werden, die zur Erreichung des festgelegten Zwecks notwendig sind. So ist es etwa verboten, Daten zu speichern, wenn lediglich ihre Erhebung für das Erreichen der Zwecke ausreicht.

[926] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 69.
[927] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 98.
[928] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 98 ff.

- Der Umgang mit den personenbezogenen Daten darf lediglich innerhalb des Zeitraums stattfinden, in dem sie für die Zweckerreichung benötigt werden. Danach sind sie frühest möglich zu löschen.[929]

Ein Weg, den Kunden in der Frage der zeitlichen Beschränkung der Nutzungsmöglichkeit ihrer Daten größtmögliche Selbstbestimmung an die Hand zu geben, besteht darin, sie selbst über eine solche Beschränkung entscheiden zu lassen. Wenn sie selbstbestimmt entscheiden könnten, wann ihre personenbezogenen Daten aus der CRM-Datenbank gelöscht werden, entspräche dies im Grundsatz dem Widerruf einer erteilten datenschutzrechtlichen Einwilligung.

Generell kann das Vertragsende ein adäquater Zeitpunkt darstellen, die personenbezogenen Daten der Kunden endgültig zu löschen. Soweit nachvertragliche Pflichten bestehen, wird der Zeitpunkt ihres Wegfalls der geeignete Löschungszeitpunkt der Daten sein. Da grundsätzlich ein anerkennenswertes Interesse des Callcenters oder dessen Auftraggebers existiert, die Daten für strategische Auswertungen auch nach Beendigung der Vertragsbeziehung weiterhin zu verarbeiten und zu nutzen, sollte für diese Fälle eine Anonymisierung der Daten stattfinden. Somit muss das Datenschutzrecht in Bezug auf diese Daten nicht mehr beachtet werden und dem Datenverarbeiter ist der Umgang mit den in Rede stehenden Daten gestattet.

8.1.4 Datenvermeidung und Datensparsamkeit

§ 3a BDSG normiert zwei der obersten Gebote des Datenschutzrechts, namentlich die Datenvermeidung und Datensparsamkeit.[930] Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten soll möglichst so gestaltet sein, dass personenbezogene Daten überhaupt nicht verwendet werden. Ist es nicht realisierbar, den Zweck der Datenverarbeitung auch ohne Personenbezug zu erreichen, sollen so wenig wie möglich personenbezogene Daten verarbeitet werden. Sofern der Umgang mit personenbezogenen Daten für das Funktionieren des Systems unumgänglich ist, sind die Prozesse vorzugsweise so zu gestalten, dass die Verarbeitung dieser Daten möglichst kurz gehalten wird, und die Daten frühest möglich gelöscht, anonymisiert oder pseudonymisiert werden.[931]

[929] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 98 f.
[930] Dazu ausführlich *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation, Recht und öffentliche Kommunikation, 2011, 41 ff.
[931] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 101; *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation, Recht und öffentliche Kommunikation, 2011, 41 (45 f.).

Einen Ansatz zur Datenvermeidung und Datensparsamkeit bietet die Verwirklichung des Prinzips „Privacy by Default“. Dahinter verbirgt sich die Idee, die Datenverarbeitungsprozesse durch Voreinstellungen im System derart zu gestalten, dass diese von vorneherein möglichst datenvermeidend und datensparsam in Bezug auf personenbezogene Daten ablaufen.

Erst dann, wenn es nicht möglich ist, die zur Zweckerreichung notwendige Datenverarbeitung anonym oder pseudonym durchzuführen, sollte auf personenbezogene Daten zurückgegriffen werden. Der Einbezug der personenbezogenen Daten hat sich auf das Minimum zu beschränken, das zur Realisation der beabsichtigten Zwecke notwendig ist. Sind mit Blick auf das CRM-System beispielsweise für die Ermittlung des Erfolgs einer Marketingmaßnahme nur die erzielten Umsätze mit einem bestimmten Produkt relevant, so ist hierzu unwichtig, welche Käufer für den Umsatz verantwortlich sind. Zu einer solchen Umsatzbestimmung müssen keine personenbezogenen Daten der Kunden mit einbezogen werden.

8.1.4.1 Vermeidung des Personenbezugs

Die grundsätzlich beste Option zur Datenvermeidung besteht in der anonymen Inanspruchnahme der Callcenter-Dienstleistung. Hier sind von vorneherein keine personenbezogenen Daten involviert, und das Datenschutzrecht ist nicht zu beachten.

Anonyme Handlungsmöglichkeit kann generell überall dort eingesetzt werden, wo es auf die tatsächliche Identität einer Person nicht ankommt. Anonymes Agieren ist zum Beispiel denkbar, wenn lediglich Informationen abgefragt oder ausgetauscht werden sollen.[932] Mit Blick auf die Callcenter-Dienstleistung kommt die Vermeidung des Personenbezugs insbesondere für reine Beratungsgespräche in Betracht.

8.1.4.2 Anonymisierung

Falls der Personenbezug der Daten für die Erbringung der Callcenter-Dienstleistung nur bis zu einem gewissen Zeitpunkt benötigt wird, sollten die personenbezogenen Daten zu diesem Zeitpunkt anonymisiert werden. Dies kommt hauptsächlich in Frage, wenn die Daten lediglich zu statistischen Zwecken weiterverarbeitet werden sollen.

[932] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 58.

Bei einer nachträglichen Anonymisierung personenbezogener Daten sollte in jedem Fall gewährleistet sein, dass eine De-Anonymisierung unmöglich ist. Andernfalls handelt es sich um pseudonymisierte Daten, die der Datenverwender selbst erzeugt hat; er kennt die Zuordnungsregel und kann den Personenbezug wieder herstellen. Für solche Daten gilt das Datenschutzrecht weiterhin.

8.1.4.3 Pseudonymisierung

Auch mit der Pseudonymisierung lässt sich das informationelle Selbstbestimmungsrecht des Betroffenen wahren. Pseudonymität bedeutet, dass der Nutzer ein Kennzeichen verwendet, durch das die Wahrscheinlichkeit der Zuordnung von Daten zu seiner Person ohne Kenntnis der Zuordnungsregel derart gering ist, dass sie nach Lebenserfahrung und Stand der Wissenschaft praktisch ausscheidet. Bei der Pseudonymität existiert stets eine Regel, über die der Betroffene dem Pseudonym zugeordnet werden kann. Daten zu einem Pseudonym lassen sich miteinander verknüpfen; so ist es möglich, umfassende Profile zu erstellen, die eine Wiedererkennung ohne die Identifizierung der hinter dem Pseudonym stehenden Person erlaubt.[933]

Besteht die Möglichkeit, die Kundendatenbank des Gesprächsmanagement-Systems, in der kundenbezogene Informationen gespeichert sind, unter verhältnismäßigem Aufwand mit einem pseudonymisierten Datenbestand zu betreiben, sollte diese Chance zu einer kundenspezifischen Informationssammlung ohne direkten Personenbezug ergriffen werden. Gerade die im Laufe der Zeit angehäuften Datenmengen, die durch die Akkumulation einer Vielzahl von Einzelinformationen entstanden sind, können zu einer schwerwiegenden Gefährdungslage in Bezug auf das informationelle Selbstbestimmungsrecht der Kunden führen: Die Spannweite des Denkbaren reicht von der Bildung eines umfassenden Käuferprofils bis hin zur Vorhersage zukünftigen Verhaltens der Kunden.[934]

Es gilt allerdings zu beachten, dass eine übermäßige Ansammlung von Kundendaten, die unter einem Pseudonym gespeichert sind, zur Aufdeckung des Individualisierungsmerkmals führen kann. Die Summe der gespeicherten Informationen lässt in einem solchen Fall Rückschlüsse auf die hinter dem Pseudonym stehende Person zu.[935]

---

[933] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 60 ff.
[934] *Scholz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.2 Rn. 35 ff.
[935] *Ranke*, M-Commerce und seine rechtsadäquate Gestaltung, 2004, 198 f.

Die systeminterne Kommunikation der einzelnen Komponenten des Gesprächsmanagement-Systems untereinander erfolgt pseudonym mittels Session-ID. Ausgetauschte Datenpakete erhalten lediglich eine laufende Nummer, mit der sich keine direkten Bezüge zu einem bestimmten Telefonkontakt und zu einem bestimmten Kunden herstellen lassen. So ist es beispielsweise nicht möglich, anhand der bei den angeschlossenen Datenbanken ankommenden Datenpakete herauszufinden, durch welche Personen die jeweiligen Suchanfragen ausgelöst wurden. Diese technische Umsetzung führt zwar zu keiner Stärkung des Datenschutzes bei den vom Callcenter unmittelbar kontrollierbaren Systemkomponenten des Gesprächsmanagement-Systems: Über die Komponente, welche die zentrale Vergabe der Session-ID vornimmt, kann die Re-Identifizierung der Person erfolgen. Voraussetzung dafür ist, dass der Personenbezug überhaupt bekannt war; bei der anonymen Inanspruchnahme der Callcenter-Dienstleistung ist dies nicht gegeben. Was jedoch die Kommunikation mit außerhalb des Verantwortungsbereichs des Callcenters liegenden Ressourcen – wie öffentlich zugängliche Wissensquellen im Internet – durch das Gesprächsmanagement-System anbelangt, so führt die Pseudonymisierung der Datenpakete dazu, dass sie gegenüber externen Datenbanken anonym sind. Eine Aufdeckung der Person ist für außenstehende Diensteanbieter somit nicht realisierbar.

8.1.4.4 Löschkonzept

Eine Vorgehensweise, den potenziellen zukünftigen Umgang mit personenbezogenen Daten möglichst datensparsam zu gestalten, besteht in der frühzeitigen Löschung von entsprechenden Daten nach Ablauf bestimmter Fristen oder beim Eintritt von bestimmten Ereignissen. Im erstgenannten Fall sind die angefallenen Daten für einen bestimmten Zeitraum rückwirkend zu löschen. Dieser Gestaltungsvorschlag kann im Rahmen des Gesprächsmanagement-Systems zum Beispiel anhand einer Kollektivvereinbarung zur Qualitätsoptimierung der Kundengespräche umgesetzt werden, in der die Löschung der Daten zur Beurteilung der Arbeitsqualität der Callcenter-Agenten entsprechend geregelt wird.

Die Datenlöschung von festzulegenden Ereignissen abhängig zu machen, bietet sich insbesondere für die Situationen an, in denen Callcenter-Mitarbeiter ausscheiden oder Kunden ihr Vertragsverhältnis beenden. Der Löschungszeitpunkt lässt sich auch automatisch an ablaufende Fristen knüpfen, so zum Beispiel an den Ablauf von Gewährleistungsansprüchen.

Da es trotz gekündigter oder abgelaufener Vertragsbeziehungen für das Callcenter zweckmäßig sein kann, Kundendaten weiterhin im CRM-System zu speichern und in Auswertungsprozesse mit einzubeziehen, müssen diese Daten vollständig anonymisiert werden, damit keine Möglichkeit einer nachträglichen Aufdeckung der betroffenen Personen bestehen kann. Außer etwaige, der Löschung entgegenstehende Aufbewahrungspflichten existieren keine Rechtfertigungsgründe zur fortwährenden Speicherung der personenbezogenen Daten.

8.1.5 Transparenz der Datenverarbeitungsprozesse

Komplexe Datenverarbeitungsprozesse, wie sie auch im Gesprächsmanagement-System stattfinden, sind für den Betroffenen nicht zu durchschauen. Die Notwendigkeit des transparenten Umgangs mit personenbezogenen Daten ergibt sich insbesondere aus der Tatsache, dass diese Daten für den Betroffenen unbemerkt erhoben, verarbeitet oder genutzt werden können. Damit der Betroffene sein Recht auf informationelle Selbstbestimmung überhaupt wahrnehmen kann, muss ihm der Datenumgang bekannt sein. Aus der fehlenden Transparenz resultiert eine faktische Rechtlosigkeit des von der Datenverarbeitung Betroffenen.[936]

Zur Herstellung der erforderlichen Transparenz bei der Datenverarbeitung sieht das Datenschutzrecht zwei wesentliche Formen vor:

1. Informationspflichten für die datenverarbeitende Stelle, wobei die Stelle selbst aktiv werden muss und
2. Auskunftsansprüche des Betroffenen, für dessen Durchsetzung der Betroffene verantwortlich ist.[937]

Transparenz im Hinblick auf die Datenverarbeitungsvorgänge erfordert zunächst, die Daten beim Betroffenen selbst zu erheben und ihn diesbezüglich im Vorfeld zu unterrichten.[938] Um zu gewährleisten, dass eine selbstbestimmte, unbefangene Kommunikation stattfinden kann, müssen die Gesprächspartner im Grundsatz im Voraus informiert sein, welche anfallenden Daten der Kommunikation wie verarbeitet werden; dies gilt für die Kunden wie für die Callcenter-Agenten gleicherma-

[936] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 82; *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 71.
[937] *Bizer*, DuD 2007, 350 (354).
[938] *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, 133.

ßen. Außerdem muss bekannt sein, wer in welcher Form an dem Informationsaustausch beteiligt sein kann.[939]

8.1.5.1 Informationspflichten

Durch § 4 Abs. 3 Satz 1 BDSG werden dem Callcenter Informationspflichten auferlegt, wenn personenbezogene Daten beim Betroffenen erhoben werden; sowohl Kunden als auch Callcenter-Agenten verkörpern Betroffene im Zusammenhang mit Datenerhebungen im Callcenter. Sofern die Kenntnis der Erhebung bereits vorliegt, entfällt diese Informationsverpflichtung. Die Pflichten beziehen sich auf Angaben

- zur Identität des Callcenters,
- zu den Zweckbestimmungen des Datenumgangs und
- zu Empfängerkategorien, soweit mit einer Datenübermittlung an sie nicht gerechnet werden muss.

In diesem Zusammenhang darf der potenzielle Akzeptanzgewinn hinsichtlich des Datenumgangs bei den Betroffenen nicht unterschätzt werden: Wenn ihnen bereits vorab verdeutlicht wird, für welche Zwecke und wie ihre personenbezogenen Daten erhoben, verarbeitet oder genutzt werden, vermag dies unter Umständen zu einer höheren Bereitschaft zu führen, solche Daten bereitzustellen.

Eine technische Maßnahme im Callcenter, die der Realisierung der Informationspflicht gegenüber den Kunden dient, besteht in einer automatischen Bandansage, die dem eigentlichen Gespräch zwischen Callcenter-Agent und Kunde vorgeschaltet ist. In einer solchen Ansage müssen Name und Anschrift der verantwortlichen Stelle enthalten sein, damit der Kunde Gewissheit hat, gegenüber wem er seine Rechte geltend machen kann.[940]

Weiterhin ist präzise und verständlich auf die Zwecke des Datenumgangs hinzuweisen; die Kunden müssen sich ohne besonderes Vorverständnis ein Bild über die Zweckbestimmungen machen können.[941] Es ist darauf zu achten, dass sämtliche – auch potenziell erst zukünftig vorgesehene – Zwecke von der Information erfasst sind. Gerade die Auswertung und Verknüpfung von personenbezogenen Daten innerhalb des CRM-Systems führen unter Umständen zu völlig neuen Daten, deren

[939] *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993, 71.
[940] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 30.
[941] *Taeger*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, § 4 Rn. 71.

Verwendungsmöglichkeit von der ursprünglichen Zweckbestimmung der Datenerhebung nicht mehr gedeckt ist.

Der Forderung nach einer adäquaten Auskunft über die Zweckbestimmungen kann in der Praxis oftmals nur schwer Rechnung getragen werden, da zwischen einer zu pauschalen und damit „schwammigen" Angabe und einer zu umfangreichen Menge an Detailinformationen zwangsläufig ein Dilemma besteht. Ist die Angabe zu generell und undifferenziert, wird sie dem Transparenzgebot ebenso wenig gerecht, wie wenn eine Überfrachtung aufgrund zu vieler Einzelinformationen vorliegt. Hier gilt es, das richtige Maß zu finden, das einerseits allgemein genug ist, dass alle Zwecke abgedeckt sind, und andererseits präzise genug, damit die Zwecke zu durchschauen sind. Ein Lösungsansatz könnte darin bestehen, eine zweistufige Information anzubieten: Erstens könnte eine allgemeine Angabe grob Aufschluss über die vorgesehenen Zwecke des Datenumgangs geben und darüber hinaus den Hinweis auf eine eingängige URL zu einer Webseite enthalten, die zweitens umfangreiche und detaillierte Informationen bereitstellt.

Aufgrund der Komplexität der technischen Struktur des Gesprächsmanagement-Systems sollte auch eine angemessene Information über die wesentlichen Systemkomponenten mit den jeweiligen Datenverarbeitungsprozessen erfolgen. Dabei ist mehr auf die Struktur und Funktionsweise der Verfahren als auf einzelne Daten abzustellen. Die Vielzahl von (potenziell) betroffenen Daten macht eine überschaubare Angabe im Grunde genommen unmöglich. In Anlehnung an § 6a Abs. 3 BDSG sollte der logische Aufbau der automatisierten personenbezogenen Datenverarbeitung offengelegt werden.[942]

Da die Kunden in der Regel nicht damit rechnen, dass ihre personenbezogenen Daten, die im Gespräch anfallen, auch zu externen Auftragnehmern des Callcenters übertragen werden, hat darüber hinaus ein Hinweis auf die Empfängerkategorien zu erfolgen. Es ist notwendig, auch interne Datenströme, also nicht nur Datenübermittlungen an Dritte, mit anzugeben.[943] Für die Informationspflicht bedeutet dies konkret, dass auch Datenübertragungen an externe Dienstleister – die sich innerhalb der „Systemgrenzen" des Gesprächsmanagement-Systems befinden können – mitzuteilen sind, bei denen etwa die Analyse des Telefonats und die Speicherung sowie die weitere Verarbeitung der daraus gewonnenen Informationen durchgeführt werden.

[942] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 86 ff.
[943] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 32 ff.

Praxistauglich lässt sich die Kundeninformation ferner für bestimmte Fälle durch schriftliche Aufklärung organisieren. Dies gilt besonders dann, wenn ein langfristiges Vertragsverhältnis mit den Kunden vorliegt und der Einsatz des Gesprächsmanagement-Systems im Rahmen von Beratungsleistungen oder eines Beschwerdemanagements erfolgt. Das Unterrichtungsschreiben hat gegenüber einer mündlichen Information den Vorteil für Kunden, dass diese jederzeit und ohne Aufwand ihr Wissen um die praktizierten Datenverarbeitungsvorgänge des Callcenters auffrischen können. Gleichzeitig ist damit ein Rückgang diesbezüglicher Nachfragen durch Kunden beim Callcenter zu erwarten; insoweit profitieren beide Seiten von einer solchen Lösung. Darüber hinaus führt – besonders in den Fällen, in denen eine schriftliche Information nicht erfolgen kann – die Veröffentlichung der Kundeninformation oder weitergehender Informationen auf der Webseite des eigenständigen Callcenters oder des Unternehmens, welches das Callcenter selbst betreibt oder für sich im Auftrag arbeiten lässt, dazu, dass Kunden die Angaben jederzeit abzurufen vermögen.

Insbesondere im Kontext von Callcentern lässt sich das Angewiesensein auf die Kommunikation mittels Telefon zunutze machen: Hier kann relativ einfach und ohne großen technischen Aufwand eine Bandansage – analog zum bereits genannten Vorschlag der Bandansage zu Gesprächsbeginn – eingerichtet werden, die sämtliche aufgezeigten Informationen enthält. Diese Ansage kann über eine separate Telefonnummer, die den Kunden bei Erstkontakt mit dem Callcenter mitgeteilt wird, erreichbar sein. Durch ein solches Vorgehen ließe sich eine automatisierte Datenschutzerklärung realisieren.[944]

Welcher Möglichkeit der Vorzug zu geben ist, lässt sich nicht allgemeingültig beantworten. Diese Entscheidung muss insbesondere vor dem Hintergrund der Rechtsbeziehung zwischen Callcenter und Kunden getroffen werden: Bei Dauerschuldverhältnissen, wie einer Versicherungsvertragsbeziehung, kann es sinnvoll sein, der Informationspflicht schriftlich nachzukommen. Ist der Kontakt hingegen nur auf kurze Dauer angelegt, etwa wenn Interessenten sich lediglich über ein neues Produkt erkundigen wollen, wird tendenziell eine Bandansage zu Gesprächsbeginn ausreichen. Im letztgenannten Beispiel ist es in der Regel nicht erforderlich, dass ein neuer Eintrag über den Interessenten und somit potenziellen Kunden in der CRM-Datenbank vorgenommen wird. Die Zweckbestimmungen dürften sich damit auf ein Minimum reduzieren.

[944] Befürworter der Einführung einer Datenschutzerklärung *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 86 f.; *Roßnagel*, MMR 2005, 71 (74).

Keine gesonderte Hinweispflicht besteht, wenn die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten der Kunden durch eine Einwilligung legitimiert wird. In diesem Fall fordert § 4a BDSG bereits die Informationen im Rahmen einer informierten Einwilligung, welche auch nach § 4 Abs. 3 BDSG durch die Informationspflicht zu erteilen sind.[945]

Die Legitimation des Datenumgangs durch eine Einwilligung kommt hauptsächlich dann in Betracht, wenn besonders schutzwürdige personenbezogene Daten, wie sie für die Gesundheitsberatung notwendig sind, erhoben, verarbeitet oder genutzt werden sollen. Wenn sich der zulässige Datenumgang aus gesetzlichen Rechtfertigungsgründen ergibt, sollte auf eine zusätzliche Einwilligung verzichtet werden.[946]

Die Callcenter-Agenten haben individuell entweder durch ihren Arbeitsvertrag selbst oder durch Zusatzvereinbarungen zum Arbeitsvertrag in den Umgang mit ihren personenbezogenen Daten eingewilligt. Alternativ kann eine kollektivvertragliche Regelung durch eine Betriebs- oder Dienstvereinbarung einen solchen vorsehen. Bei einer individuellen Einwilligung müssen gemäß § 4a Abs. 1 Satz 2 BDSG die Zwecke der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten benannt werden. Dasselbe gilt für eine Kollektivvereinbarung. Eine Betriebsvereinbarung ist gemäß § 77 Abs. 2 Satz 3 BetrVG an geeigneter Stelle im Betrieb auszulegen. Dies gewährleistet für nichtöffentliche Callcenter-Betriebe, dass sich die Callcenter-Agenten innerhalb der Geschäftsräume über vorgesehene Datenverarbeitungen informieren können. Das Personalvertretungsrecht geht nicht so weit; es verlangt nicht ausdrücklich den Aushang einer Dienstvereinbarung in der Dienststelle, dennoch ist die Vereinbarung gemäß § 73 Abs. 1 Satz 2 BPersVG in geeigneter Weise bekannt zu machen.

Was die Förderung der Transparenz in Bezug auf die Datenverarbeitungsvorgänge für die Callcenter-Agenten angeht, kann darüber hinaus eine Datenschutzerklärung in der Frontend-Software implementiert werden, die zum Beispiel über die Menüleiste jederzeit abrufbar ist. So haben die Mitarbeiter eine unkomplizierte Möglichkeit, sich über die betroffenen Daten sowie über die Zwecke des Datenumgangs zu erkundigen.

[945] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4 Rn. 40.
[946] Die Probleme einer solchen Vorgehensweise wurden bereits in Kapitel 3.1.1.1.3 „Erlaubnis aus einer Einwilligung“ aufgezeigt.

8.1.5.2 Auskunftsansprüche

Betroffenen von Datenverarbeitungsprozessen steht ein allgemeiner Auskunftsanspruch[947] zu, der ihnen die zur Wahrnehmung ihres Rechts auf informationelle Selbstbestimmung notwendige Transparenz verschaffen soll. Dieser Rechtsanspruch gilt als fundamentales Datenschutzrecht. Die bereits anhand der Informationspflichten hergestellte Durchschaubarkeit der Datenverarbeitungsvorgänge wird durch das Auskunftsrecht erweitert.[948]

Eine gesteigerte Sensibilität der Bevölkerung in Sachen Datenschutz ist – insbesondere vor dem Hintergrund bekanntgewordener „Datenschutzskandale" – zukünftig zu erwarten. Bereits aus diesem Grund gilt es, ein vorausschauendes Vorgehen bei der Umsetzung der Auskunftserteilung durch Callcenter-Betriebe zu erreichen. Generell könnte die Zahl der Auskunftsersuchen dadurch minimiert werden, dass eine Webseite des Callcenters oder dessen Auftraggebers Angaben zum Datenumgang und Datenschutz enthält.

Das Auskunftsrecht erstreckt sich auf die gespeicherten Angaben über persönliche und sachliche Verhältnisse, die auf die Person des Betroffenen bezogen oder beziehbar sind.[949] Im Hinblick auf die „Granularität" der Datenschutzauskunftsbescheide kann auf die Ausführungen zu den oben aufgezeigten Informationspflichten verwiesen werden: Hauptsächlich nicht mehr zu überblickende Datenverarbeitungsprozesse und deren Ergebnisse – primär im Kontext des Data-Warehousings und Data-Minings – erfordern, dass sich die Auskunft weniger auf sämtliche betroffenen Daten und Datenkategorien im Einzelnen bezieht als vielmehr auf die Abläufe und auf die Strukturen der Prozesse. So sind beispielsweise bei Profilerstellungen eher die ausschlaggebenden Kriterien für deren Entstehung, als sämtliche im konkreten Fall vorliegenden Einzeldaten zu benennen.

Im Übrigen müssen die Zwecke der gespeicherten Daten offengelegt werden. In bestimmten Fällen kann hierzu eine abstrakte Angabe, wie „...zum Zwecke der Auftragsdurchführung...", ausreichen.[950]

[947] Darüber hinaus existieren bereichsspezifische Auskunftsansprüche, die den allgemeinen Auskunftsanspruch verdrängen.
[948] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 171; *Weichert*, DuD 2006, 694.
[949] *Hoss*, RDV 2011, 6.
[950] *Hoss*, RDV 2011, 6.

Damit die kurzfristige Reaktion auf Anfragen durch Kunden möglich ist, sollte durch technisch-organisatorische Maßnahmen sichergestellt sein, dass ein schnelles Zusammentragen der notwendigen Daten und Angaben über den jeweiligen Kunden realisiert werden kann. Die betreffenden Informationen sollten ohne großen Aufwand auffindbar sein; bei verteilten Systemen – wie unter Umständen dem Gesprächsmanagement-System – stellt dies eine große Herausforderung dar. Die dezentrale Datenverarbeitung in den verschiedenen Systemkomponenten gestaltet sich dabei als praktische Schwierigkeit.[951] Allerdings führte ein möglichst einheitliches Vorgehen bei unterschiedlichen Kampagnen im Hinblick auf die Speicherung kundenbezogener Daten im System – in einer nachvollziehbaren Struktur – zur leichteren Auffindbarkeit von Daten. So könnte etwa mittels Arbeitsanweisung im Callcenter angeordnet werden, dass das Abspeichern von Dateien, die kundenspezifische Inhalte aufweisen, in der Archivdatenbank des CRM-Systems nur anhand einer bestimmten Verzeichnisstruktur durchgeführt werden darf.

Auf Verlangen der Kunden ist die Datenschutzauskunft durch nichtöffentliche Callcenter gemäß § 34 Abs. 6 BDSG in Textform zu erteilen, soweit keine besonderen Umstände vorliegen, die eine andere Form der Auskunftserteilung rechtfertigen. Damit ist die Auskunft auch in Form einer E-Mail-Nachricht zulässig. Falls das Callcenter die E-Mail-Adresse des Kunden kennt, stellt die Möglichkeit der E-Mail-Auskunft eine vergleichsweise zeitnah zu realisierende und kostengünstige Alternative zu einem per Post versandten Schreiben dar.

Besteht hingegen kein ausdrücklicher Wunsch nach einem textuellen Auskunftsbescheid, kann die Auskunft auch in anderer Form durchgeführt werden. Aus rechtlicher Perspektive spricht grundsätzlich nichts gegen eine telefonische Datenschutzauskunft. Ideal wäre eine Situation, in der Kunden beim Callcenter anriefen, um die Auskunft bitten würden und diese direkt von dem mit ihnen verbundenen Callcenter-Mitarbeiter erteilt bekämen.

Soll die telefonische Variante der Auskunftserteilung umgesetzt werden, ist eine Methode notwendig, die die eindeutige Identifizierung des jeweiligen Kunden ermöglicht. Die Abfrage eines Passworts oder die Eingabe einer PIN und TAN am Telefon des Kunden können, abhängig vom Einzelfall, adäquate Mechanismen zur Identifizierung darstellen. Die Sicherheit der eingesetzten Methode ist jedenfalls an die Schutzwürdigkeit der (potenziell) betroffenen Daten anzupassen.

[951] Zu dem Vorschlag, in verteilten Systemen allgemein einen Datentreuhänder einzurichten, s. *Weichert*, DuD 2006, 694 ff.

Öffentliche Callcenter-Betriebe bei Bundeseinrichtungen können über die Form der Auskunftserteilung gemäß § 19 Abs. 1 Satz 4 BDSG nach pflichtgemäßem Ermessen selbst entscheiden. In den Datenschutzgesetzen der Länder ist dies analog geregelt.[952]

8.1.6 Datensicherheit

§ 9 BDSG und dessen Anlage fordern bestimmte Maßnahmen zur Datensicherheit, die von den datenverarbeitenden Stellen zu erfüllen sind. Als datenverarbeitende Stellen gelten ausdrücklich auch Auftragsdatenverarbeiter, sodass diese Maßnahmen bei einer solchen Konstellation des Gesprächsmanagement-Systems, bei der die verschiedenen Systemkomponenten von unterschiedlichen Dienstleistern betrieben werden, bei jedem einzelnen Unternehmen umgesetzt werden müssen. Erforderlich sind jedoch nur solche Maßnahmen zur Datensicherheit, die in einem angemessenen Verhältnis zu ihrem angestrebten Schutzzweck stehen.

Die Feststellung, welche konkreten Vorkehrungen dem Kriterium Erforderlichkeit genügen, sollte idealerweise auf Grundlage einer standardisierten Risikoanalyse getroffen werden. Der BSI-Grundschutzkatalog und insbesondere die Risikoanalyse auf Grundlage des IT-Grundschutzes bilden einen adäquaten Handlungsrahmen, an dem sich diese Untersuchung orientieren sollte.[953]

In diesem Zusammenhang ist weitergehend zu beachten, dass die Risikoanalyse und die gegebenenfalls notwendig werdende Anpassung der Schutzvorkehrungen in regelmäßigen Abständen stattfinden müssen. Der Bereich der informationstechnischen Systeme entwickelt sich mit rasanter Geschwindigkeit. Dementsprechend schnell entstehen auch programmtechnische „Einfallstore“, mit denen die Umgehung von Schutzmaßnahmen möglich wird.

Konkrete Datensicherheitsmaßnahmen, die im Gesprächsmanagement-System implementiert werden, sind nachfolgend aufgezeigt.

Zur Feststellung, welcher Callcenter-Mitarbeiter sich am Gesprächsmanagement-System anmeldet, ist die Eingabe einer Benutzerkennung mit dazugehörigem Passwort erforderlich. Damit wird eine angemessene Zugangskontrolle verwirklicht.

[952] So zum Beispiel in § 24 Abs. 1 Satz 4 DSG M-V und in § 21 Abs. 3 Satz 1 LDSG.
[953] S. www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html #doc471418bodyText3.

Beim Anmeldevorgang erfolgt die Generierung einer Session-ID; sie ermöglicht einen zeitlich befristeten Zugriff auf bestimmte Daten.[954]

Die Zugriffskontrolle wird durch ein feingliedriges Rechtemodell realisiert. Jeder Benutzer des Systems ist einer bestimmten Benutzerrolle zugeordnet, die auf seine spezifische Tätigkeit zugeschnittene Rechte enthält. Der Callcenter-Agent beispielsweise darf nur auf solche Daten zugreifen, die er in der jeweiligen Arbeitssituation benötigt. Falls der Callcenter-Agent in mehreren Kampagnen eingesetzt wird, ist es ausgeschlossen, dass er personenbezogene Daten zu Gesicht bekommt, die aus einer anderen Kampagne stammen, als derjenigen, in der er aktuell tätig ist.

Eine schriftliche Dokumentation und Aktualisierung des Rechtemodells ist zwingend notwendig.[955] Durch sie bleibt auf einen Blick ersichtlich, welche Person über welche Zugriffsrechte verfügt.

Ferner ist besonderer Wert darauf zu legen, dass personenbezogene Daten nicht unerlaubt aus dem System abfließen können. Hierzu lassen sich einfache Sicherheitsmechanismen, wie die Einschränkung oder Abschaltung der Datenexport- und Druckfunktion sowie der Copy-and-Paste-Funktion, einsetzen.[956]

Der Anforderung, dass personenbezogene Daten während ihrer elektronischen Übertragung nicht unbefugt mitgelesen werden dürfen, wird durch Anwendung einer Verschlüsselungsmethode in der Datenübertragung zwischen den einzelnen verteilten Systemkomponenten Rechnung getragen. Kryptografische Mechanismen wandeln die Daten derart um, dass sie für Angreifer nicht zu verstehen sind; sie dienen der Gewährleistung von Datenvertraulichkeit.[957] Die konkrete Verschlüsselungsmethode, die im Gesprächsmanagement-System zum Einsatz gelangt, ist die SSL-Verschlüsselung.

Als weitere Anforderung gilt die nachträgliche Nachvollziehbarkeit sämtlicher am System vorgenommenen Aktionen eines Benutzers, die personenbezogene Daten betreffen. Es muss generell feststellbar sein, ob und durch wen personenbezogene Daten eingegeben, verändert oder entfernt wurden.

Diese Eingabekontrolle wird durch die Protokollierung der durchgeführten Aktionen jedes einzelnen Callcenter-Agenten umgesetzt. Dazu wird im Gesprächsmana-

[954] *Volkmann/Gaßmann*, K&R 2011, 30.
[955] *Baumgärtner et al.*, DSB 4/2004, 9.
[956] So realisiert bei *CAS Software AG*, Datenschutz mit CAS genesisWorld, Stand: Juli 2010, 10 f.
[957] *Tanenbaum/van Steen*, Verteilte Systeme, 2. Aufl. 2007, 414.

gement-System eine Journal-Funktion implementiert. Durch sie ist beispielsweise detailliert nachvollziehbar, welcher Callcenter-Mitarbeiter zu welchem Zeitpunkt auf welchen Datensatz in der Kundendatenbank zugegriffen hat.

Dem Trennungsgebot trägt das Gesprächsmanagement-System dadurch Rechnung, dass die zu unterschiedlichen Zwecken erhobenen Daten separat gespeichert werden. So erfolgt zum Beispiel die Speicherung personenbezogener Daten im CRM-System auf einer anderen Datenbank, als auf derjenigen, auf der aufgezeichnete Telefongespräche abgelegt werden. Die Herstellung eines Zusammenhangs zwischen Einträgen in der Kundendatenbank und den jeweiligen Gesprächen mit Kunden, aus denen die Datensätze resultierten, ist ohne Kenntnis der konkreten Zuordnungsnummer nicht möglich.

8.1.7 Kontrolle der Datenverarbeitungsprozesse

Ab einer bestimmten Größe oder in Abhängigkeit von der Art der Datenverarbeitung schreibt das Bundesdatenschutzgesetz die Bestellung eines internen Datenschutzbeauftragten vor.[958]

Gemäß § 4f Abs. 2 Satz 1 und 2 BDSG muss der Datenschutzbeauftragte die erforderliche Fachkunde vorweisen, die er zur Ausübung seiner Tätigkeit benötigt. Diese Fachkunde hat sich primär am Umfang der Datenverarbeitungsprozesse und der Schutzwürdigkeit der betroffenen Daten zu orientieren. Der Datenschutzbeauftragte sollte sich in Zweifelsfragen oder bei speziellen Fragestellungen in Bezug auf den organisationsinternen Datenschutz, die über seinen Kenntnisstand hinausgehen, an einschlägige Experten wenden. Besonders im Hinblick auf die professionelle Umsetzung der genannten Datensicherheitsmaßnahmen drängt sich die Frage auf, ob hierfür nicht ein spezialisierter IT-Sicherheitsbeauftragter hinzugezogen werden sollte. Diese Tätigkeit können externe Dienstleister oder innerbetriebliche Personen wahrnehmen. Eine gesetzliche Verpflichtung zur Bestellung eines solchen Funktionsträgers besteht im Zusammenhang mit dem Gesprächsmanagement-System allerdings nicht.

Beispielsweise für Telekommunikationsdiensteanbieter, die ihre Dienste für die Öffentlichkeit erbringen, ist die Bestellung eines Sicherheitsbeauftragten gemäß § 109 Abs. 3 TKG eine gesetzliche Pflicht. Der bestellte Beauftragte verfügt über fach-

[958] Dazu näher Kapitel 7.1.1 „Beauftragter für Datenschutz".

spezifische Kompetenzen und entlastet das Unternehmen, das sich auf seine originären Geschäftsfelder konzentrieren kann.[959]

8.1.8 Beachtung der Mitwirkungsrechte der Betroffenen

Werden personenbezogene Daten eines Betroffenen erhoben, verarbeitet oder genutzt, stehen ihm verschiedene Ansprüche zu, die der Wahrung seines informationellen Selbstbestimmungsrechts dienen. Damit der Betroffene überhaupt von diesen Rechten Gebrauch machen kann, muss er zunächst vom Umgang mit seinen personenbezogenen Daten wissen. Insofern stellen seine Rechte auf Benachrichtigung und Auskunft wichtige Grundvoraussetzungen zur Wahrnehmung von Einwirkungsrechten dar – wie das Recht auf Löschung –, wenn ein unzutreffender, unrichtiger oder missbräuchlicher Umgang mit seinen Daten stattfindet.[960]

Um sicherzustellen, dass den Kunden, aber auch den Beschäftigten im Callcenter, ein fachlich kompetenter Ansprechpartner in Sachen Datenschutz zur Seite steht, sollte der organisationsinterne Datenschutzbeauftragte als zentrale „Beschwerdeinstanz“ fungieren.[961] Es wäre damit wenig Koordinierungsaufwand bei der Abwicklung datenschutzrelevanter Anliegen erforderlich. Im Übrigen verfügt der Datenschutzbeauftragte über ein fundiertes Fachwissen und wird bei einschlägigen Problemen im Normalfall angemessene Abhilfe leisten können.

Wenn Betroffene ihre Rechte gegenüber dem Callcenter-Betreiber geltend machen, sollte der Datenschutzbeauftragte den gesamten Prozess steuern und begleiten. Der Datenschutzbeauftragte hat den besten Einblick in die stattfindenden Datenverarbeitungsvorgänge. Kommt etwa das Recht auf Löschung zum Tragen, wird er in der Regel wissen, wo überall (potenziell) innerhalb des Systems personenbezogene Daten des Betroffenen gespeichert sind, welche gelöscht werden müssen.

8.1.9 Zusammenfassende Darstellung der Gestaltungsvorschläge

Um ein möglichst hohes Datenschutzniveau zu realisieren, lassen sich den oben aufgezeigten wesentlichen Prinzipen des Datenschutzes und den weiteren datenschutzrechtlichen Forderungen technische und organisatorische Vorschläge (Stellschrauben) zuordnen, deren Umsetzung das Datenschutzniveau positiv beeinflussen.

[959] *Heckmann*, MMR 2006, 280 (285).
[960] *Wedde*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.4 Rn. 12 ff.
[961] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 175 f.

Nachfolgende Abbildung zeigt diese Vorschläge in einem Ursache-Wirkungs-Diagramm:

Abb. 7: Ursache-Wirkungs-Diagramm: Stellschrauben für das Datenschutzniveau.
Quelle: Der Verfasser.

8.2 Rechtliche Regelungsvorschläge zur Erhöhung des Datenschutzniveaus

Die Datenschutzrichtlinie bildet den Rechtsrahmen, der von den nationalen Gesetzgebern ausgefüllt werden kann.[962] Aus der oben dargestellten datenschutzrechtlichen Bewertung des Gesprächsmanagement-Systems ergibt sich nicht das zwingende Erfordernis, das geltende Datenschutzrecht anzupassen. Eine Fortentwicklung des Rechts ist also nicht notwendig, um ungerechtfertigte Hindernisse für die Nutzung des Gesprächsmanagement-Systems zu beseitigen. Dennoch konnten bei der detaillierten Betrachtung der datenschutzrechtlichen Vorgaben einige Ansatzpunkte identifiziert werden, die zur Erhöhung des allgemeinen Datenschutzniveaus beitragen könnten. Diese Aspekte sollen im Folgenden aufgezeigt werden.

[962] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 55 f.

8.2.1 Vereinfachung des Datenschutzrechts

Die Zersplitterung des deutschen Datenschutzrechts in eine große Anzahl bereichsspezifischer Vorschriften stellt ein bedeutendes Problem im Hinblick auf die Übersichtlichkeit dar. Das Bundesdatenschutzgesetz als allgemeines Auffanggesetz wird von den spezialgesetzlichen Regelungen gemäß § 1 Abs. 3 Satz 1 BDSG verdrängt.

Zukünftig sollte diese Systematik umgekehrt werden: Das Bundesdatenschutzgesetz sollte im Verhältnis zu bereichsspezifischen Gesetzen vorrangig anzuwenden sein. So könnten die Normenflut eingedämmt und Widersprüche ausgeräumt werden. Nur im Ausnahmefall, wenn der Datenumgang ein besonders hohes Risiko für die Rechte der Betroffenen darstellt, müsste durch bereichsspezifische Ausnahmen dieser Tatsache Rechnung getragen werden. Ebenso kommen Ausnahmeregelungen für die Fälle in Betracht, in denen der Umgang mit personenbezogenen Daten unterdurchschnittliche Gefahren birgt.[963]

Ein weiterer Ansatzpunkt zur Vereinheitlichung stellt die grundsätzliche Aufhebung der Differenzierung nach öffentlichen und nichtöffentlichen Stellen dar. Die Idee ist, dass für beide Bereiche grundsätzlich dasselbe Datenschutzniveau vorliegen muss, das nicht mehr bereichs-, sondern risikoabhängig zu bestimmen ist. Es müsste dabei allerdings berücksichtigt werden, dass die Adressaten der Vorschriften im nichtöffentlichen Bereich Grundrechtsträger sind, und der öffentliche Bereich die Verfolgung von Allgemeininteressen zum Ziel hat.[964]

Darüber hinaus ist anzustreben, die bereichsspezifischen Datenschutzregelungen des Telekommunikationsgesetzes und des Telemediengesetzes in das Bundesdatenschutzgesetz zu integrieren, um bestehende Überschneidungen und Wertungswidersprüche zukünftig zu vermeiden.[965]

8.2.2 Regelung des Beschäftigtendatenschutzes

Seit vielen Jahren besteht gemeinhin das Bedürfnis, den Bereich des Datenschutzes für Beschäftigte eigenständig zu regeln. Der aktuell gültige § 32 BDSG zum Beschäftigtendatenschutz konnte noch kurz vor Ablauf der 16. Legislaturperiode ver-

[963] *Roßnagel*, RDV 2002, 61 f.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 13; ebenso *Jacob*, DuD 2000, 5 (8), der von einer „...Rückbesinnung auf das BDSG als Ausgangspunkt und Schnittstelle der Regelungen zum Datenschutz“ spricht.
[964] *Roßnagel*, RDV 2002, 61 (62).
[965] *Roßnagel*, RDV 2002, 61 (62).

abschiedet werden. An dieser Tatsache ist festzustellen, dass der Gesetzgeber hier den Handlungsbedarf erkannt hat. Die Regelung des § 32 BDSG wurde vom Gesetzgeber quasi als „Statthalter“ für ein umfangreicheres Beschäftigtendatenschutzrecht angesehen.

Zwischenzeitlich wurde von der Bundesregierung ein Gesetzentwurf[966] vorgelegt, der den Beschäftigtendatenschutz umfassend regeln soll. Im Grundsatz ist dieser Entwurf begrüßenswert, dennoch besteht in vielen Punkten noch Notwendigkeit zur Nachbesserung. Dies kommt insbesondere in der Stellungnahme des Bundesrats[967] zum Ausdruck, die eine Vielzahl von zutreffenden Kritikpunkten in Bezug auf den Gesetzentwurf enthält.

Die umfassende Festschreibung datenschutzrechtlicher Vorschriften hinsichtlich Beschäftigungsverhältnisse führte jedenfalls zu größerer Rechtssicherheit für beide Parteien des Beschäftigungsverhältnisses.

8.2.2.1 Konkretisierung der Zulässigkeitsvoraussetzungen für den Umgang mit Beschäftigtendaten für bestimmte Fälle

Allgemein ist das Ziel zu verfolgen, nicht mehr vorrangig vom Gesetzgeber sehr detailliert vorgegebene Beschreibungen des zulässigen Datenumgangs im Gesetz zu verankern. Das Aufstellen eindeutiger, aber grundsätzlicher Verarbeitungsregeln könnte die Vielzahl verschiedenster Erlaubnistatbestände obsolet machen. Wo es möglich ist, sollte die Kontrolle und Beeinflussung des Datenumgangs durch den Betroffenen selbst erfolgen. Die individuelle Einwilligung sicherte dabei die Selbstbestimmung und sollte die tragende Rolle der Neukonzeption spielen.[968]

Für bestimmte Verarbeitungssituationen könnten jedoch, entgegen dem vorgeschlagenen Prinzip, die Aufnahme konkreter Erlaubnistatbestände und die Präzisierung unbestimmter Rechtsbegriffe zu besserer Rechtsverständlichkeit und damit zu höherer Rechtssicherheit führen. Eine explizite Regelung käme insbesondere für Sachverhalte in Betracht, die als Ausnahmefälle einzuordnen sind.

Begrüßenswert erscheint in diesem Kontext, dass der Gesetzgeber mit § 32i Abs. 2 Satz 2 BDSG-E ausdrücklich die besonderen Verhältnisse in Callcentern berücksichtigt: Hier wurde zutreffend erkannt, dass der Telekommunikation bei Callcen-

[966] S. BT-Drs. 17/4230.
[967] S. BT-Drs. 17/4230.
[968] *Roßnagel*, RDV 2002, 61 (63).

tern im Vergleich zur herkömmlichen betrieblichen oder dienstlichen Nutzung der Telekommunikationseinrichtung ein anderes Gewicht zukommt; bei Callcentern stellt die Telekommunikation der überwiegende und maßgebliche Arbeitsinhalt der Callcenter-Mitarbeiter dar.

Mit der Vorschrift des § 32i Abs. 2 Satz 2 BDSG-E soll ein Zulässigkeitstatbestand im Gesetz manifestiert werden, der Kontrollen in Bezug auf die Telekommunikationsinhalte in beschränktem Umfang und unter bestimmten Voraussetzungen zulässt. Somit ließen sich valide Erkenntnisse im Hinblick auf das Verhalten oder die Leistung der Callcenter-Mitarbeiter gewinnen. Dem berechtigten Kontrollinteresse des Callcenter-Betreibers würde damit adäquat Rechnung getragen. Die in Satz 3 enthaltene Informationspflicht, wonach der Arbeitgeber den kontrollierten Beschäftigten im Nachhinein unmittelbar über den Überwachungsvorgang aufklären muss, diente zusätzlich der Entschärfung des Eingriffs in die Rechte der Callcenter-Mitarbeiter.

8.2.2.2 Festlegung von Kriterien für eine freiwillige Einwilligung

Selbstbestimmtes Handeln setzt voraus, Entscheidungen in eigener Verantwortung treffen zu können. Dies muss auch im Rahmen von Beschäftigungsverhältnissen gelten.

Der zu erwartende Beschäftigtendatenschutz versucht mit § 32l Abs. 1 BDSG-E dem grundsätzlichen Machtungleichgewicht zwischen den Vertragsparteien im Beschäftigungsverhältnis dadurch Rechnung zu tragen, dass die datenschutzrechtliche Einwilligung nur noch in gesetzlich vorgesehenen Fällen möglich sein soll. Dies führte jedoch zu einer faktischen Bevormundung des Betroffenen. Er hätte keine Möglichkeit mehr, Datenverarbeitungsvorgänge seines Arbeitgebers zu legitimieren, die von ihm tatsächlich gewollt oder zu seinem offensichtlichen Vorteil sind. In vielen Fällen würde diese Restriktion zu einer Benachteiligung des Beschäftigten führen. Der Gesetzgeber ist mit dieser geplanten Regelung über sein verfolgtes Ziel hinausgeschossen, die Disparität im Beschäftigungsverhältnis auszugleichen.

Der Gesetzgeber sollte sich darauf beschränken, einen zulässigen Handlungsrahmen vorzugeben, der durch selbstbestimmtes Handeln der beteiligten Akteure ausgefüllt werden kann. Dabei muss lediglich sichergestellt sein, dass tatsächliche Freiwilligkeit bei der Entscheidungsfindung vorliegt.[969] Allgemein sollte die Befugnis, grund-

[969] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 45.

sätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen zu können, nicht nur in den Vordergrund gestellt, sondern zur Grundregel der Datenverarbeitung werden.[970]

Hilfreich in diesem Zusammenhang wären gesetzlich verankerte Kriterien, die die tatsächliche Freiwilligkeit des Einverständnisses absichern. Solche Merkmale lassen sich allerdings schwer konkret festmachen. Denkbar sind zum Beispiel

- *Kompensationsmöglichkeiten:* Der Beschäftigte könnte im Einzelfall einen weiterreichenden Datenumgang, als dieser aufgrund gesetzlicher Erlaubnistatbestände möglich wäre, gestatten, wenn der Eingriff in das Persönlichkeitsrecht des Betroffenen durch Kompensationsmaßnahmen ausgeglichen würde. Beispielsweise könnte der Umgang mit seinen personenbezogenen Daten an anderer Stelle weniger einschneidend ausgestaltet werden, als dies gesetzlich zulässig wäre. Konkret: Der Beschäftigte hätte die Möglichkeit, in einzelne weitergehende Kontrollen durch den Arbeitgeber einzuwilligen, wenn dies zum Wegfall anderer, sonst zusätzlich eingesetzter Überprüfungen führte – eine vergleichbare Eingriffstiefe der Überwachungsmaßnahmen vorausgesetzt. Anhand einer Gesamtbetrachtung müsste sichergestellt werden, dass die Schwere des Eingriffs der intensivierten Kontrollmaßnahme nicht größer ist, als alle anderen – unter normalen Voraussetzungen – durchgeführten Kontrollen in Summe.
- *Entscheidungen zum Vorteil des Beschäftigten:* Einwilligungen müssten stets zulässig sein, wenn sie sich für den Betroffenen offensichtlich als vorteilhaft erweisen. Eine derartige Vorteilhaftigkeit läge bei Einwilligungen vor, die potenziell überhaupt keine Nachteile für den Betroffenen befürchten lassen müssten, oder wenn die Vorteile in einem solchen Maß überwögen, dass eventuelle Nachteile ohne weiteres zu vernachlässigen wären.

Auch die umgekehrte Systematik ist denkbar: So könnte gesetzlich festgelegt werden, dass die Einwilligung – unter dem allgemeinen Freiwilligkeitsvorbehalt – grundsätzlich zulässig ist, auf sie jedoch nur in bestimmten Fällen nicht zurückgegriffen werden darf. Es müsste ein Ausnahmekatalog in die Vorschrift mit aufgenommen werden, unter welchen Bedingungen eine datenschutzrechtliche Einwilligung nicht wirksam erteilt werden kann.

[970] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 72.

8.2.3 Nutzung innerorganisatorischer Regelungsmöglichkeiten

Den betriebs- oder dienststelleninternen Datenschutz mittels Kollektivvereinbarung zu regeln, stellt eine praxisgerechte Möglichkeit dar, die jeweils vorliegenden spezifischen Gegebenheiten adäquat berücksichtigen zu können. Der aktuelle § 4 Abs. 1 BDSG eröffnet eine solche – vom Bundesdatenschutzgesetz abweichende – Regelungsmöglichkeit dadurch, dass unter anderem „andere Rechtsvorschriften" den Umgang mit personenbezogenen Daten erlauben oder anordnen können. Mit dem voraussichtlich zusätzlich im Gesetz aufgenommenen § 4 Abs. 1 Satz 2 BDSG-E würde dies ausdrücklich festgeschrieben. Darüber hinaus enthält § 32l Abs. 3 BDSG-E die Vorgabe, dass die Rechte der Interessenvertretungen der Beschäftigten unberührt bleiben sollen.

Ferner sieht allerdings § 32l Abs. 5 BDSG-E vor, dass ein Abweichen vom Niveau des Beschäftigtendatenschutzes zu Ungunsten der Beschäftigten verboten sein soll. Diese Regelung berücksichtigt zu Recht die oft geübte Praxis, dass im Kontext von Vereinbarungen zu unterschiedlichen Regelungsbereichen der Datenschutz zur Verhandlungsmasse wurde, um an anderer Stelle Vorteile zu erzielen: So könnte etwa ein niedrigeres Datenschutzniveau durch eine höhere Betriebsrente „entschädigt" werden.

Betriebs- oder Dienstvereinbarungen können dazu dienen, abstrakt-generelle Normen auf die spezifischen Gegebenheiten hin zu konkretisieren und damit Rechtsklarheit zu schaffen.[971] Unter Umständen sind hierzu in Detailfragen Alternativen notwendig, die von Vorschriften des Beschäftigtendatenschutzes negativ abweichen. Es sollte daher klargestellt werden, dass ein Abweichen von den Vorschriften des Beschäftigtendatenschutzes – bezogen auf den gesamten Datenschutzstandard, den die Regelungsmaterie bietet – zu Lasten der Beschäftigten verboten ist. Wohl aber sollten im Detail, insbesondere zur Lösung von Einzelfallproblemen, derartige Abweichungen zulässig sein.

8.2.4 Auferlegung von weitergehenden Transparenzpflichten

Zwar unterliegen datenverarbeitende Stellen bereits bestimmten Informationspflichten.[972] Moderne Informationstechnik beinhaltet jedoch immer komplexer werdende Verarbeitungsabläufe, die oftmals selbst von Fachleuten kaum mehr zu durchschau-

[971] So auch BT-Drs. 17/4230, 22.
[972] S. bereits Kapitel 8.1.5 „Transparenz der Datenverarbeitungsprozesse" zu technisch-organisatorischen Vorschlägen, die der Sicherstellung von mehr Transparenz dienen.

en sind. Zu fordern sind daher weitgehende Offenlegungspflichten hinsichtlich der Funktionsweise der Technik für Hersteller und datenverarbeitende Stellen als Technikanwender, die unterschiedliche Techniken so miteinander kombinieren können, dass die Komplexität des Gesamtsystems und die mögliche Gefährdung des informationellen Selbstbestimmungsrechts von Betroffenen sich potenzieren.

Es sollte daher durch unabhängige Kontrollinstanzen überprüfbar sein, welche Datenverarbeitungsprozesse (potenziell) im zu begutachtenden technischen System ablaufen können. Schnittstellen zu anderen Systemen und Menschen müssen in die Betrachtung mit einbezogen werden.[973]

Als kontrollierende Stellen kommen vorrangig der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Landesdatenschutzbeauftragten, die Aufsichtsbehörden für den Datenschutz sowie unabhängige Prüforganisationen, wie der TÜV, in Betracht.

Wenn eine Überprüfung der Technik zu einem positiven Ergebnis führen sollte, könnte diese Tatsache mit einem speziellen Zertifikat „belohnt“ werden, das sich wettbewerbswirksam einsetzen ließe.[974]

Einen weiteren Ansatz zur Erhöhung der datenschutzrechtlichen Transparenz beim Betroffenen böte die Ausdehnung der Informationspflichten der datenverarbeitenden Stelle. Anknüpfungspunkte sollten dabei zum einen die Sensitivität der personenbezogenen Daten, mit denen der Umgang erfolgt, und zum anderen der potenzielle Zugriffsbereich sein.[975] Je sensitiver der Gehalt der Daten ist, desto detaillierter und umfassender sollte die Beschreibung sein, was mit den Daten im Rahmen des Datenverarbeitungsprozesses geschieht. Ebenso sollten die Anforderungen an die Information des Betroffenen in Abhängigkeit von der Anzahl der (potenziell) zugriffsberechtigten Personen steigen.

8.2.5 Überarbeitung des § 9 BDSG

Der § 9 BDSG sowie dessen Anlage betreffen technische und organisatorische Maßnahmen, die der Sicherstellung dienen, dass die im Bundesdatenschutzgesetz

[973] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 88 f.; *Koch*, MMR 1998, 458 (461).
[974] S. zum Datenschutzaudit ausführlich *Roßnagel*, in: Hempel/Krasmann/Bröckling (Hrsg.), Sichtbarkeitsregime, Leviathan Sonderheft 25/2010, 263 ff.
[975] *Baeriswyl*, RDV 2000, 6 (8).

enthaltenen Vorgaben eingehalten werden und die datenverarbeitende Stelle die besonderen Anforderungen des Datenschutzes erfüllen kann.

Positiv zu bewerten ist die Tatsache, dass § 9 BDSG nur solche Vorkehrungen fordert, die verhältnismäßig in Bezug auf ihren Schutzzweck ausfallen. Somit müssen nicht grundsätzlich die wirkungsvollsten und sichersten Maßnahmen getroffen werden; ansonsten entwickelte sich die Einhaltung des Datenschutzes für nichtöffentliche Unternehmen und öffentliche Verwaltungseinheiten zum Kostentreiber.

Die Anlage zu § 9 BDSG enthält eine nicht abschließende Aufzählung, anhand welcher Maßnahmen der Datenschutz sicherzustellen ist. Während die Vorschrift des § 9 BDSG von sowohl technischen als auch organisatorischen Vorkehrungen spricht, findet in ihrer Anlage lediglich die „Organisation“ Erwähnung, an welche die aufgezählten Forderungen zu richten sind; der technische Aspekt bleibt in der Anlage unerwähnt. Dabei sind die Anforderungen insbesondere an die Technik zu stellen: Es müsste klar hervorgehoben werden, dass sich Hersteller und Anwender der Technik an den Vorgaben auszurichten haben.[976]

Der Übersichtlichkeit wäre gedient, wenn die Vorgaben im Anhang zu § 9 BDSG in die Norm selbst mit aufgenommen würden. Überdies ließe sich somit der Eindruck vermeiden, bei dem Anhang handele es sich um weniger verbindliche Forderungen.[977]

Die in der Anlage der Vorschrift enthaltenen Schutzvorkehrungen müssen aufgrund gewachsener Risiken der automatisierten Datenverarbeitung einer grundlegenden Überarbeitung unterzogen werden, die sich an den Schutzzielen der IT-Sicherheit auszurichten hat.[978] Als bedeutende Schutzziele der IT-Sicherheit im Zusammenhang mit der Verarbeitung personenbezogener Daten sind zu nennen:

- Vertraulichkeit,
- Integrität,
- Authentizität,
- Verfügbarkeit,
- Revisionsfähigkeit,
- Datensparsamkeit und

[976] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 25.
[977] *von Stechow*, Datenschutz durch Technik, 2005, 130.
[978] *Ernestus*, RDV 2002, 22.

- Transparenz.[979]

Die sich rasant vollziehende Entwicklung im Bereich der Informationstechnologie birgt ständig neue Gefahren für die informationelle Selbstbestimmung der Betroffenen. Welche Sicherheitsvorkehrungen zu treffen sind, muss anhand einer Gefahrenanalyse evaluiert werden.[980] Um die Notwendigkeit einer fortlaufenden Überprüfung der zu treffenden Sicherheitsmaßnahmen zu verdeutlichen, sollte in der Vorschrift ausdrücklich verankert sein, dass einzuleitende Vorkehrungen dem jeweiligen „Stand der Technik" entsprechen müssen.[981] Mit der Aufnahme dieses unbestimmten Rechtsbegriffs enthielte § 9 BDSG einen dynamischen Maßstab. Der jeweils vorliegende Stand der Technik ist einschlägiger Fachliteratur und Normen zu entnehmen. DIN-Normen und das Grundschutzhandbuch des BSI stellen beispielsweise diesbezügliche Informationsquellen dar.[982]

8.2.6 Verabschiedung des Auditgesetzes

Ein auf freiwilliger Basis durchgeführtes Datenschutzaudit[983], welches der Verbesserung des Datenschutzes und der Datensicherheit dienen soll, kann als werbewirksames „Gütesiegel" eingesetzt werden. § 9a BDSG enthält eine diesbezügliche Vorschrift. Das geplante Auditgesetz[984], auf welches § 9a BDSG verweist (Gesetzesauftrag), konnte am 3. Juli 2009 – wie ursprünglich geplant – nicht verabschiedet werden.

Das Datenschutzaudit bezieht sich auf das Datenschutzmanagement-System der datenverarbeitenden Stelle und besteht in dessen Überprüfung. Idealerweise sollte das Ergebnis in der Bestätigung seinen Niederschlag finden, dass das vorhandene Management-System zur fortlaufenden Verbesserung des innerorganisatorischen

[979] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 129 f.; *Ernestus*, RDV 2000, 146 (148); *Jacob*, DuD 2000, 5 (10); dazu *Bedner/Ackermann*, DuD 2010, 323 ff., die eine Konkretisierung und Fortschreibung der allgemeinen IT-Schutzziele vornehmen.
[980] *Gaycken/Karger*, MMR 2011, 3 (6).
[981] *von Stechow*, Datenschutz durch Technik, 2005, 132; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 130; so sieht beispielsweise § 5 Abs. 3 BlnDSG vor, dass die Ermittlung der notwendigen technischen und organisatorischen Maßnahmen entsprechend der technischen Entwicklung in regelmäßigen Abständen zu wiederholen ist.
[982] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 130.
[983] S. zu diesem Komplex ausführlich *Roßnagel*, Datenschutzaudit, 2000; die Idee der Einführung eines Datenschutzaudits geht zurück auf einen Vorschlag der Projektgruppe verfassungsverträgliche Technikgestaltung (provet), *Roßnagel*, DuD 1997, 505.
[984] BT-Drs. 16/12011.

Datenschutzes führt. Letztendlich soll eine Erhöhung des Datenschutzniveaus durch freiwillige Selbstregulierung erreicht werden.[985]

Trotz der Kernelemente

- Freiwilligkeit,
- Selbstregulierung und
- Wettbewerb

des Datenschutzaudits besteht die Notwendigkeit einer gesetzlichen Regelung. Nur sie vermag zu gewährleisten, dass insbesondere die Bevölkerung Vertrauen in ein Datenschutzauditsiegel aufbauen kann und ein einheitliches Prüfniveau eingehalten wird sowie insgesamt die Zweckerreichung des Verfahrens sichergestellt ist.[986]

Im Ergebnis führte die Etablierung des Datenschutzaudits zu einer höheren Selbstregulierung – und damit auch zu größerer Akzeptanz und zu Wettbewerb im Bereich des Datenschutzes. Für Technikentwickler und -anwender stünden Belohnungen und Anreize anstatt Ge- und Verbote im Vordergrund. Wenn Unternehmen um die Einhaltung des „besten" Datenschutzniveaus konkurrierten, würden die gewünschten Gestaltungsziele quasi von selbst erreicht.[987] Aus diesen Gründen sollte der Gesetzgeber möglichst zeitnah das Datenschutzauditgesetz auf den Weg bringen. Als Vorbild kann das Umweltaudit dienen, das sich für Zertifizierungen auf dem Gebiet der Umweltverantwortung von Unternehmen bewährt hat.[988]

Datenschutzbeauftragte, Aufsichtsbehörden und Datenschutzverbände kommen als unterstützende Institutionen in Betracht. Sie könnten einen konstruktiven Beitrag leisten, indem sie den Unternehmen durch Beratungen und Empfehlungen zur Seite stünden sowie durch die Vergabe von Preisen für herausragende Datenschutzkonzepte Anreize schafften.[989]

Ein datenschutzrechtliches Gütesiegel, mit dem ein das Gesprächsmanagement-System anwendendes Callcenter an die Öffentlichkeit treten könnte, führte mit großer Wahrscheinlichkeit zu einer gesteigerten Akzeptanz bei den Kunden.

---

[985] *Roßnagel*, in: Hempel/Krasmann/Bröckling (Hrsg.), Sichtbarkeitsregime, Leviathan Sonderheft 25/2010, 263 (265); *Karper/Maseberg*, DuD 2010, 704 ff.
[986] *Roßnagel*, in: Hempel/Krasmann/Bröckling (Hrsg.), Sichtbarkeitsregime, Leviathan Sonderheft 25/2010, 263 (275).
[987] *Roßnagel*, MMR 2005, 71 (75); *ders.*, DuD 2000, 231 (232); *Boehme-Neßler*, K&R 2002, 217 (223).
[988] *Roßnagel*, DuD 1997, 505 (506); s. zum Umweltaudit *Langerfeldt*, NVwZ 2002, 1156 ff.
[989] *Roßnagel*, MMR 2005, 71 (75).

9 Schlussbetrachtung

Das Bestreben nichtöffentlicher Unternehmen, ihre Serviceorientierung durch spezialisierte Callcenter-Dienstleistungen zu optimieren, erscheint wegen des ständig wachsenden Wettbewerbsdrucks legitim. Ebenso wollen auch Behörden und öffentliche Organisationen beispielsweise mit erweiterter Erreichbarkeit über telefonische Dienste von Callcentern zur Bürgerfreundlichkeit beitragen.

Als innovative Unterstützung der Callcenter-Mitarbeiter gilt dabei die Nutzung eines Gesprächsmanagement-Systems, das automatisiert die Gesprächsinhalte und den Gesprächskontext analysiert und den Mitarbeitern situationsadäquat weiterführende Informationen am Frontend-System präsentiert. Dadurch können insbesondere komplexe Anliegen und umfangreiche Fragestellungen der Kunden in kurzer Zeit beantwortet werden, was nicht zuletzt zur gesteigerten Zufriedenheit auf beiden Seiten – sowohl aufseiten der Kunden als auch aufseiten der Callcenter-Mitarbeiter – führt.

Neben den unbestreitbaren Vorzügen eines solchen Gesprächsmanagement-Systems bestehen jedoch bei seiner Nutzung zahlreiche Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen. So sind zum einen die Kunden in erheblichem Maße von automatisiert ablaufenden personenbezogenen Datenverarbeitungsprozessen innerhalb des Systems tangiert; gerade die Anbindung des CRM-Systems ermöglicht grundsätzlich die Erstellung von detaillierten Kundenprofilen, die unter Umständen zutreffende Rückschlüsse auf die Persönlichkeit der Kunden erlauben. Zum anderen sind es die Callcenter-Agenten, die aufgrund der Systemeigenschaften potenziell lückenlos in Bezug auf ihr Verhalten oder ihre Leistung überwacht werden können.

Die vorliegende Arbeit zeigt, dass die Einführung und Anwendung eines Gesprächsmanagement-Systems, das den Zweck der situativen Bereitstellung gesprächsrelevanter Informationen für die Callcenter-Mitarbeiter erfüllt, nach dem geltenden Datenschutzrecht – unter Einhaltung der dargelegten Voraussetzungen – zulässig realisierbar sind.

Kernelemente im Hinblick auf die Gestaltung des Gesprächsmanagement-Systems stellen dabei Maßnahmen des Systemdatenschutzes dar: Der Systemdatenschutz gewährleistet durch technische, aber auch organisatorische Vorkehrungen, dass die Grundsätze des Datenschutzes beim normalen Systembetrieb eingehalten werden. Durch rechtsadäquate Technikentwicklung und -implementierung sowie durch den

Einbau von Schutzvorkehrungen lässt sich der bestimmungsgemäße Gebrauch des Techniksystems von vorneherein sicherstellen und diesbezüglicher Kontrollaufwand minimieren.

Eine praktikable Möglichkeit, den innerbetrieblichen oder -behördlichen Datenschutz zu regeln, besteht im Abschluss entsprechender Kollektivvereinbarungen. Diese Vereinbarungen eignen sich als Instrument, den jeweiligen organisatorischen Gegebenheiten gerecht zu werden, die Rechte des Arbeitgebers oder Dienstherrn in Bezug auf Verhaltens- oder Leistungskontrollen konkret festzuschreiben und einen Ausgleich zwischen Arbeitgeber- oder Dienstherrn- und Arbeitnehmerinteressen herbeizuführen.

Neben der Darstellung der rechtlichen Vorgaben für die Einführung und Anwendung des Gesprächsmanagement-Systems wurden technische und organisatorische Vorschläge für Vorkehrungen in diesem System beziehungsweise im Callcenter-Betrieb aufgezeigt, deren Umsetzung einen besseren Datenschutz gewährleisten.

Auch wurden Ansatzpunkte im bestehenden Datenschutzrecht identifiziert, an denen Anpassungen zur Stärkung des informationellen Selbstbestimmungsrechts von Betroffenen beitragen könnten. Allgemein betrachtet bleibt festzustellen, dass die Zahl der personenbezogenen Datenverarbeitungsprozesse mit rasanter Geschwindigkeit zunimmt. Die globale digitale Vernetzung gilt als Grundvoraussetzung für eine Informationsgesellschaft. Zukünftig ist zu erwarten, dass die Datenverarbeitung für Betroffene stetig undurchsichtiger werden wird. Unter dem Schlagwort „Ubiquitous Computing“ werden immer mehr Gegenstände des Alltags mit kleinen Computern ausgestattet, die mit anderen Gegenständen kommunizieren und kontext-sensitiv reagieren können. Gerade derartige verselbstständigte und nicht mehr kontrollierbare Datenverarbeitungsprozesse sind es, die das Datenschutzrecht vor neue Herausforderungen stellen.[990]

Im Rahmen der Untersuchung konnten kritikwürdige Schwachstellen im aktuellen, allerdings auch im geplanten Beschäftigtendatenschutz festgestellt werden. Positiv zu bewerten ist indes die Tatsache, dass sich die Bundesregierung nach jahrzehntelanger „Enthaltsamkeit“ dazu durchringen konnte, einen Gesetzentwurf mit umfassenden Regelungen zum Beschäftigtendatenschutz auf den Weg zu bringen. Einen Impuls dazu haben wohl die „Datenschutzskandale“ der jüngeren Vergangen-

[990] S. dazu ausführlich *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, 133.

heit[991] gegeben; ferner war aufgrund aktueller Fragestellungen zeitnahes Handeln gefragt.

Der aktuelle Datenschutz für Beschäftigte ist von einer erheblichen Rechtszersplitterung geprägt, die sich auch auf zahlreiche Gerichtsentscheidungen erstreckt. Dieser Zustand bringt gravierende Probleme mit sich. Mit den künftigen Regelungen zum Beschäftigtendatenschutz soll eine komplexe Rechtsmaterie in verständliche Gesetzesform gegossen und Rechtssicherheit hergestellt werden. Der Beschäftigtendatenschutz soll dabei Schutz der Beschäftigten vor unrechtmäßiger Erhebung und Verwendung ihrer personenbezogenen Daten sicherstellen, gleichzeitig aber auch dem Informationsinteresse der Arbeitgeber ausreichend Rechnung tragen.[992] Es bleibt abzuwarten, wann die bereichsspezifischen Vorschriften zum Beschäftigtendatenschutz in Kraft treten werden und inwiefern die von vielen Seiten vorgebrachte Kritik[993] in diesen Regelungen Berücksichtigung finden wird.

Nicht zuletzt zeigt die vorliegende Dissertation, dass die Begutachtung von zu konzipierenden Techniksystemen aus dem Blickwinkel des Datenschutzes bereits im Stadium ihrer Entwicklung unnötigen Aufwand und Kosten vermeiden kann. Wird andernfalls beispielsweise erst in der Phase, in der bereits ein Prototyp vorliegt, oder sogar erst dann, wenn das Endprodukt Marktreife erreicht hat, geprüft, ob die rechtlichen Vorgaben eingehalten werden, kann es im Extremfall für Nachbesserungen zu spät sein. Die Konkurrenz hat möglicherweise zwischenzeitlich einen nicht mehr einzuholenden Vorsprung erreicht. Allein aus ökonomischen Erwägungen heraus wäre das verspätete Einbeziehen einer datenschutzrechtlichen Bewertung vollkommen irrational. Generell – also nicht nur bei der Entwicklung neuer Techniken – sollte verstärkt dazu übergegangen werden, innovative Prozesse unter der ständigen juristischen Begleitung zu vollziehen.

[991] So etwa bei Lidl, bei der Deutschen Bahn und bei T-Mobile.
[992] BT-Drs. 17/4230, 1.
[993] S. BT-Drs. 17/4230, 17 ff.; BT-Drs. 17/4853; BT-Drs. 17/69; BT-Drs. 17/121; BT-Drs. 17/779; BT-Drs. 17/7176.

Anhang

Anhangsverzeichnis

Anlage 1: Mustererklärung zur Wahrung des Datengeheimnisses

Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes (BDSG) zur Wahrung des Datengeheimnisses

_____
Name der verantwortlichen Stelle

Sehr geehrte(r) Herr/Frau _____ ,

aufgrund Ihrer Aufgabenstellung verpflichte ich Sie auf die Wahrung des Datengeheimnisses nach § 5 BDSG. Es ist Ihnen nach dieser Vorschrift untersagt, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen das Datengeheimnis können nach §§ 44 und 43 Absatz 2 BDSG sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. In der Verletzung des Datengeheimnisses kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten liegen; ebenso können Schadenersatzansprüche entstehen. Eine sich gegebenenfalls aus dem Arbeitsvertrag oder aus einem sonstigen Dienstvertrag oder aus gesonderten Anweisungen ergebende allgemeine Geheimhaltungsverpflichtung wird durch die vorliegende Erklärung nicht berührt.

Eine unterschriebene Zweitschrift dieser Erklärung geben Sie bitte an die Personalabteilung zurück.

_____ _____
Ort, Datum Unterschrift des Vertretungsberechtigten der verantwortlichen Stelle

Über die Notwendigkeit der gewissenhaften Einhaltung des Datengeheimnisses und die sich daraus für meine Aufgabenerfüllung ergebenden Verhaltensweisen wurde ich umfassend unterrichtet.

_____ _____
Ort, Datum Unterschrift der/des Verpflichteten

Quelle: in Anlehnung an *Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*, Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes (BDSG) zur Wahrung des Datengeheimnisses (abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/Verpflichtungserklaerung/VerpflichtungDatengeheimnis.pdf).

Anlage 2: Mustervereinbarung zur Auftragsdatenverarbeitung

Hinweis: *Die nachfolgende Mustervereinbarung dient der Veranschaulichung, wie eine Vereinbarung über eine Auftragsdatenverarbeitung zwischen einem Unternehmen (Auftraggeber) und einem Callcenter (Auftragnehmer) exemplarisch aussehen kann. Eine solche Vereinbarung muss abhängig von den Umständen des konkreten Einzelfalls getroffen werden. Bei komplexen Auftragsverhältnissen oder der Verarbeitung besonders schützenswerter personenbezogener Daten im Auftrag werden weitere Vertragsbestimmungen notwendig sein.*

Auftrag gemäß § 11 BDSG

Vereinbarung

zwischen der

Beispiel KG.....
- nachstehend Auftraggeber genannt -

und dem

Muster-Callcenter
GmbH.....
- nachstehend Auftragnehmer genannt -

1 Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung ..... vom ....., auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung“).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

……
(Aufzählung und Beschreibung der Aufgaben)

Dauer des Auftrags

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum.....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von vier Wochen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2 Konkretisierung des Auftragsinhalts

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

☐ Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers: .....

Die Verarbeitung oder Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b und 4c BDSG erfüllt sind.

Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Gegenstand der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung und Beschreibung der Datenarten/-kategorien):

- □ Personenstammdaten
- □ Vertragsstammdaten (Vertragsbeziehung, Produkt- oder Vertragsinteresse)
- □ Anrufhistorie
- □ Angaben zum Grund der jeweiligen Anrufe der Kunden
- □ ...

Kreis der Betroffenen

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung und Beschreibung der betroffenen Personenkategorien):

- □ Kunden
- □ Interessenten
- □ Abonnenten
- □ Ansprechpartner
- □ ...

3 Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Ist der Auftraggeber einverstanden, werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots. Auftragsspezifische Maßnahmen, besonders im Hinblick auf die Art des Datenaustauschs, auf die Bereitstellung von Daten, auf die Art und Umstände der Verarbeitung und auf die Datenhaltung können – soweit sie sich nicht aus der vorliegenden Vereinbarung ergeben – wie folgt gesondert beschrieben werden:

.....

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

4 Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5 Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zur Einhaltung der Regelungen dieses Auftrags insbesondere folgende Pflichten:

- ⇨ schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- ⇨ Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- und Zweckbindung belehrt werden.
- ⇨ Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und dessen Anlage.
- ⇨ unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.
- ⇨ Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen im Hinblick auf die Vertragsausführung und -erfüllung, insbesondere bezüglich der Einhaltung der Regelungen und Maßnahmen zur Durchführung des Auftrags und Vornahme gegebenenfalls notwendiger Anpassungen.

6 Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- ⇨ Die Einschaltung von Unterauftragnehmern ist nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.
- ⇨ Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- ⇨ Bei der Unterauftragsvergabe sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i. V. m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen zum Beispiel Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigung, Prüfungen oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7 Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen von der Einhaltung der Regelungen dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (zum Beispiel von Datenschutzauditoren) oder einer Bescheinigung über eine geeignete Zertifizierung (zum Beispiel BSI-Grundschutz) erbracht werden.

8 Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach § 42a BDSG, § 15a TMG und § 93 Abs. 3 TKG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9 Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ord-

nungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10 Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder nach Aufforderung durch den Auftraggeber, spätestens jedoch nach Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

_____	_____
Unterschrift des Vertretungsberechtigten des Auftraggebers	Unterschrift des Vertretungsberechtigten des Auftragnehmers

Quelle: in Anlehnung an *Gesellschaft für Datenschutz und Datensicherheit e. V.*, Muster zur Auftragsdatenverarbeitung gemäß § 11 BDSG, o. J.

Anlage 3: Formular zur Bestellung des Datenschutzbeauftragten

Bestellung zur/zum Datenschutzbeauftragten

Sehr geehrte(r) Frau/Herr _____,

mit Wirkung vom _____ bestelle ich Sie zur/zum Datenschutzbeauftragten.

In dieser Funktion sind Sie der Geschäftsleitung/Behördenleitung unmittelbar unterstellt. Ihre Aufgabe ist es, unbeschadet der eigenen Datenschutzverantwortung der jeweiligen Organisationseinheiten, durch Beratung und jederzeitige auch unangemeldete Kontrolle auf die Einhaltung des Bundesdatenschutzgesetzes sowie anderer Rechtsvorschriften über den Datenschutz hinzuwirken. Im Einzelnen ergibt sich die Aufgabe aus § 4g BDSG. Sie sind bei der Erfüllung Ihrer Aufgabe von allen Mitarbeiterinnen und Mitarbeitern zu unterstützen.

Alle Mitarbeiterinnen und Mitarbeiter des Betriebs/der Behörde können sich in Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an Sie wenden.

Mit freundlichen Grüßen

_____
(Unterschrift des Vertretungsberechtigten
der Geschäftsleitung/Behördenleitung)

_____
(Unterschrift des zukünftigen Datenschutzbeauftragten)

Quelle: in Anlehnung an *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 32.

Anlage 4: Muster eines Verfahrensverzeichnisses für nichtöffentliche Stellen

Verfahrensverzeichnis nach § 4e BDSG

1 Angaben zur verantwortlichen Stelle

Name/Firma der verantwortlichen Stelle	
Straße	
PLZ und Ort	
Telefon- und Faxnummer	
E-Mail-Adresse	
Internet-Adresse	

2 Angaben zu Leitungspersonen

2.1 Inhaber, Vorstände, Geschäftsführer oder sonstige Personen der Unternehmensleitung

2.2 Leiter der Datenverarbeitung

2.3 Leitender Datenschutzbeauftragter

Name	
Straße	
PLZ und Ort	
Telefon- und Faxnummer	
E-Mail-Adresse	
Internet-Adresse	

3 Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung

Das Unternehmen erhebt, verarbeitet oder nutzt personenbezogene Daten zu folgenden Zwecken:

4 Beschreibung der betroffenen Personengruppen und Daten oder Datenkategorien

betroffene Personengruppen	diesbezügliche Daten oder Datenkategorien

5 Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

6 Regelfristen für die Löschung der Daten

7 Geplante Datenübermittlung in Drittstaaten

Name des Drittstaates	
Empfänger oder Kategorien von Empfängern	
Art der betroffenen Daten oder Datenkategorien	

8 Angaben zu den Sicherheitsmaßnahmen gemäß § 9 BDSG

8.1 Art der zu schützenden personenbezogenen Daten oder Datenkategorien

8.2 Umsetzung der Schutzmaßnahmen

Zutrittskontrolle	
Zugangskontrolle	
Zugriffskontrolle	
Weitergabekontrolle	
Eingabekontrolle	
Auftragskontrolle	
Verfügbarkeitskontrolle	
Trennungsgebot	

Quelle: in Anlehnung an *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl. 2008, 34 ff.

Literaturverzeichnis

Abel, Ralf,
Der behördliche Datenschutzbeauftragte, MMR 2002, 289-294.

Abel, Ralf,
Rechtsfragen von Scoring und Rating, RDV 2006, 108-115.

Albrecht, Florian,
Datenschutz im Arbeitsverhältnis: Die Neuregelung des § 32 BDSG, jurisPR-ITR 20/2009, 1-5.

Altenburg, Stephan/von Reinersdorff, Wolfgang/Leister, Thomas,
Betriebsverfassungsrechtliche Aspekte der Telekommunikation am Arbeitsplatz, MMR 2005, 222-226.

Ambs, Friedrich [ehem. Erbs, Georg/Kohlhaas, Max] (Hrsg.),
Strafrechtliche Nebengesetze, 179. Ergänzungslieferung, München 2010 (zitiert als: *Bearbeiter*, in: Erbs/Kohlhaas).

Ascheid, Reiner/Preis, Ulrich/Schmidt, Ingrid (Hrsg.),
Kündigungsrecht. Großkommentar zum gesamten Recht der Beendigung von Arbeitsverhältnissen, 3. Aufl., München 2007.

Auernhammer, Herbert,
Die Aufsichtsbehörde nach § 38 BDSG, DuD 1992, 621-626.

Aufhauser, Rudolf,
Das deutsche Bundesrecht, BildscharbV, Baden-Baden 2011.

Baeriswyl, Bruno,
Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?, RDV 2000, 6-11.

Bake, Christian/Blobel, Bernd/Münch, Peter (Hrsg.),
Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen. Spezielle Probleme des Datenschutzes und der Datensicherheit im Bereich des Gesundheits- und Sozialwesens (GSW) in Deutschland, 3. Aufl., Frechen 2009.

Barton, Dirk,
Betriebliche Übung und private Nutzung des Internetarbeitsplatzes – „Arbeitsrechtliche Alternativen" zur Wiedereinführung der alleinigen dienstlichen Verwendung, NZA 2006, 460-466.

Bauer, Hans/Grether, Mark,
CRM für öffentliche Verwaltungen, in: Hippner, Hajo/Wilde, Klaus (Hrsg.), Management von CRM-Projekten. Handlungsempfehlungen und Branchenkonzepte, Wiesbaden 2004, 347-368.

Baumeister, Klaus,
Informationsquelle Funkverkehr: Strafbarkeitsrisiken erläutert am Beispiel Polizeifunk und unter besonderer Berücksichtigung von Art. 5 Abs. 1 GG, ZUM 2000, 114-126.

Baumgärtner, Johannes/Behrmann, Henning/Denecke, Hans Peter/Frahm, Jörg/Koch, Holger/Kramer, Philipp/Kroschel, Jutta,
Customer Relationship Management und Datenschutz, DSB 4/2004, 9.

Bausewein, Christoph,
Der sachliche Anwendungsbereich des BDSG im Beschäftigtendatenschutz. Reichweite des § 32 Abs. 2 BDSG, DuD 2011, 94-97.

Beckhusen, Michael,
Das Scoring-Verfahren der SCHUFA im Wirkungsbereich des Datenschutzrechts, BKR 2005, 335-344.

Beckschulze, Martin/Henkel, Wolfram,
Der Einfluss des Internets auf das Arbeitsrecht, DB 2001, 1491-1506.

Bedner, Mark/Ackermann, Tobias,
Schutzziele der IT-Sicherheit, DuD 2010, 323-328.

Behling, Thorsten,
Compliance versus Fernmeldegeheimnis. Wo liegen die Grenzen bei E-Mail-Kontrollen als Antikorruptionsmaßnahme?, BB 2010, 892-896.

Beisenherz, Gerhard/Tinnefeld, Marie-Theres,
Aspekte der Einwilligung. Zivil- und strafrechtliche Bezüge der Einwilligung im Datenschutzrecht, DuD 2011, 110-115.

Bergmann, Lutz/Möhrle, Roland/Herb, Armin,
Datenschutzrecht. Kommentar, Stuttgart, München, Hannover, Berlin, Weimar, Dresden, Band 1, 42. Ergänzungslieferung, Stand: Januar 2011 (zitiert als: *Bergmann/Möhrle/Herb*, BDSG).

Berkowsky, Wilfried,
Die verhaltensbedingte Kündigung – Teil 2, NZA-RR 2001, 57-76.

Bernhardt, Marion/Barthel, Thomas,
Beispiel unerlaubte Internetnutzung. Die außerordentliche Tat- und Verdachtskündigung, AuA 2008, 150-153.

Besgen, Nicolai/Prinz, Thomas,
Dienstliche und private Nutzung von Internet, Intranet und E-Mail – Individualarbeitsrecht, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.), Neue Medien und Arbeitsrecht. Internet, E-Mail und andere moderne Kommunikationsmittel, Bonn 2006, 37-82.

Besgen, Nicolai/Prinz, Thomas,
Internet, Intranet und E-Mail – Kollektives Arbeitsrecht, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.), Neue Medien und Arbeitsrecht. Internet, E-Mail und andere moderne Kommunikationsmittel, Bonn 2006, 83-118.

Bizer, Johann,
Die angekündigte Datenschutzkontrolle, DuD 2000, 673.

Bizer, Johann,
Sieben Goldene Regeln des Datenschutzes, DuD 2007, 350-356.

Bizer, Johann/Kamp, Meike/Bock, Kirsten/Körffer, Barbara/Janneck, Kai/Leopold, Nils/Möller, Jan/Rost, Martin,
Erhöhung des Datenschutzniveaus zugunsten der Verbraucher. Studie im Auftrag des BMELV, Kiel 2006.

Blomeyer, Wolfgang,
Das Günstigkeitsprinzip in der Betriebsverfassung – Die Betriebsvereinbarung zwischen Individual- und Tarifvertrag, NZA 1996, 337-346.

Boehme-Neßler, Volker,
Datenschutz in der Informationsgesellschaft. Vom Datenschutzrecht zum Informationswirtschaftsrecht, K&R 2002, 217-224.

Böker, Karl-Hermann/Kamp, Lothar,
Betriebliche Nutzung von Internet, Intranet und E-Mail. Analyse und Handlungsempfehlungen, Frankfurt 2003.

Bösing, Sebastian,
Authentifizierung und Autorisierung im elektronischen Rechtsverkehr. Qualifizierte Signaturschlüssel- und Attributszertifikate als gesetzliche Instrumente digitaler Identität, Baden-Baden 2005.

Boewer, Dietrich,
Die Bedeutung des § 94 BetrVG für die DV-gestützte Personaldatenverarbeitung, RDV 1988, 13-20.

Braun-Lüdicke, Sebastian,
Der Konzerndatenschutzbeauftragte. Eine Analyse der rechtlichen und praktischen Bedeutung, Wiesbaden 2008.

Brisch, Klaus/Laue, Philip,
Unified Communications – Rechtliche Stolpersteine auf dem Weg zur einheitlichen Unternehmenskommunikation, MMR 2009, 813-818.

Büllesbach, Alfred,
Das neue Bundesdatenschutzgesetz, NJW 1991, 2593-2600.

Büllesbach, Alfred,
Datenschutz bei Data Warehouses und Data Mining, CR 2000, 11-17.

Büllesbach, Alfred/Rieß, Joachim,
Outsourcing in der öffentlichen Verwaltung, NVwZ 1995, 444-449.

Bull, Hans Peter,
Entscheidungsfragen in Sachen Datenschutz, ZRP 1975, 7-13.

Bull, Hans Peter,
Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, NJW 2006, 1617-1624.

Bull, Hans Peter,
Die „völlig unabhängige" Aufsichtsbehörde. Zum Urteil des EuGH vom 9.3.2010 in Sachen Datenschutzaufsicht, EuZW 2010, 488-494.

Bundesamt für Sicherheit in der Informationstechnik (BSI),
IT-Grundschutz-Kataloge (abrufbar unter: https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/m/m06/m06032.html).

Busse, Julia,
Datenschutz, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.), Neue Medien und Arbeitsrecht. Internet, E-Mail und andere moderne Kommunikationsmittel, Bonn 2006, 341-399.

CAS Software AG,
Datenschutz mit CAS genesisWorld, Karlsruhe, Stand: Juli 2010.

Däubler, Wolfgang,
Verschlechterung der Arbeitsbedingungen durch Betriebsvereinbarung?, ArbuR 1984, 1-28.

Däubler, Wolfgang,
Nutzung des Internet durch Arbeitnehmer, K&R 2000, 323-327.

Däubler, Wolfgang,
Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht, NZA 2001, 874-881.

Däubler, Wolfgang,
Internet und Arbeitsrecht, 3. Aufl., Frankfurt 2004.

Däubler, Wolfgang,
Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., Frankfurt 2010.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo,
Bundesdatenschutzgesetz. Kompaktkommentar zum BDSG, 3. Aufl., Frankfurt 2010 (zitiert als: D/K/W/W).

Dann, Matthias/Gastell, Roland,
Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, NJW 2008, 2945-2949.

Dannhorn, Melanie/Mohnke, Lars,
Call-Center. Arbeitnehmer-Monitoring, AuA 2006, 210-213.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Die Datenschutzbeauftragten in Behörde und Betrieb, 7. Aufl., Bonn 2008.
Deutsch, Markus/Diller, Martin,
Die geplante Neuregelung des Arbeitnehmerdatenschutzes in § 32 BDSG, DB 2009, 1462-1465.
Ditscheid, Alexander/Ufer, Frederic,
Die Novellierung des TKG 2009 – ein erster Überblick, MMR 2009, 367-372.
Dölling, Dieter/Duttge, Gunnar/Rössner, Dieter (Hrsg.),
Gesamtes Strafrecht. StGB, StPO, Nebengesetze. Handkommentar, Baden-Baden 2008 (zitiert als: HK-GS/*Bearbeiter*).
Dörner, Klemens,
Die Verdachtskündigung im Spiegel der Methoden zur Auslegung von Gesetzen, NZA 1992, 865-873.
Dreier, Horst (Hrsg.),
Grundgesetz-Kommentar, Band I, 2. Aufl., Tübingen 2004.
Duhr, Elisabeth/Naujok, Helga/Peter, Martina/Seiffert, Evelyn,
Neues Datenschutzrecht für die Wirtschaft. Erläuterungen und praktische Hinweise zu § 1 bis § 11 BDSG, DuD 2002, 5-36.
Duisberg, Alexander/Picot, Henriette,
Rechtsfolgen von Pannen in der Datensicherheit, CR 2009, 823-828.
Eckert, Claudia,
IT-Sicherheit. Konzepte – Verfahren – Protokolle, 6. Aufl., München 2009.
Eckert, Michael,
Keine Kontrolle des Betriebsrats durch den betrieblichen Datenschutzbeauftragten, DStR 1998, 1691.
Eckhardt, Jens,
Wie weit reicht der Schutz des Fernmeldegeheimnisses (Art. 10 GG)? Zugleich Anmerkung zu BVerfG, Urt. v. 2.3.2006, 2 BVR 2099/04, DuD 2006, 365-368.
Elbel, Thomas,
Zur Abgrenzung von Auftragsdatenverarbeitung und Übermittlung, RDV 2010, 203-209.
Elschner, Günter,
Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, Lohmar, Köln 2004.

Engelien-Schulz, Thomas,
Die Vorabkontrolle gemäß § 4d Abs. 5 und Abs. 6 Bundesdatenschutzgesetz (BDSG) – für die oder den behördliche/n Datenschutzbeauftragte/n eine neue Aufgabe, für die Leitung einer datenschutzrechtlich verantwortlichen Stelle und das dort wahrzunehmende Datenschutzmanagement eine neue Richtschnur?, RDV 2003, 270-278.

Engelien-Schulz, Thomas,
Zu den Prinzipien und Grundsätzen des bereichsspezifischen und allgemeinen Datenschutzrechts, VR 2009, 366-374.

Engelien-Schulz, Thomas,
Zur Bedeutung und Ausgestaltung der datenschutzrechtlichen Einwilligungserklärung für öffentliche Stellen, VR 2009, 73-79.

Engelien-Schulz, Thomas,
Zu den Anforderungen an eine Datenerhebung, -verarbeitung und -nutzung im Auftrag für öffentliche Stellen des Bundes, VR 2010, 361-369.

Engelien-Schulz, Thomas,
Einrichtung automatisierter Abrufverfahren – Zu den allgemeinen datenschutzrechtlichen Anforderungen für öffentliche Stellen des Bundes, VR 2011, 1-8.

Epping, Volker/Hillgruber, Christian (Hrsg.),
Beck'scher Online-Kommentar Grundgesetz, Ed. 11, Stand: 1. Juli 2011 (zitiert als: BeckOK/*Bearbeiter*, GG).

Erfurth, René,
Der „neue" Arbeitnehmerdatenschutz im BDSG, NJOZ 2009, 2914-2927.

Erler, Andreas,
Die private Nutzung neuer Medien am Arbeitsplatz, München 2003.

Ernestus, Walter,
Bedarf die Anlage zu § 9 BDSG einer Modernisierung?, RDV 2000, 146-149.

Ernestus, Walter,
„... da waren's nur noch 8!", RDV 2002, 22-25.

Ernst, Stefan,
Der Arbeitgeber, die E-Mail und das Internet, NZA 2002, 585-591.

Ernst, Stefan,
Gleichklang des Persönlichkeitsschutzes im Bild- und Tonbereich?, NJW 2004, 1277-1279.

Ernst, Stefan,
Interessenkonflikt bei Personalunion zwischen Revisionsabteilung und Datenschutzbeauftragtem, NJOZ 2010, 2443-2446.

Europäisches Parlament,
Charta der Grundrechte der Europäischen Union (abrufbar unter: http://www.europarl.europa.eu/charter/default_de.htm).

Europarat,
Der Europarat in Kürze (abrufbar unter: http://www.coe.int/aboutCoe/index.asp?page=nepasconfondre&l=de und http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=de).

Fabricius, Nicolai,
Die Mitbestimmung des Betriebsrats bei der Umsetzung des neuen Arbeitsschutzrechts, BB 1997, 1254-1258.

Fitting, Karl/Engels, Gerd/Schmidt, Ingrid/Trebinger, Yvonne/Linsenmaier, Wolfgang,
Handkommentar zum Betriebsverfassungsgesetz, 25. Aufl., München 2010 (zitiert als: *Fitting et al.*, HK BetrVG).

Fleischmann, Michael,
Betriebliche Übung zur Privatnutzung üblicher elektronischer Kommunikationsmittel – Erwiderung auf *Koch*, NZA 2008, 911, NZA 2008, 1397.

Forst, Gerrit,
Wie viel Arbeitnehmerdatenschutz erlaubt die EG-Datenschutzrichtlinie?, RDV 2010, 150-155.

Franzen, Martin,
Die Zulässigkeit der Erhebung und Speicherung von Gesundheitsdaten der Arbeitnehmer nach dem novellierten BDSG, RDV 2003, 1-6.

Franzen, Martin,
Arbeitnehmerdatenschutz – rechtspolitische Perspektiven, RdA 2010, 257-263.

Freund, Ferdinand/Knoblauch, Rolf/Eisele, Daniela,
Praxisorientierte Personalwirtschaftslehre, 6. Aufl., Stuttgart 2003.

Frosch-Wilke, Dirk,
Data Warehouse, OLAP und Data Mining. State of the Art und zukünftige Entwicklungen, DuD 2003, 597-604.

Gabel, Detlev,
Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten, BB 2009, 2045-2049.

Garstka, Hansjürgen,
Informationelle Selbstbestimmung und Datenschutz. Das Recht auf Privatsphäre (abrufbar unter: http://www.bpb.de/files/YRPN3Y.pdf).

Garstka, Hansjürgen,
Datenschutzkontrolle: Das Berliner Modell, DuD 2000, 289-291.

Gaycken, Sandro/Karger, Michael,
Entnetzung statt Vernetzung – Paradigmenwechsel bei der IT-Sicherheit, MMR 2011, 3-8.

Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.),
Beck'scher TKG-Kommentar, 3. Aufl., München 2006 (zitiert als: *Bearbeiter*, in: Beck'scher TKG-Kommentar).

Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD),
Muster zur Auftragsdatenverarbeitung gemäß § 11 BDSG, o. J.

Giesen, Thomas,
Rechtsstellung, Aufgaben und Befugnisse der Datenschutzkontrollstellen nach Art. 28 der EG-Datenschutzrichtlinie, RDV 1998, 15-19.

Gliss, Hans,
Lehren aus Datenmissbräuchen: Vom Umgang mit Call-Centern, DSB 11/2008, 8-11.

Gliss, Hans/Kramer, Philipp,
Arbeitnehmerdatenschutz. Aktionsfelder für Betriebsräte, Frankfurt 2006.

Gola, Peter,
Mitbestimmung bei technischen Überwachungseinrichtungen. Voraussetzungen und Reichweite, ArbuR 1988, 105-114.

Gola, Peter,
Neuer Tele-Datenschutz für Arbeitnehmer? Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 1999, 322-330.

Gola, Peter,
Die Erhebung und Verarbeitung „besonderer Arten personenbezogener Daten" im Arbeitsverhältnis, RDV 2001, 125-127.

Gola, Peter,
Informationelle Selbstbestimmung in Form des Widerspruchsrechts, DuD 2001, 278-281.

Gola, Peter,
Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, RDV 2002, 109-116.

Gola, Peter,
Das Mithören und Aufzeichnen von Call Center-Telefonaten, RDV 2005, 105-111.

Gola, Peter,
Datenschutz im Call Center. Anforderungen an Wirtschaft und öffentliche Verwaltung, 2. Aufl., Frechen 2006.
Gola, Peter,
Datenschutz und Multimedia am Arbeitsplatz. Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 3. Aufl., Heidelberg, München, Landsberg, Frechen, Hamburg 2010.
Gola, Peter/Klug, Christoph,
Grundzüge des Datenschutzrechts, München 2003.
Gola, Peter/Klug, Christoph,
Neuregelungen zur Bestellung betrieblicher Datenschutzbeauftragter, NJW 2007, 118-122.
Gola, Peter/Reif, Yvette,
Kundendatenschutz. Leitfaden für die Praxis, hrsg. v. Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD)/Zentralverband der deutschen Werbewirtschaft e. V. (ZAW), 3. Aufl., Heidelberg 2011.
Gola, Peter/Schomerus, Rudolf,
BDSG-Kommentar, 10. Aufl., München 2010.
Gola, Peter/Wronka, Georg,
Arbeitnehmerdatenverarbeitung beim Betriebs-/Personalrat und der Datenschutz, NZA 1991, 790-795.
Gola, Peter/Wronka, Georg,
Handbuch zum Arbeitnehmerdatenschutz. Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 4. Aufl., Frechen 2008.
Gräff, Johannes/Günzel, Hermann,
Datensicherung – Anmerkungen zum Löschen personenbezogener Daten durch Vernichtung der Datenträger, DuD 1990, 77-80.
Grentzenberg, Verena/Schreibauer, Marcus/Schuppert, Stefan,
Die Datenschutznovelle (Teil II). Ein Überblick zum „Gesetz zur Änderung datenschutzrechtlicher Vorschriften“, K&R 2009, 535-543.
Grobys, Marcel,
Die Überwachung von Arbeitnehmern in Call Centern, Baden-Baden 2007.
Gröseling, Nadine/Höfinger, Frank Michael,
Hacking und Computerspionage – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 549-553.
Grosskreutz, Henrik/Lemmen, Benedikt/Rüping, Stefan,
Privacy-Preserving Data-Mining, Informatik Spektrum 2010, 380-383.

Gurlit, Elke,
Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035-1041.

Hahn, Oliver,
Data Warehousing und Data Mining in der Praxis, DuD 2003, 605-608.

Hammer, Volker/Pordesch, Ulrich/Roßnagel, Alexander,
Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, Berlin, Heidelberg, New York 1993.

Hammer, Volker/Roßnagel, Alexander,
Datensicherung in ISDN-Telefonanlagen, DuD 1990, 394-406.

Hanau, Peter/Hoeren, Thomas,
Private Internetnutzung durch Arbeitnehmer. Die arbeits- und betriebsverfassungsrechtlichen Probleme, München 2003.

Hanebeck, Alexander/Neunhoeffer, Friederike,
Anwendungsbereich und Reichweite des telekommunikationsrechtlichen Fernmeldegeheimnisses – Rechtliche Schwierigkeiten bei der Anwendung des TKG, K&R 2006, 112-115.

Hanloser, Stefan,
Die BDSG-Novelle II: Neuregelungen zum Kunden- und Arbeitnehmerdatenschutz, MMR 2009, 594-599.

von Hase, Karl,
Fristlose Kündigung und Abmahnung nach neuem Recht, NJW 2002, 2278-2283.

Haug, Thomas,
Stellen Anrufe zu Zwecken der Kundenzufriedenheitsermittlung oder der Werbezustellungskontrolle Telefonwerbung dar?, K&R 2010, 767-770.

Hecker, Manfred,
Neue Regeln gegen unerlaubte Telefonwerbung, K&R 2009, 601-606.

Heckmann, Dirk,
Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für ein IT-Sicherheitsrecht, MMR 2006, 280-285.

Heghmanns, Michael/Niehaus, Holger,
Datenschutz und strafrechtliche Risiken beim Outsourcing durch private Versicherungen, wistra 2008, 161-167.

Heghmanns, Michael/Niehaus, Holger,
Outsourcing im Versicherungswesen und der Gehilfenbegriff des § 203 III 2 StGB, NStZ 2008, 57-62.

Heidemann-Peuser, Helke,
Rechtskonforme Gestaltung von Datenschutzklauseln. Erkenntnisse aus der Praxis der AGB-Verbandsklage, DuD 2002, 389-394.
Heinemann, Oliver/Wäßle, Florian,
Datenschutzrechtlicher Auskunftsanspruch bei Kreditscoring - Inhalt und Grenzen des Auskunftsanspruchs nach § 34 BDSG, MMR 2010, 600-604.
Helfrich, Marcus,
Haftung des betrieblichen Datenschutzbeauftragten, CR 1992, 456-461.
Herb, Armin,
Die Struktur der Datenschutzkontrollstellen in der Bundesrepublik, ZUM 2004, 530-532.
Herzog, Roman/Scholz, Rupert/Herdegen, Matthias/Klein, Hans [ehem. Maunz, Theodor/Dürig, Günter] (Hrsg.),
Grundgesetz. Kommentar, Loseblatt, Band I und II, München, 61. Ergänzungslieferung, Stand: Januar 2011 (zitiert als: Maunz/Dürig-*Bearbeiter*, GG).
Heun, Sven-Erik (Hrsg.),
Handbuch Telekommunikationsrecht, 2. Aufl., Köln 2007.
Hilbrans, Sönke,
Beschäftigtendatenschutz und betriebliche Telefonanlagen. Kritische Anmerkung zum Entwurf eines § 32i BDSG, AuR 2010, 424-426.
Hladjk, Jörg,
Online-Profiling und Datenschutz. Eine Untersuchung am Beispiel der Automobilindustrie, Baden-Baden, 2007.
Höfling, Wolfram/Burkiczak, Christian,
Das Günstigkeitsprinzip - ein grundrechtsdogmatischer Zwischenruf, NJW 2005, 469-473.
Höld, Florian,
Die Überwachung von Arbeitnehmern. Nicht-technische Überwachungsmethoden, technische Überwachungsmethoden und ärztliche Untersuchungen, Hamburg 2006.
Hoenike, Mark/Hülsdunk, Lutz,
Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung?, MMR 2004, 788-792.
Hoeren, Thomas,
Grundzüge des Internetrechts. E-commerce, Domains, Urheberrecht, 2. Aufl., München 2002.
Hoeren, Thomas,
Das neue BDSG und die Auftragsdatenverarbeitung, DuD 2010, 688-691.

Hoeren, Thomas,
Luftverkehr, Check-In und Pass-/Personalausweisdaten, NVwZ 2010, 1123-1127.

Hoeren, Thomas/Sieber, Ulrich (Hrsg.),
Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, 28. Ergänzungslieferung, München 2011.

Hornung, Gerrit,
Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, 3-8.

Hornung, Gerrit,
Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005.

Hornung, Gerrit,
Informationen über „Datenpannen" – Neue Pflichten für datenverarbeitende Unternehmen, NJW 2010, 1841-1845.

Hornung, Gerrit/Steidle, Roland,
Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotenzial, AuR 2005, 201-207.

Hoss, Dennis,
Internet- und E-Mail-Überwachung am Arbeitsplatz, Kassel 2009.

Hoss, Dennis,
Callcenter: Mitarbeiterkontrollen auf dem datenschutzrechtlichen Prüfstand, 2010 (abrufbar unter: http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2010050732848/3/HossCallcenter.pdf).

Hoss, Dennis,
Auskunftsrecht des Betroffenen aus § 34 Abs. 1 BDSG in der Praxis: wirksames Instrument oder zahnloser Tiger?, RDV 2011, 6-11.

Hümmerich, Klaus/Boecken, Winfried/Düwell, Franz Josef (Hrsg.),
AnwaltKommentar Arbeitsrecht, Band 2, Bonn 2008 (zitiert als: AnwK-ArbR/*Bearbeiter*).

Hunold, Wolf,
Die Rechtsprechung zur Abmahnung, NZA-RR 2000, 169-175.

Iraschko-Luscher, Stephanie,
Einwilligung – ein stumpfes Schwert des Datenschutzes?, DuD 2006, 706-710.

Iraschko-Luscher, Stephanie/Kiekenbeck, Pia,
Welche Krankheitsdaten darf der Arbeitgeber von seinem Mitarbeiter abfragen?, NZA 2009, 1239-1242.

Jacob, Joachim,
Perspektiven des neuen Datenschutzrechts. Zur Zukunft des Bundesdatenschutzgesetzes, DuD 2000, 5-11.

Jacob, Joachim/Jost, Tanja,
Marketingnutzung von Kundendaten und Datenschutz – ein Widerspruch? Die Bildung von Konsumentenprofilen auf dem datenschutzrechtlichen Prüfstand, DuD 2003, 621-624.

Jandach, Thomas,
Datenschutzmaßnahmen beim Outsourcing der Bürokommunikation. Technisch-organisatorische Anforderungen, DuD 2001, 224-227.

Joecks, Wolfgang,
Strafgesetzbuch. Studienkommentar, 8. Aufl., München 2009.

Joecks, Wolfgang/Miebach, Klaus (Hrsg.),
Münchener Kommentar zum Strafgesetzbuch, Band 3, München 2003 (zitiert als: MüKo-StGB/*Bearbeiter*).

Jordan, Christopher/Bissels, Alexander/Löw, Christine,
Arbeitnehmerkontrolle im Call-Center durch Silent Monitoring und Voice Recording, BB 2008, 2626-2631.

Jürgens, Uwe,
Die Vernichtung von Datenträgern mit personenbezogenen medizinischen Daten, DuD 1998, 449-454.

Jürgens, Uwe,
Grenzen für Videoüberwachung, Data-Warehousing und Data-Mining, DSB 4/2000, 8.

Karper, Irene/Maseberg, Sönke,
Zertifikat für Datenschutz-Management, DuD 2010, 704-708.

Kettlitz, Eberhardt,
„Hier Amt, was beliebt?“. Geschichte und Geschichten der Callcenter in Deutschland, Halle 2008.

Kilian, Wolfgang,
Rechtliche Aspekte bei Verwendung von Patientenchipkarten, NJW 1992, 2313-2317.

Kilian, Wolfgang/Heussen, Benno (Hrsg.),
Computerrechts-Handbuch. Informationstechnologie in der Rechts- und Wirtschaftspraxis, 29. Ergänzungslieferung, München, Stand: Februar 2011.

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich (Hrsg.),
Kommentar zum Strafgesetzbuch, Band 2, 3. Aufl., Baden-Baden 2010 (zitiert als: NK-StGB-*Bearbeiter*).

Kläver, Magdalene,
Der Schutz des nichtöffentlich gesprochenen Wortes. Zugleich eine Anmerkung zur beim BGH anhängigen Entscheidung des OLG Koblenz (Az.: 8 U 1967/99), DuD 2003, 228-233.

Klebe, Thomas,
Mitbestimmung bei technischer Überwachung, NZA 1985, 44-47.

Klein, Karsten,
Zur datenschutzrechtlichen Relevanz des Scorings von Kreditrisiken, BKR 2003, 488-491.

Klett, Detlef/Hilberg, Söntje Julia,
Die neue DIN-Spezifikation für das Outsourcing – Inhalt und praktische Anwendung, CR 2010, 417-421.

Klug, Christoph,
Die Vorabkontrolle – Eine neue Aufgabe für betriebliche und behördliche Datenschutzbeauftragte, RDV 2001, 12-20.

Klumpp, Dieter/Kubicek, Herbert/Roßnagel, Alexander (Hrsg.),
next generation information society? Notwendigkeit einer Neuorientierung, Mössingen-Talheim 2003.

Koch, Christian,
Scoring-Systeme in der Kreditwirtschaft - Einsatz unter datenschutzrechtlichen Aspekten, MMR 1998, 458-462.

Koch, Frank,
Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel, NZA 2008, 911-916.

Köhler, Helmut,
Neue Regelungen zum Verbraucherschutz bei Telefonwerbung und Fernabsatzverträgen, NJW 2009, 2567-2572.

Koeppen, Thomas,
Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz. Deutschland, Großbritannien und USA im Vergleich, Hamburg 2007.

Körffer, Barbara,
Datenschutzrechtliche Anforderungen an Kundenbindungssysteme, DuD 2004, 267-271.

Körner, Marita,
Moderner Datenschutz für die Beschäftigten: Ein Ende der Skandale? Gutachten zum Regierungsentwurf zur Regelung des Beschäftigtendatenschutzes, Frankfurt 2010, (abrufbar unter: www.hugo-sinzheimer-institut.de/fileadmin/user_data_hsi/Dokumente/Gutachten_Arbeitnehmerdatenschutz_HSI.pdf).

Körner-Damman, Maria,
Datenschutzprobleme beim Praxisverkauf, NJW 1992, 1543-1545.
Kollmer, Norbert/Klindt, Thomas (Hrsg.),
Arbeitsschutzgesetz. Kommentar, 2. Aufl., München 2011.
Kort, Michael,
Die Auswirkungen des neuen Bundesdatenschutzgesetzes auf die Mitbestimmung im Arbeitsrecht, RdA 1992, 378-386.
Kraemer, Dieter/Kaufung, Harald,
Bürgerämter sind nur der Anfang, VR 2000, 200-206.
Kramer, Bernhard,
Heimliche Tonbandaufnahmen im Strafprozeß, NJW 1990, 1760-1764.
Kramer, Philipp/Herrmann, Michael,
Auftragsdatenverarbeitung. Zur Reichweite der Privilegierung durch den Tatbestand des § 11 Bundesdatenschutzgesetz, CR 2003, 938-941.
Kramer, Stefan,
Internetnutzung als Kündigungsgrund, NZA 2004, 457-464.
Kruse, Hans Ludwig,
Das Informationsrecht der Personalvertretung, Der Personalrat 1993, 64-71.
Kühling, Jürgen/Bohnen, Simon,
Zur Zukunft des Datenschutzrechts – Nach der Reform ist vor der Reform, JZ 2010, 600-610.
Lackner, Karl/Kühl, Kristian,
Kommentar zum StGB, 26. Aufl., München 2007 (zitiert als: *Lackner/Kühl*, StGB).
Lambrich, Thomas/Cahlik, Nina,
Austausch von Arbeitnehmerdaten in multinationalen Konzernen – Datenschutz- und betriebsverfassungsrechtliche Rahmenbedingungen –, RDV 2002, 287-299.
Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,
Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes (BDSG) zur Wahrung des Datengeheimnisses (abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/Verpflichtungserklaerung/VerpflichtungDatengeheimnis.pdf).
Langerfeldt, Michael,
Das novellierte Umweltauditgesetz, NVwZ 2002, 1156-1164.
Langkeit, Jochen,
Umfang und Grenzen der ärztlichen Schweigepflicht gemäß § 203 I Nr. 1 StGB, NStZ 1994, 6-9.

Langner, Sören/Witt, Boris,
Aktuelles zur Verdachtskündigung, DStR 2008, 825-830.
Latendorf, Michael/Rademacher, Axel,
Betriebsvereinbarungen als andere Rechtsvorschriften. Widersprüchliche Rechtsprechung des BAG zur Ausweitung des § 3 S. 1 Ziff. 1 BDSG, CR 1989, 1105- 1108.
Laue, Philip,
Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung. Rechtliche Rahmenbedingungen und Gestaltungsanforderungen, Kassel 2010.
Lelley, Jan Tibor,
Internet am Arbeitsplatz. Arbeitsrechtliche Grundlagen zur Vermeidung von unerwünschter Privatnutzung und Missbrauchsfällen, hrsg. v. Worzalla, Michael, Berlin 2006.
Lensdorf, Lars,
Auftragsdatenverarbeitung in der EU/EWR und Unterauftragsdatenverarbeitung in Drittländern. Besonderheiten der neuen EU-Standardvertragsklauseln, CR 2010, 735-741.
Lettl, Tobias,
Rechtsfragen des Direktmarketings per Telefon und e-mail, GRUR 2000, 977-984.
von Lewinski, Kai,
Persönlichkeitsprofile und Datenschutz bei CRM, RDV 2003, 122-132.
Lindner, Christian,
Persönlichkeitsrecht und Geo-Dienste im Internet – z. B. Google Street View/Google Earth, ZUM 2010, 292-301.
Link, Jörg/Gary, Alexander,
Grundlagen und rechtliche Aspekte von Kundendatenbanken (abrufbar unter: http://www.marketing-boerse.de/fachartikel/details/grundlagen-und-rechtliche-aspekte-von-kundendatenbanken/14366).
Linnenkohl, Karl/Rauschenberg, Hans-Jürgen/Schütz, Regina,
Auf dem Wege zu einem „kollektiven Datenschutz“? Gedanken zum Beschluß des Bundesarbeitsgerichts vom 27. Mai 1986 über die Mitbestimmung bei Telefondatenerfassung, BB 1987, 1454-1456.
Linnenkohl, Karl/Schütz, Regina,
Anm. zum BAG-Urt. v. 22.10.1986, RDV 1987, 129-136.
Linnenkohl, Karl/Schütz, Regina/Rauschenberg, Hans-Jürgen,
Unterscheidung zwischen „Verhaltens- und Leistungs-“ sowie „anderen“ oder „persönlichen“ Daten bei moderner Informationsverarbeitung, NZA 1986, 769-772.

Löwisch, Manfred,
Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle, DB 2009, 2782-2787.

Lorenz, Stephan,
Arbeitsrechtlicher Aufhebungsvertrag, Haustürwiderrufsgesetz und „undue influence“, JZ 1997, 277-282.

Lüderssen, Klaus,
Gesprächskontrollen im Call Center. Schutz der Kunden durch Straf- und Ordnungswidrigkeitenrecht?, wistra 2006, 441-446.

Marcks, Peter/Neumann, Dirk/Bleutge, Peter/Böhme, Ralph/Fuchs, Bärbel/Gotthardt, Michael/Kahl, Georg/Schönleiter, Ulrich/Stenger, Anja,
Gewerbeordnung. Kommentar, Band I, 57. Ergänzungslieferung, München, Stand: 1. Juli 2010 (zitiert als: *Bearbeiter*, in: Landmann/Rohmer, GewO).

Maties, Martin,
Änderung des BDSG, RdA 2009, 261-262.

Mattl, Tina,
Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz: unter besonderer Berücksichtigung der Vorgaben des Telekommunikationsgesetzes, Hamburg 2008.

Mengel, Anja,
Kontrolle der Telefonkommunikation am Arbeitsplatz. Wege durch einen juristischen Irrgarten?, BB 2004, 1445-1453

Menzel, Hans-Joachim,
Datenschutzrechtliche Einwilligungen. Plädoyer für eine Rückkehr zur Selbstbestimmung, DuD 2008, 400-408.

Menzler-Trott, Eckart,
Mitarbeiterdatenschutz im Call Center und entsprechende Regelungen in Betriebsvereinbarungen – Ein Praxisbericht, RDV 1999, 257-263.

Menzler-Trott, Eckart/Hasenmaile, Christa,
Arbeitnehmer im Call-Center. Situation – Rechte – Gestaltungsmöglichkeiten, Frankfurt 2000.

Mester, Britta Alexandra,
Arbeitnehmerdatenschutz – Notwendigkeit und Inhalt einer gesetzlichen Regelung, Edewecht 2008.

Mester, Britta Alexandra,
Reform des Beschäftigtendatenschutzes, DuD 2011, 79.

Meyer, Jürgen (Hrsg.),
Kommentar zur Charta der Grundrechte der Europäischen Union, Baden-Baden 2003.

Möller, Frank,
Data Warehouse als Warnsignal an die Datenschutzbeauftragten, DuD 1998, 555-560.

Möller, Jan/Florax, Björn-Christoph,
Kreditwirtschaftliche Scoring-Verfahren - Verbot automatisierter Einzelentscheidungen gem. § 6a BDSG, MMR 2002, 806-810.

Möller, Jan/Florax, Björn-Christoph,
Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken?, NJW 2003, 2724-2726.

Möncke, Ulrich,
Data Warehouses – eine Herausforderung für den Datenschutz?, DuD 1998, 561-569.

Moll, Wilhelm (Hrsg.),
Münchener Anwaltshandbuch Arbeitsrecht, 2. Aufl., München 2009 (zitiert als: Moll/*Bearbeiter*, MAH Arbeitsrecht).

Moos, Flemming,
Entwicklung eines supra- und internationalen Rechtsrahmens für das Internet, in: Kröger, Detlef/Gimmy, Marc André (Hrsg.), Handbuch zum Internetrecht. Electronic Commerce – Informations-, Kommunikations- und Mediendienste, 2. Aufl., Berlin, Heidelberg, New York, Barcelona, Hongkong, London, Mailand, Paris, Tokio 2002, 757-797.

Moos, Flemming,
Unzulässiger Handel mit Persönlichkeitsprofilen? Erstellung und Vermarktung kommerzieller Datenbanken mit Personenbezug, MMR 2006, 718-723.

Moos, Flemming,
Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010. Die wesentlichen Neuerungen und Kritikpunkte im Überblick, CR 2010, 281-286.

Müglich, Andreas,
Datenschutzrechtliche Anforderungen an die Vertragsgestaltung beim eShop-Hosting – Anspruch, Wirklichkeit und Vollzugsdefizit, CR 2009, 479-484.

Müller, Gerd,
Einrichtung von Bürgerbüros/Verbesserung der Dienstleistungsorientierung, DÖD 2000, 16-22.

Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid (Hrsg.),
Erfurter Kommentar zum Arbeitsrecht, 11. Aufl., München 2011 (zitiert als: ErfK/*Bearbeiter*).

Neuhaus, Kai-Jochen/Kloth, Andreas,
Gesundheitsdaten(schutz) im Versicherungsrecht – Der aktuelle Stand, NJW 2009, 1707-1711.

Niese, Marcus,
Die faktische Sicherstellung der Unabhängigkeit der Datenschutzbeauftragten im Bund und in den Ländern – eine rechtsvergleichende Übersicht –, DuD 1994, 635-638.

Oberwetter, Christian,
Arbeitnehmerrechte bei Lidl, Aldi & Co., NZA 2008, 609-613.

OECD,
About the Organisation for Economic Co-operation and Development (OECD), (abrufbar unter: http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html).

Oecking, Christian/Westerhoff, Thomas,
Erfolgsfaktoren langfristiger Outsourcing-Beziehungen, in: Köhler-Frost, Wilfried (Hrsg.), Outsourcing. Schlüsselfaktoren der Kundenzufriedenheit, 5. Aufl., Berlin 2005, 35-52.

Ohly, Ansgar/Sosnitza, Olaf,
Gesetz gegen den unlauteren Wettbewerb. Kommentar, 5. Aufl., München 2010 (zitiert als: *Bearbeiter*, in: Piper/Ohly/Sosnitza).

Olbert, Hans,
Recht im Call Center. Vertragsgestaltung, Wettbewerbsrecht, Datenschutz, Arbeitsrecht, Heidelberg 2001.

Opfermann, Rainer/Rückert, Anette,
Sicherheit und Gesundheitsschutz bei der Arbeit – Neuregelungen zur Tätigkeit an Bildschirmgeräten, AuA 1997, 69-72.

o. V.,
CTI - Computer Telephony Integration (abrufbar unter: http://www.elektronik-kompendium.de/sites/kom/0603051.htm).

o. V.,
Datenschutzgerechtes eGovernment (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/egovern/egovern.pdf).

o. V.,
Vom Bürgerbüro zum Internet. - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung - (abrufbar unter: http://www.datenschutz.hessen.de/download.php?download_ID=140).

o. V.,
Vorhabensbeschreibung des Forschungsprojekts SIGMUND, 2008.

o. V.,
Direkt Marketing 12/2009, 01/2010, 22.

Pahlen-Brandt, Ingrid,
Sind Datenschutzbeauftragte zahnlose Papiertiger? Von der Unwirksamkeit der Datenschutzkontrolle in Deutschland, DuD 2007, 24-28.

Panzer, Andrea,
Mitarbeiterkontrolle und neue Medien, Frankfurt, Berlin, Bern, Brüssel, New York, Oxford, Wien 2004.

Pauly, Stephan/Jankowski, Julia,
Rechtliche Aspekte der Telefonwerbung im B-to-B-Bereich, GRUR 2007, 118-124.

Peifer, Markus,
Neue Regeln für die Datennutzung zu Werbezwecken – Die Reform des BDSG, MMR 2010, 524-527.

Petri, Thomas,
Inhaltliche Anforderungen an die Verfahrensübersicht nach §§ 4g Absatz 2, 4e BDSG als Grundlage für ein effektives Datenschutzmanagement, RDV 2003, 267-270.

Petri, Thomas,
Sind Scorewerte rechtswidrig?, DuD 2003, 631-636.

Petri, Thomas/Kieper, Marcus,
Datenbevorratungs- und -analysesysteme in der Privatwirtschaft, DuD 2003, 609-613.

Petri, Thomas/Tinnefeld, Marie-Theres,
Völlige Unabhängigkeit der Datenschutzkontrolle - Demokratische Legitimation und unabhängige parlamentarische Kontrolle als moderne Konzeption der Gewaltenteilung, MMR 2010, 157-161.

Pflüger, Norbert,
Die Hinzuziehung eines Sachverständigen gem. § 80 III BetrVG, NZA 1988, 45-49.

Piltz, Gisela/Holländer, Corinna,
Scoring als modernes Orakel von Delphi - Wie die geplante Änderung des Bundesdatenschutzgesetzes (BDSG) Transparenz und Rechtssicherheit schaffen will, ZRP 2008, 143-146.

Plath, Kai-Uwe/Frey, Anna-Mirjam,
Direktmarketing nach der BDSG-Novelle: Grenzen erkennen, Spielräume optimal nutzen, BB 2009, 1762-1768.

Podlech, Adalbert/Pfeifer, Michael,
Die informationelle Selbstbestimmung im Spannungsverhältnis zu modernen Werbestrategien, RDV 1998, 139-154.

Pulte, Peter,
Beteiligungsrechte des Betriebsrates außerhalb der Betriebsverfassung, NZA 1996, 913-920.

Raatz, Günther,
Personalleitung und Betriebsverfassung. Aufgaben und Verfahren nach dem neuen Betriebsverfassungsgesetz, DB 1972, 1-4.

Räther, Philipp,
Datenschutz und Outsourcing, DuD 2005, 461-466.

Raffler, Andrea/Hellich, Peter,
Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-e-mails zulässig?, NZA 1997, 862-868.

Ranke, Johannes,
M-Commerce und seine rechtsadäquate Gestaltung. Vorschläge für vertrauenswürdige mobile Kommunikationsnetze und -dienste, Baden-Baden 2004.

Rasmussen, Heike,
Der Schutz medizinischer Daten im Sozialdatenschutz, NZS 1998, 67-73.

Rath, Michael/Karner, Sophia,
Private Internetnutzung am Arbeitsplatz – rechtliche Zulässigkeit und Kontrollmöglichkeiten des Arbeitgebers, K&R 2007, 446-452.

Rehberg, Jan,
Kosten sparen ist Hauptmotiv, Personalmagazin 11/2009, 63-65.

Rengier, Rudolf,
Strafrecht. Besonderer Teil II. Delikte gegen die Person und die Allgemeinheit, 10. Aufl., München 2009.

Reska, Reinhild,
Call Center. Analyse und Handlungsempfehlungen, Frankfurt 2006.

Richardi, Reinhard,
Eingriff in eine Arbeitsvertragsregelung durch Betriebsvereinbarung, RdA 1983, 201-217.

Richardi, Reinhard,
Zum Verhältnis zwischen Betriebsverfassungs- und Personalvertretungsrecht, Der Personalrat 1993, 49-54.

Richardi, Reinhard (Hrsg.),
Kommentar zum Betriebsverfassungsgesetz, 12. Aufl., München 2010.

Richardi, Reinhard/Dörner, Hans-Jürgen/Weber, Christoph (Hrsg.),
Kommentar zum Personalvertretungsrecht, 3. Aufl., München 2008.

Richardi, Reinhard/Wlotzke, Otfried/Wißmann, Hellmut/Oetker, Hartmut (Hrsg.),
Münchener Handbuch zum Arbeitsrecht, 3. Aufl., München 2009 (zitiert als: MHA/*Bearbeiter*).

Riegel, Reinhard,
Entfernung und Vernichtung von Vermerken aus der Ausländerakte, NJW 1984, 2194-2195.

Röller, Jürgen [ehem. Küttner, Wolfdieter](Hrsg.),
Personalbuch 2011. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, 18. Aufl., München 2011 (zitiert als: Küttner/*Bearbeiter*, *Stichwort*).

Rolfs, Christian/Giesen, Richard/Kreikebohm, Ralf/Udsching, Peter (Hrsg.),
Beck'scher Online-Kommentar Arbeitsrecht, BetrVG, Ed. 20, Stand: 1. Juni 2011 (zitiert als: BeckOK/*Bearbeiter*, BetrVG).

Rose, Edgar,
Betriebsvereinbarung, DuD 2011, 136.

Roßnagel, Alexander,
Datenschutz bei Praxisübergabe, NJW 1989, 2303-2309.

Roßnagel, Alexander,
Das Recht auf (tele-)kommunikative Selbstbestimmung, KJ 1990, 267-289.

Roßnagel, Alexander,
Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin, Baden-Baden 1993.

Roßnagel, Alexander,
Datenschutz-Audit, DuD 1997, 505-515.

Roßnagel, Alexander,
Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger. Thesen zur Änderung der Staatsaufgaben in einer „civil information society", ZRP 1997, 26-30.

Roßnagel, Alexander,
Datenschutz in globalen Netzen. Das TDDSG – ein wichtiger erster Schritt, DuD 1999, 253-257.

Roßnagel, Alexander,
Audits stärken Datenschutzbeauftragte. Replik zum Beitrag „Datenschutzaudit" von Drews und Kranz, DuD 2000, 231-232.

Roßnagel, Alexander,
Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung, Braunschweig, Wiesbaden 2000.

Roßnagel, Alexander,
Modernisierung des Datenschutzrechts – Empfehlungen eines Gutachtens für den Bundesinnenminister, RDV 2002, 61-70.

Roßnagel, Alexander,
20 Jahre Volkszählungsurteil, MMR 2003, 693-694.

Roßnagel, Alexander (Hrsg.),
Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

Roßnagel, Alexander,
Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71-75.
Roßnagel, Alexander,
Datenschutz in der künftigen Verkehrstelematik, NZV 2006, 281-288.
Roßnagel, Alexander,
Datenschutz in einem informatisierten Alltag, Berlin 2007.
Roßnagel, Alexander,
Konflikte zwischen Informationsfreiheit und Datenschutz?, MMR 2007, 16-21.
Roßnagel, Alexander,
Die Novellen zum Datenschutzrecht – Scoring und Adresshandel, NJW 2009, 2716-2722.
Roßnagel, Alexander,
Datenschutzaudit – ein modernes Steuerungsinstrument, in: Hempel, Leon/Krasmann, Susanne/Bröckling, Ulrich (Hrsg.), Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 25/2010, 263-280.
Roßnagel, Alexander,
Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes?, in: Eifert, Martin/Hoffmann-Riem, Wolfgang (Hrsg.), Innovation, Recht und öffentliche Kommunikation, Berlin 2011, 41-66.
Roßnagel, Alexander/Jandt, Silke,
Rechtskonformes Direktmarketing – Gestaltungsanforderungen und neue Strategien für Unternehmen MMR 2011, 86-91.
Roßnagel, Alexander/Knopp, Michael,
Mobilisierte Verwaltung: Perspektiven und rechtlicher Gestaltungsbedarf, DÖV 2006, 982-988.
Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen,
Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.
Roßnagel, Alexander/Scholz, Philip,
Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721-731.
Roßnagel, Alexander/Wedde, Peter/Hammer, Volker/Pordesch, Ulrich,
Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen 1990.

Roth, Birgit,
Organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten. Vorgaben der Anlage zu § 9 Satz 1 BDSG, ITRB 2010, 60-63.

Runge, Gerd,
Datengeheimnis und Mitarbeiterschulung. Eine Betrachtung zur Rolle des Menschen in der Praxis des Datenschutzes, DuD 1993, 321-324.

Runkler, Thomas,
Data Mining. Methoden und Algorithmen intelligenter Datenanalyse, Wiesbaden 2010.

Sachs, Michael (Hrsg.),
Grundgesetz-Kommentar, 2. Aufl., München 1999.

Säcker, Franz Jürgen/Rixecker, Roland (Hrsg.),
Münchener Kommentar zum Bürgerlichen Gesetzbuch, 5. Aufl., München 2010 (zitiert als: MüKo-BGB/*Bearbeiter*).

Sassenberg, Thomas/Bamberg, Niclas,
Betriebsvereinbarung contra BDSG?, DuD 2006, 226-229.

Schaar, Peter,
Persönlichkeitsprofile im Internet, DuD 2001, 383-388.

Schaffland, Hans-Jürgen/Wiltfang, Noeme,
Kommentar zum Bundesdatenschutzgesetz, Berlin, Stand: April 2011.

Scheja, Gregor,
Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank. Eine Untersuchung unter besonderer Berücksichtigung der §§ 4b, 4c BDSG, Baden-Baden 2006.

Schierbaum, Bruno,
Behördlicher Datenschutzbeauftragter und Personalrat – doppelter Kontrollauftrag bei der Verarbeitung von Beschäftigtendaten, Der Personalrat 2001, 454-462.

Schild, Hans-Hermann,
Meldepflichten und Vorabkontrolle, DuD 2001, 282-286.

Schild, Hans-Hermann,
Die völlige Unabhängigkeit der Aufsichtsbehörden aus europarechtlicher Sicht, DuD 2010, 549-553.

Schill, Alexander/Springer, Thomas,
Verteilte Systeme. Grundlagen und Basistechnologien, Berlin, Heidelberg, New York 2007.

Schmidl, Michael,
Aspekte des Rechts der IT-Sicherheit, NJW 2010, 476-481.

Schmitt, Holger Erik,
CRM-Systeme in der öffentlichen Verwaltung. Eine Analyse von Einsatzpotentialen mit Schwerpunkt A2C, Berlin 2003.

Schönfeld, Anja/Strese, Franziska/Flemming, Anne,
Ausgewählte Probleme der Nutzung des Internet im Arbeitsleben, MMR-Beil. 2001, 8-13.

Schuler, Karin,
Gesetz zum Beschäftigtendatenschutz, DuD 2011, 126-128.

Schultz, Alexander,
Neue Strafbarkeiten und Probleme – Der Entwurf des Strafrechtsänderungsgesetzes (StrafÄndG) zur Bekämpfung der Computerkriminalität vom 20.09.2006, MIR 2006, Dok. 180, Rn. 1-52.

Schulz, Gabriel/Waldenspuhl, Andreas/Hermerschmidt, Sven,
Data Warehouse und Data Mining im öffentlichen Bereich. Datenschutzrechtliche und -technische Aspekte, 2002, (abrufbar unter: http://www.lfd.m-v.de/dschutz/informat/dwh/dwh.pdf).

Schulze, Reiner (Hrsg.),
Bürgerliches Gesetzbuch. Handkommentar, 6. Aufl., Baden-Baden 2009 (zitiert als: HK-BGB/*Bearbeiter*).

Schumann, David,
Anonymität bewahrendes Data Mining, DuD 2010, 709-712.

Schumann, Kay,
Das 41. StrÄndG zur Bekämpfung der Computerkriminalität, NStZ 2007, 675-680.

Schwarz, Gerd,
Outsourcing: Eine Einführung, in: Hermes, Heinz-Josef/Schwarz, Gerd (Hrsg.), Outsourcing. Chancen und Risiken, Erfolgsfaktoren, rechtssichere Umsetzung, Freiburg, Berlin, München, Zürich 2005, 15-38.

Schwenke, Matthias Christoph,
Individualisierung und Datenschutz. Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung, Wiesbaden 2006.

Seifert, Bernd,
Videoüberwachung im künftigen Beschäftigtendatenschutzrecht. Was bleibt, was geht, was kommt?, DuD 2011, 98-109.

Siegmund, Carsten,
Einführung in Text Mining, in: Witte, René/Mülle, Jutta (Hrsg.), Text Mining: Wissensgewinnung aus natürlichsprachigen Dokumenten, Karlsruhe 2006, 41-58.

Siemen, Birte,
Datenschutz als europäisches Grundrecht, Berlin 2006.
Simitis, Spiros,
Datenschutz – Rückschritt oder Neubeginn??, NJW 1998, 2473-2479.
Simitis, Spiros,
Die betrieblichen Datenschutzbeauftragten – Zur notwendigen Korrektur einer notwendigen Kontrollinstanz, NJW 1998, 2395-2398.
Simitis, Spiros (Hrsg.),
Kommentar zum Bundesdatenschutzgesetz, 6. Aufl., Baden-Baden 2006 (zitiert als: Simitis/*Bearbeiter*, BDSG, 6. Aufl. 2006).
Simitis, Spiros (Hrsg.),
Kommentar zum Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011 (zitiert als: Simitis/*Bearbeiter*, BDSG, 7. Aufl. 2011).
Spielmann, Dean,
Das anwaltliche Berufsgeheimnis in der Rechtsprechung des EGMR, AnwBl 2010, 373-380.
Spindler, Gerald/Schuster, Fabian (Hrsg.),
Recht der elektronischen Medien, 2. Aufl., München 2011 (zitiert als: *Bearbeiter*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, *BDSG*).
von Stechow, Constantin,
Datenschutz durch Technik. Rechtliche Förderungsmöglichkeiten von Privacy Enhancing Technologies am Beispiel der Videoüberwachung, Wiesbaden 2005.
Steidle, Roland,
Multimedia-Assistenten im Betrieb. Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme, Wiesbaden 2005.
Stein, Torsten/von Buttlar, Christian,
Völkerrecht, 11. Aufl., Köln, Berlin, München 2005.
Sutschet, Holger,
Auftragsdatenverarbeitung und Funktionsübertragung, RDV 2004, 97-104.
Taeger, Jürgen,
CRM und Datenschutz – stirbt der Datenschutz im Data Warehouse?, in: Schubert, Sigrid/Reusch, Bernd/Jesse, Norbert (Hrsg.), Informatik bewegt. Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e. V. (GI), Bonn 2002, 537-545.

Taeger, Jürgen,
Kundenprofile im Internet. Customer Relationship Management und Datenschutz, K&R 2003, 220-227.
Taeger, Jürgen,
Datenschutz im Versandhandel: Übermittlung von Kundendaten mit positivem Bonitätswert, BB 2007, 785-790.
Taeger, Jürgen/Gabel, Detlev (Hrsg.),
Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Frankfurt 2010.
Tanenbaum, Andrew/van Steen, Maarten,
Verteilte Systeme. Prinzipien und Paradigmen, 2. Aufl., München, Boston, San Francisco, Harlow, Don Mills, Sydney, Mexico City, Madrid, Amsterdam 2007.
Tettinger, Peter/Wank, Rolf,
Gewerbeordnung. Kommentar, 7. Aufl., München 2004.
Thannheiser, Achim,
Personalrat und neue Technologien (3), Computer Fachwissen 3/1999, 13-18.
Thüsing, Gregor,
Vom Ende einer betrieblichen Übung, NZA 2005, 718-723.
Thüsing, Gregor,
Datenschutz im Arbeitsverhältnis – Kritische Gedanken zum neuen § 32 BDSG, NZA 2009, 865-870.
Thüsing, Gregor,
Licht und Schatten im Entwurf eines neuen Beschäftigtendatenschutzgesetzes, RDV 2010, 147-149.
Thüsing, Gregor/Forst, Gerrit,
Der geplante Beschäftigtendatenschutz: Strenger oder großzügiger als das geltende Recht?, RDV 2011, 163-170.
Tillenburg, Gereon,
Stimmt die Stimme? Biometrielösungen am Arbeitsplatz, DuD 2011, 197-199.
Timner, Hanno/Schreier, Michael,
Der neue Beschäftigtendatenschutz, AuA Sonderausgabe 2010, 4-7.
Tinnefeld, Marie-Theres/Ehmann, Eugen/Gerling, Rainer,
Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht, 4. Aufl., München 2005.

Tinnefeld, Marie-Theres/Petri, Thomas/Brink, Stefan,
Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz. Eine erste Analyse und Bewertung, MMR 2010, 727-735.

Tonner, Klaus/Reich, Anke,
Die Entwicklung der wettbewerbsrechtlichen Beurteilung der Telefonwerbung, VuR 2009, 95-103.

Trappehl, Bernhard/Schmidl, Michael,
Arbeitsrechtliche Konsequenzen von IT-Sicherheitsverstößen, NZA 2009, 985-990.

Trittin, Wolfgang/Fischer, Esther,
Datenschutz und Mitbestimmung. Konzernweite Personaldatenverarbeitung und die Zuständigkeit der Arbeitnehmervertretung, NZA 2009, 343-346.

Tuchbreiter, Stephan,
Beteiligungsrechte des Betriebsrats bei der Einführung und Anwendung moderner Kommunikationsmittel, Hamburg 2007.

United Nations,
UN at a Glance (abrufbar unter: http://www.un.org/en/aboutun/index.shtml).

Urban, Arnd/Roßnagel, Alexander/Jandt, Silke/Löhle, Stephan/Groh, Henriette/Wilke, Daniel,
RFID zur Weiterentwicklung der Kreislaufwirtschaft: datenschutzgerecht Ressourcen schonen, Marburg 2011.

Vander, Sascha,
Auftragsdatenverarbeitung 2.0? Neuregelungen der Datenschutznovelle II im Kontext von § 11 BDSG, K&R 2010, 292-298.

Vassilaki, Irini,
Das 41. StrÄndG – Die neuen strafrechtlichen Regelungen und ihre Wirkung auf die Praxis, CR 2008, 131-136.

Vietmeyer, Katja/Byers, Philipp,
Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis – Geplante BDSG-Novelle lässt Anwendbarkeit des TKG im Arbeitsverhältnis unangetastet, MMR 2010, 807-811.

Vogel, Florian/Glas, Vera,
Datenschutzrechtliche Probleme unternehmensinterner Ermittlungen, DB 2009, 1747- 1754.

Vogelgesang, Klaus,
Mitbestimmung bei Datenerhebung und EDV-Einführung in Behörden, CR 1992, 405-412.

Voigt, Paul,
Gesprächsaufzeichnungen im Servicecallcenter – Opt-In oder Opt-Out? Eine datenschutzrechtliche Betrachtung, DuD 2008, 780-784.

Volkmann, Christian/Gaßmann, Raphael,
Urheberrechtsverletzung durch Umgehung technischer Schutzmaßnahmen – „Session-ID". Zugleich Kommentar zu BGH, 29.4.2010 – I ZR 39/08, K&R 2010, 802 ff. (Heft 12), K&R 2011, 30-31.

Volle, Peter,
Datenschutz als Drittwirkungsproblem: Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beim Customer Relationship Management, Diss. 2007.

Wäßle, Florian/Heinemann, Oliver,
Scoring im Spannungsfeld von Datenschutz und Informationsfreiheit. Rechtliche Rahmenbedingungen für den Einsatz von Scoringverfahren nach der Novellierung des Bundesdatenschutzgesetzes, CR 2010, 410-416.

Wagner, Joachim,
Betriebsrat und betrieblicher Datenschutzbeauftragter – wer kontrolliert wen?, BB 1993, 1729-1734.

von Wallenberg, Gabriela,
Ist das Telefonmarketing gegenüber Verbrauchern tot?, BB 2009, 1768-1773.

Waltermann, Raimund,
Die betriebliche Übung, RdA 2006, 257-269.

Waltermann, Raimund,
Anspruch auf private Internetnutzung durch betriebliche Übung?, NZA 2007, 529-533.

Wanagas, Susanne,
Ein Jahr BDSG-Novelle II – Rückblick unter besonderer Berücksichtigung der Fragen der Auftragsdatenverarbeitung und der Informationspflichten, DStR 2010, 1908-1911.

Weber, Jürgen/Jacob, Harald/Rieß, Joachim/Ullmann, Alfons,
Neue Wege der Kundenbindung aus Datenschutzsicht: Bonuskarten-Systeme, DuD 2003, 614-620.

Weber, Juliane,
Mit undurchsichtigen Methoden zum durchsichtigen Verbraucher? Eine wettbewerbsrechtliche Analyse neuer Marketingmethoden zur gezielten Verbraucherwerbung im Internet, DuD 2003, 625-630.

Wedde, Peter,
Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht, DuD 2004, 169-174.

Wedde, Peter,
Schutz vor verdeckten Kontrollen im Arbeitsverhältnis. Die höchstrichterliche Rechtsprechung, DuD 2004, 21-26.

Weichert, Thilo,
Datenschutzrechtliche Anforderungen an Data-Warehouse-Anwendungen bei Finanzdienstleistern, RDV 2003, 113-122.

Weichert, Thilo,
Kundenbindungssysteme – Verbraucherschutz oder der gläserne Konsument, DuD 2003, 161-168.

Weichert, Thilo,
Auskunftsanspruch in verteilten Systemen. Zur Einschaltung von Datentreuhändern, DuD 2006, 694-699.

Weißgerber, Michael,
Arbeitsrechtliche Fragen bei der Einführung und Nutzung vernetzter Computerarbeitsplätze, Berlin 2003.

Weißnicht, Elmar,
Die Nutzung des Internet am Arbeitsplatz, MMR 2003, 448-453.

Wessels, Johannes/Hettinger, Michael,
Strafrecht. Besonderer Teil 1. Straftaten gegen Persönlichkeits- und Gemeinschaftswerte, 32. Aufl., Heidelberg 2008.

Wiese, Günther,
Personale Aspekte und Überwachung der häuslichen Telearbeit, RdA 2009, 344-353.

Wittig, Petra,
Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, 59-62.

Wöhe, Günter/Döring, Ulrich,
Einführung in die Allgemeine Betriebswirtschaftslehre, 23. Aufl., München 2008.

Wölfl, Bernd,
Ist die Verwendung befugt hergestellter Tonaufnahmen strafbar?, JURA 2003, 742-744.

Wohlgemuth, Hans,
Kollektives Arbeitsrecht und Informationstechnik, CR 1988, 1005-1008.

Wronka, Georg,
Zur Interessenlage bei der Auftragsdatenverarbeitung, RDV 2003, 132-135.

Wuermeling, Ulrich,
Scoring von Kreditrisiken, NJW 2002, 3508-3510.
Wybitul, Tim/Reuling, Hendrik,
Umgang mit § 44 BDSG im Unternehmen: Die weitreichenden zivilrechtlichen Folgen einer unscheinbaren Strafnorm, CR 2010, 829-832.
Zerbst, Jens-Tobias,
IT-Sicherheit und Outsourcing, in: Schoolmann, Jürgen/Rieger, Holger (Hrsg.), Praxishandbuch IT-Sicherheit. Risiken, Prozesse, Standards, Düsseldorf 2005, 401-418.
Zilkens, Martin,
Europäisches Datenschutzrecht – Ein Überblick, RDV 2007, 196-201.
Zoebisch, Michael,
Stimmungsanalyse durch Call-Center. Datenschutzrechtliche Zulässigkeit der Analyse der emotionalen Verfassung anhand der Stimme, DuD 2011, 394-397.
Zscherpe, Kerstin,
Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, 723-727.
Zundel, Frank,
Die wachsende Bedeutung der „Kleinbetriebsklausel" des Kündigungsschutzgesetzes, NJW 2006, 3467-3470.

ISBN 978-3-86219-324-0