
Unternehmens**F**ührung & **C**ontrolling **UF&C**

Univ.-Professor Dr. Wolfgang Becker

Bamberger Betriebswirtschaftliche Beiträge

– Band 142 –

Privacy Benchmarking 2004 – Strategie und Funktion des Datenschutzes in der ITK-Branche

Wolfgang Becker, Stefan Fischer
und Christian Semmler

ISBN 3-931810-46-1



Otto-Friedrich-Universität Bamberg

Impressum

Herausgeber

Univ.-Professor Dr. Wolfgang Becker
Lehrstuhl **UnternehmensFührung&Controlling**

Otto-Friedrich-Universität Bamberg
Feldkirchenstrasse 21
D-96052 Bamberg

Fon +49.(0)951.863.2507

Fax +49.(0)951.39705

Mail ufc@sowi.uni-bamberg.de

Internet www.professorwbecker.de

Druck

Copyright © by Univ.-Professor Dr. Wolfgang Becker, Universität Bamberg.

Diese Publikation ist urheberrechtlich geschützt. Respect Creativity!

Bamberg 2006, Printed in Germany.

Inhaltsverzeichnis

1	Einleitung	5
2	Klassifikation und Teilnehmerstruktur	11
2.1	Branchenbereiche	12
2.2	Unternehmensgröße und Betreuungsaufwand	14
2.3	Primary Business	16
2.4	Zertifizierung	17
3	Strategie und Funktion des Datenschutzes	19
3.1	Beauftragter für den Datenschutz	19
3.1.1	Ressourcen	19
	(1) Personelle Ausstattung	20
	(2) Finanzielle Mittel	22
	(3) Zugriff auf externes Know-How	25
3.1.2	Qualifikation	25
3.1.3	Schnittstellen	26
	(1) Datenschutz-Aufsichtsbehörden	26
	(2) Andere Funktionsträger im Unternehmen	28
3.2	Aufgaben des Beauftragten für den Datenschutz	31
3.2.1	Tätigkeitsschwerpunkt	31
3.2.2	Schulung	33
	(1) Analyse der Schulungsmaßnahmen	33
	(2) Bestandteil der fachlichen Fortbildung	37
3.2.3	Beratung und Kontrolle	37
	(1) Interne Kontrollen	38
	(2) Auftragsdatenverarbeitung – Kontrolle nach § 11 BDSG	40
3.2.4	Informationspolitik	43
3.2.5	Verfahrensverzeichnis	44
3.3	Unternehmenspolitischer Auftrag	47
3.3.1	Institutionalisierung	48

3.3.2 Leistungen	50
(1) Leistungsdefinition	50
(2) Leistungen am Markt	52
(3) Datenschutzfreundliche Produkte bzw. Technologien ..	52
(4) Leistungsverrechnung.....	53
3.3.3 Lobbying	54
3.3.4 Verpflichtung auf das Datengeheimnis.....	55
4 Übermittlung personenbezogener Daten ins Ausland	57
4.1 Ergebnisse	58
4.2 Rechtsgrundlage der Datenübermittlung in Drittstaaten	59
5 Allgemeine Einschätzung	61
5.1 Gütesiegel im Datenschutz	61
5.2 Datenschutzrechtsnormen	64
6 Zusammenfassung und Ausblick	66
6.1 Ergebnis der Untersuchung und Handlungsempfehlungen.....	66
6.2 Trends und Entwicklungen.....	68
Literatur	71
BBB-History	77

1 Einleitung

Angesichts zunehmenden Wettbewerbsdrucks und anhaltend schlechter Konjunkturlage sehen sich heute selbst Unternehmen, die in Zeiten ungebremsten Wachstums noch Millionen in Informationstechnologien (IT) investieren konnten, gezwungen, ihre Anstrengungen wieder auf Aktivitäten zu beschränken, die konkrete Vorteile für das Kerngeschäft versprechen.¹ Dies gilt nicht nur für Unternehmen der Privatwirtschaft, auch öffentliche Verwaltungen können und dürfen sich in Zeiten knapper Kassen auf ihr „Kerngeschäft“ konzentrieren und im Zuge einer effizienteren Aufgabenerledigung bestimmte Tätigkeiten an spezialisierte Dienstleister übertragen, die diese kostengünstig, zuverlässig und v.a. rechtskonform erbringen. Das trifft auch und in besonderem Maße für den Bereich IT zu.

Zunehmend gerät dabei auch die Übertragung der Verarbeitung personenbezogener Daten in den Fokus von Outsourcing-Aktivitäten. Neben den technologischen und organisatorischen Aspekten der Datensicherheit ist hierbei v.a. das Vertrauen in die Dienste, Produkte und Leistungen des Dienstleisters entscheidend. Insbesondere muss der Auftraggeber sich darauf verlassen können, dass seine Daten ausschließlich zweckbestimmt verarbeitet und vor missbräuchlicher Verwendung geschützt werden.

Die Ressource Information ist inzwischen neben Arbeit, Kapital und Rohstoffen zum vierten Produktionsfaktor geworden, der in vielfältiger Weise aufbereitet, strukturiert und rationalisiert wird, um gezielt eingesetzt zu werden.² Die fortschreitende Durchdringung selbst der privatesten Lebensbereiche durch moderne Informations- und Kommunikationstechnologien (IKT) führt dabei zu riesigen Datenbeständen. Deren wachsender wirtschaftlicher Wert lässt dem Schutz der eigenen, ganz persönlichen Daten vor missbräuchlicher Verwendung daher auch aus Verbrauchersicht eine immer größere Bedeutung zukommen.

Das heute zum Teil noch vorrangige klassische Sicherheitsziel elektronischer Kommunikation erweitert sich damit im Allgegenwärtigkeitsparadigma moderner IKT zum Vertrauensziel bezüglich des Verhaltens eines Transaktions-

¹ Vgl. Smith, S. (2003), S. 5.

² Vgl. Büllsbach, A. (2002), S. 45.

und Kommunikationspartners im Umgang mit den eigenen, ganz persönlichen Daten.³

Je nach Kunde bzw. in Abhängigkeit der Art der Daten ist daher damit zu rechnen, dass Ansprüche an einen Dienstleister bestehen (werden), die über die gesetzlichen Anforderungen hinausgehen. Um in einem solchen Szenario jedoch das erforderliche Vertrauen zu schaffen, reicht es für den Dienstleister nicht aus, das Thema Datenschutz mit einigen vertraglichen Vereinbarungen unter Nennung der einschlägigen Gesetze abzuhandeln. Ein anerkannt hohes Datenschutzniveau stellt hier einen klaren Wettbewerbsvorteil dar und ist als Alleinstellungsmerkmal geeignet, den Erfolg eines Unternehmens am Markt entscheidend mitzubestimmen.

Die zunehmende Durchdringung selbst der letzten Lebensbereiche mit moderner Informationstechnik lässt den Schutz der eigenen Daten dabei über kurz oder lang von der Leistungsanforderung zur elementaren Basisanforderung seitens der Kunden und Verbraucher und damit zum zentralen Technologieakzeptanzfaktor werden.⁴ Insbesondere den Unternehmen der Informations- und Telekommunikations-Branche (ITK-Branche) kommt dabei als

³ Angelehnt an Eggs, H./Müller, G. (2002), S. 215; Vgl. genauer Eggs, H. (2001). Vgl. dazu sowie zum Allgegenwärtigkeitsparadigma auch Mattern, F./Langheinrich, M. (2001); Eggs, H./Müller, G. (2002), S. 214ff.

⁴ Eine hilfreiche Systematisierung von Kundenanforderungen liefert KANO, der in seinem Modell drei Gruppen von Anforderungen unterscheidet, deren (Nicht-)Erfüllung unterschiedliche Auswirkungen auf die Kundenzufriedenheit haben. Demgemäß beschreiben *Begeisterungsanforderungen* latent vorhandene, jedoch dem Kunden bislang selbst oft nicht bekannte Anforderungen an ein Produkt. Kann ein Unternehmen z.B. durch eine Innovation einen unerwarteten Zusatznutzen bieten, sind die Kunden begeistert und kaufen das Produkt. *Leistungsanforderungen* beziehen sich auf diejenigen Produktmerkmale, die der Kunde mit dem Angebot der Wettbewerber vergleichen kann. Sie werden von ihm wahrgenommen und bestimmen maßgeblich seine Zufriedenheit sowie den Kaufentscheidungsprozess. *Basisanforderungen* hingegen (wie z.B. ein bestimmtes Mindestdatenschutzniveau) werden vom Kunden vorausgesetzt und sind so selbstverständlich, dass sie nicht (mehr) explizit geäußert werden. D.h., nicht die Maximierung des Kundennutzens steht hier im Vordergrund, sondern die zunächst vollständige und sodann kostenminimale Realisierung der Anforderungen. Eine Nichterfüllung der Basisanforderungen fällt dem Kunden sofort negativ auf und führt zu Unzufriedenheit. Vgl. Arnaut, A./Hildebrandt, J./Werner, H. (1998), S. 308; Kano, N./Seraku, N./Tsuji, S. (1984); Bailom, F. et al. (1996). Einen Überblick gibt auch Becker, W. (2002), S. 70.

Die These, dass der Datenschutz einen sehr hohen Stellenwert genießt und zum Akzeptanzfaktor avanciert, ist im Übrigen durch eine Reihe repräsentativer Umfragen belegt. So zeigt z.B. eine 2001 in Deutschland durchgeführte Umfrage, dass 53% der Befragten wünschen, dass dem Datenschutz künftig mehr Bedeutung zukommen soll. Vgl. auch Opaschowski, H. W. (2001), ders. (2002).

weltweit größte Verarbeiter personenbezogener Daten die zentrale Rolle zu. Als Konsequenz ist das Schutzbedürfnis des Individuums vor Verletzung seiner Persönlichkeitsrechte und folglich ein hohes Datenschutzniveau speziell für diese Unternehmen als strategisches Erfolgspotential⁵ zu begreifen.

Dies erfordert in Anlehnung an das GÄLWEILERSche Konzept des betrieblichen Wertschöpfungskreislaufes⁶ anhaltend umfangreiche Investitionen, um den Datenschutz durch geeignete Maßnahmen als integralen Qualitätsbestandteil des betrieblichen Ressourcen- und Prozessgefüges entlang der gesamten Wertschöpfungskette zu etablieren.⁷ Nur die Unternehmen, denen dies gelingt, werden im Allgegenwärtigkeitsparadigma der Informationsgesellschaft von morgen über ein wesentliches Erfolgspotential verfügen, um dauerhaft unternehmerischen Erfolg in diesen Märkten zu realisieren.

Elementare Voraussetzung hierfür ist es, den Datenschutz als Qualitätsmerkmal am Markt zu kommunizieren und bei den Kunden z.B. durch entsprechende Datenschutzaudits oder Gütesiegel⁸ das nötige Vertrauen in die eigenen Produkte und Dienstleistungen zu schaffen. Der auf dieser Basis nachhaltig realisierte Erfolg wiederum sichert die notwendige Liquidität, um Datenschutz und auch Datensicherheit als Technikfolger und Voraussetzung für Datenschutz dauerhaft zu gewährleisten und den beschriebenen Wirkungskreislauf aufrechtzuerhalten.

⁵ Vgl. zu Begriff und Eigenschaften von Erfolgspotentialen z.B. Becker, W. (2001), S. 23. Danach zeichnen sich Erfolgspotentiale insbesondere dadurch aus, dass sie (1) bewusst aufbaubar, nutzbar und abbaubar sind, (2) vom Kunden wahrgenommen werden, (3) Wettbewerbsvorteile schaffen können, (4) Voraussetzung sind für dauerhaften (und möglichst überdurchschnittlichen) Erfolg und schließlich (5) im Zeitablauf vergänglich sind und daher der kontinuierlichen Erneuerung bedürfen.

⁶ Dieser aus Sicht der Unternehmensführung bedeutsame Regelkreis, der die betriebliche Wertschöpfung überhaupt erst ermöglicht und aufrechterhält, setzt sich aus operativen und strategischen Führungsgrößen zusammen. Als operative Führungsgrößen lassen sich betriebswirtschaftlicher Erfolg und Liquidität klassifizieren, die ihrerseits der Wertsphäre eines Unternehmens zuzuordnen sind. Erfolgspotentiale hingegen stellen als Vorsteuergrößen des zu realisierenden Erfolgs strategische Führungsgrößen dar. Der sämtliche Führungsgrößen berücksichtigende Regelkreis nimmt dabei seinen Ursprung im Etablieren geeigneter Erfolgspotentiale und führt durch deren gezielte Nutzung über die dauernde Realisation von Erfolg sowie die darauf gründende Sicherung von Liquidität zur existenzhaltenden Pflege und Erneuerung der Erfolgspotentiale. Vgl. Gälweiler, A. (1990), S. 23ff.; Becker, W. (1999), S. 5f.

⁷ Vgl. z.B. auch Reith, H.-K. (2005).

⁸ Vgl. zu Datenschutzaudits und Gütesiegeln als Wettbewerbselemente Diek, A. C. (2002); Roßnagel, A. (2002); Vossbein, R. (2002).

Datenschutz ist heute also nicht mehr nur gesetzliche Anforderung, sondern als Qualitätsbestandteil in immer stärkerem Maße ein weltweit maßgebliches Differenzierungskriterium bei der Gewinnung und Stärkung von Stakeholder-Beziehungen.⁹ Als „Corporate Value Factor“¹⁰ wird er damit zur Pflichtaufgabe der Unternehmensführung.¹¹

Dem Datenschutz kommt somit aus wirtschaftlicher und wissenschaftlicher Sicht eine Schlüsselrolle für die weitere Entwicklung der ITK-Branche zu. Welch hohen Stellenwert auch die Unternehmen dem Thema beimessen, zeigt eine im Jahr 2001 durchgeführte Branchenstudie.¹² Hier stand bei der Frage nach einer Änderung der rechtlichen Rahmenbedingungen, die entscheidenden Einfluss auf die Chancen und Risiken der Unternehmen haben, der Datenschutz an oberster Stelle der Dringlichkeitsliste. Im gleichen Jahr trat auch die Novellierung des Bundesdatenschutzgesetzes (BDSG) in Kraft. Die Umsetzungsfrist endete im Mai 2004. Höchste Zeit also, eine Standortbestimmung vorzunehmen und zu erfahren, wie die Unternehmen dieses Sektors – und hier vorrangig die verantwortlichen Datenschutzbeauftragten – das Thema heute einschätzen.

⁹ Vgl. Kern, H. (2003), S. 1.

¹⁰ So z.B. in DTAG (2004).

¹¹ Vgl. z.B. auch Reith, H.-K. (2005); Büllsbach, A. (2002).

¹² Vgl. KPMG (2001), S. 15f.

Zu diesem Zweck wurde ein Benchmarking-Konzept¹³ entwickelt, auf dessen Basis Datenschutzbeauftragte ausgewählter Unternehmen der ITK-Branche mit Sitz in Deutschland angesprochen wurden. Das eigentliche Benchmarking basiert dabei auf einer schriftlichen Befragung durch eine „Trusted-Third-Party“. Neben reinen Leistungsparametern der aus dem BDSG ableitbaren Aufgabenfelder werden dabei auch Faktoren wie die strategische Würdigung des Themas in der Unternehmenspolitik oder die Akzeptanz bestimmter gesetzlicher Regelungen erfasst. Ein weiteres Augenmerk wird dabei auf die besonderen datenschutzrechtlichen Anforderungen der sog. Auftragsdatenverarbeitung¹⁴ im Rahmen des IT-Outsourcing¹⁵ sowie bei der

¹³ Das in den USA entwickelte Instrument des *Benchmarking* wurde zunächst vorrangig für das Qualitätsmanagement erarbeitet und kann im weitesten Sinne als ein Prozess des Messens, Auswertens und Umsetzens von wirtschaftlich verwertbaren Größen und Merkmalen bezeichnet werden, die durch inter- und intraorganisationalen Vergleich gewonnen werden. Der Leistungsvergleich beim Benchmarking stützt sich dabei auf ein breiteres Spektrum an Indikatoren und bindet eine Ursachenanalyse der Leistungslücken ein. Die sog. *Benchmarks* bezeichnen dabei die quantitativen und im Zeitablauf veränderlichen Orientierungs- und Referenzwerte, die im Rahmen des Leistungsvergleichs ermittelt und benutzt werden. *Best Practices* hingegen werden als Oberbegriff verwendet, der verschiedenste Verfahren und Methoden ebenso wie die Rahmenbedingungen (Unternehmenskultur, Mitarbeiterführung usw.) subsumiert, die Unternehmen zu Spitzenleistungen führen.

Die übergeordnete Zielsetzung eines Benchmarking-Projekts liegt demnach in der Leistungssteigerung der eigenen Organisation. Dabei sind je nach Schwerpunkt grundsätzlich zwei Ausprägungen möglich, die sich jedoch gegenseitig nicht ausschließen: (1) *Messen und relatives Positionieren* (Quantitatives Benchmarking: Leistungsvergleich und Standortbestimmung anhand objektiver Kriterien und Ableitung von Zielvorgaben.) sowie (2) *Lernen von erfolgreichen Praktiken* (Qualitatives Benchmarking: Ableiten von Gestaltungsempfehlungen und Übertragung der Best Practices.). Im engeren Sinne konzentriert sich das Benchmarking dabei auf die Durchführung wettbewerbsbezogener Analysen. Vgl. Horváth, P./Herter, R. N. (1992), passim.; Keller, T. (1996), S. 2; Legner, C. (1999), S. 9ff.; Ulrich, P. (1998), S. 15f.; Pieske, R. (1995), S. 28ff.; Leibfried, K. H. J./McNair, C. J. (1993), S. 201ff.; Rau, H. (1996), S. 27; Camp, R. C. (1994), S. 16.

¹⁴ Eine Auftragsdatenverarbeitung i.S. von § 11 BDSG ist dadurch charakterisiert, dass sich eine „verantwortliche Stelle“ (vgl. BDSG § 3 (7)), im Folgenden als Auftraggeber bezeichnet, eines Dienstleistungsunternehmens bedient, welches dem Auftraggeber weisungsgebundene Unterstützung bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten leistet. Das Serviceunternehmen fungiert somit gleichsam als „verlängerter Arm“ oder als eine Art ausgelagerte technische Abteilung der nach wie vor verantwortlichen Stelle, die weiterhin die volle Verfügungsgewalt hinsichtlich des Umgangs mit den Daten behält. Der Auftragnehmer ist in diesem Fall kein „Dritter“ im Sinne des BDSG (vgl. BDSG § 3 (8)). Vgl. dazu z.B. Stöber, K. (2005); Gola, P./Jaspers, A. (2001), S. 19; BITKOM (2005), S. 24.

¹⁵ IT-Outsourcing kann allgemein definiert werden als mittel- bis langfristige Auslagerung von einzelnen innerbetrieblich erfüllten Aufgaben der Informationsverarbeitung (IV) bis hin zu kompletten IV-Geschäftsprozessen an rechtlich unabhängige Dienstleistungsunternehmen. Vgl. Mertens, P./Knolmayer, G. (1998), S. 17. Eine

Übermittlung personenbezogener Daten ins Ausland (insbes. beim sog. Offshoring) gelegt.

Auf Basis der ermittelten Realtatbestände lassen sich so Trendaussagen und konkrete Anhaltspunkte für die weitere Entwicklung der Branche ableiten. Zusammen mit den identifizierten „Best Practices“ ermöglichen sie den Unternehmen nicht nur eine Standortbestimmung bezüglich der jeweils eigenen Datenschutzorganisation, sondern liefern darüber hinaus wichtige Kenndaten für die eigene Strategieentwicklung.

Gegenstand dieses Beitrags stellt die vorwiegend deskriptive Darstellung der Ergebnisse des Privacy Benchmarking 2004 auf Basis der Auswertung der eingegangenen Rückmeldungen dar. Der Schwerpunkt liegt dabei primär auf einer Wiedergabe der ermittelten Realtatbestände, Zusammenhänge und beobachteter Tendenzen. Die Analyse von Abweichungsursachen, tiefergehende Interpretationen und insbesondere Detaildiskussionen zu den aus den empirischen Erkenntnissen abzuleitenden Gestaltungsempfehlungen für eine Datenschutzstrategie sind nicht Kernbestandteil der folgenden Ausführungen. Dies bleibt im Rahmen der Umsetzungsphase des Benchmarking den Teilnehmern und anderen Interessierten vorbehalten.

Einen grundlegenden Überblick über die in Deutschland geltenden datenschutzrechtlichen Regelungen und eine Reihe weiterer Bestimmungen für datenverarbeitende Stellen geben z.B. GOLA/JASPERS¹⁶ und GLOSSNER¹⁷. Wo zum Verständnis notwendig, werden spezielle Bestimmungen im Weiteren an entsprechender Stelle zudem kurz erläutert.

aktuelle und umfassende Darstellung des IT-Outsourcing aus rechtlicher, technischer, wirtschaftlicher und vertraglicher Sicht gibt Bräutigam, P. (2004). Vgl. hier zu technischen und wirtschaftlichen Grundlagen und insbesondere zur Begriffsbildung auch KÜCHLER, P. (2004). Diesem Verständnis folgend umfasst der Begriff des IT-Outsourcing im weiteren Verlauf der Untersuchung auch das sog. Application Service Providing (ASP) als Spezialfall des Outsourcing in einer 1:n Beziehung. Beim ASP sollen durch das Vermieten von Anwendungs- und Programmfunktionalität *mit dem gleichen IT-System* möglichst viele Kunden bedient werden. Vgl. KÜCHLER, P. (2004), S. 70f., Rdnr. 59 und 63.

¹⁶ Vgl. Gola, P./Jaspers, A. (2001).

¹⁷ Vgl. Glossner, S. (2004).

2 Klassifikation und Teilnehmerstruktur

Im ersten Teil des Fragebogens wurden zunächst allgemeine Strukturdaten zu den befragten Unternehmen erhoben, die im Folgenden vorgestellt werden sollen. Ziel hierbei ist festzustellen, inwieweit die teilnehmenden Unternehmen ein ausgewogenes Gesamtbild widerspiegeln und/oder ob einzelne Ausprägungen der untersuchten Kriterien dominieren. Wo angebracht, wird auf diese Daten im weiteren Verlauf der Darstellung zurückgegriffen.

Ausgangspunkt der Betrachtung bildeten dabei die jährlich von der Lünendonk GmbH ermittelten und als Marktbarometer geltenden sog. Lünendonk-Listen mit jeweils 25 führenden IT-Service-¹⁸ bzw. IT-Beratungs- und Systemintegrations¹⁹ - Unternehmen in Deutschland. Ferner wurden 15 weitere Unternehmen – darunter einige große und aufgrund ihrer Marktpräsenz bekannte Telekommunikationsunternehmen und Internet-Provider – bewusst ausgewählt. Als Kooperationspartner zur Ansprache weiterer Unternehmen der Zielgruppe konnten zudem die Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) sowie der Verband der deutschen Internetwirtschaft, das eco –Electronic Commerce Forum e.V. (eco-Forum) gewonnen werden.

Da ein Benchmarking der Funktion des Datenschutzs prinzipiell auch funktional möglich ist, wurden stellvertretend auch zwei zwar bezüglich ihres Kerngeschäfts branchenfremde Unternehmen hinzugezogen, die erstens aufgrund spezifischer Besonderheiten im Rahmen dieser Untersuchung trotzdem von Interesse sind und von denen zweitens ein hohes Datenschutzniveau vermutet wurde. Es handelt sich dabei um einen großen Logistikdienstleister, der insbesondere auch im Bereich der Auftragsdatenverarbeitung tätig ist und hier in großem Umfang personenbezogene Daten verarbeitet sowie um ein Unternehmen mit Kerngeschäft im Immobilienmanagement, das mehrere hundert Standorte mit spezifischen IT-Komponenten betreut.

¹⁸ Aufnahmekriterium für diese Liste: Mehr als 50 Prozent des Umsatzes werden mit IT-Dienstleistungen, z.B. Outsourcing, ASP, RZ-Services, Maintenance, Schulung oder Software erzielt. Die Rangfolge der Übersicht basiert auf kontrollierten Selbstauskünften der Unternehmen und Schätzungen der Lünendonk GmbH über in Deutschland bzw. von Deutschland aus bilanzierte/erwirtschaftete Umsätze. Vgl. Lünendonk (2004a).

¹⁹ Aufnahmekriterium für diese Liste: Das Unternehmen erwirtschaftet mehr als 60 Prozent des Umsatzes mit DV-Beratung, Individualsoftware-Entwicklung und Systemintegration. Vgl. Lünendonk (2004b).

Bei der Interpretation der Ergebnisse ist somit stets darauf zu achten, dass die Datenerhebung auf der Basis einer bewussten bzw. willkürlichen Stichprobenauswahl²⁰ nach verschiedenen Kriterien z.T. im Abschneideverfahren (Umsatz in bestimmten Marktsegmenten, subjektiv empfundene Marktpräsenz, bestehende Kontakte u.a.) erfolgte.

Augrund des nicht exakt bekannten Umfangs der Ursprungsauswahl konnte zwar die Rücklaufquote nicht bestimmt werden, dennoch übertraf der Rücklauf angesichts des sensiblen Themas mit 21 antwortenden Unternehmen die Erwartungen. Lediglich ein Fragebogen musste aufgrund nicht vergleichbarer Daten von der Auswertung ausgeschlossen werden.

2.1 Branchenbereiche

Die dieser Auswertung zugrunde liegende Einteilung in Branchenbereiche und Marktsegmente orientiert sich an der von LÜNENDONK getroffenen Systematisierung. Hierbei wurde separiert in IT-Service, IT-Beratung (Consulting) und IT-Systemintegration. Ferner wurden aufgrund der weiteren Unternehmen, die mit in die Untersuchung aufgenommen wurden, die zusätzlichen Antwortmöglichkeiten Internet-Provider bzw. Telekommunikations-Unternehmen angeboten. Außerdem konnten sonstige Branchen(bereiche) durch offene Antwort spezifiziert werden. Die Ergebnisse können der **Abbildung 1** entnommen werden. Im Bereich der Sonstigen konnten folgende und z.T. zusätzliche Einzelnennungen registriert werden: Online-Dienst, Immobilienmanagement, Logistik, Funk/Breitband/KFZ-Telematik, System-Development und Schulung. Es zeigt sich erwartungsgemäß eine Dominanz der durch die Lünendonk-Listen erfassten Marktsegmente (vgl. **Abb. 1**).

²⁰ Vgl. Diekmann, A. (2002), S. 328f.; Eine Übersicht über Auswahlverfahren geben auch Schnell, R./Hill, P. B./Esser, E. (1993), S. 285.

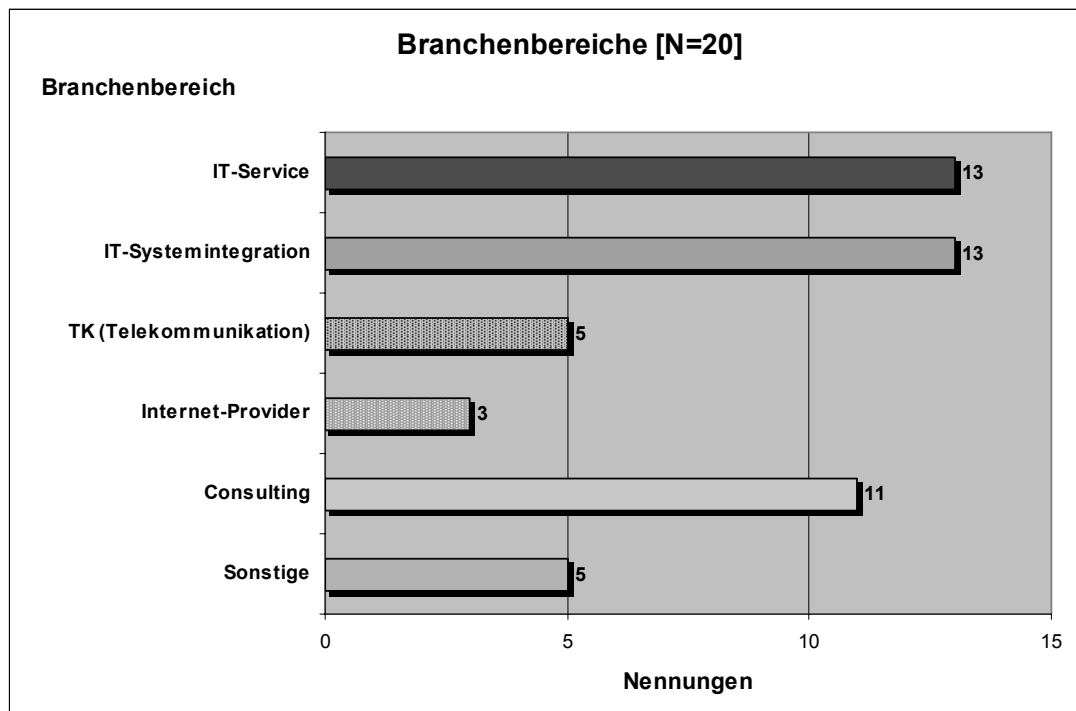


Abbildung 1: Branchenbereiche

Insbesondere die Abgrenzung zwischen den IT-Dienstleistungs-, Software- und Unternehmensberatungsmärkten ist dabei schwierig. Einige große IT-Unternehmen der Ursprungsauswahl, die durch Fusionen und Übernahmen entstanden und die ursprünglich hauptsächlich im IT-Beratungs- und Systemintegrations-Geschäft tätig waren, bestreiten heute beträchtliche Teile ihrer Umsätze auch mit Outsourcing-Services. Einige Anbieter veröffentlichen ferner keine aufgeschlüsselten Daten für die einzelnen Leistungskategorien, und manche internationale Unternehmen machen überhaupt keine entsprechenden Angaben für Deutschland und/oder Europa. Die Zuordnung einzelner Unternehmen zu diesen Marktsegmenten ist deshalb nur beschränkt aussagekräftig und ändert sich auch von Jahr zu Jahr.²¹

Aus diesem Grund und weil hier Mehrfachnennungen akzeptiert wurden, ist die Trennschärfe für detaillierte Trendanalysen bei der absolut betrachtet geringen Anzahl an Rückläufern regelmäßig nicht ausreichend. Ziel ist daher nicht, an jeder Stelle eine möglichst umfassende und eindeutige Clusterung der Ergebnisse hinsichtlich dieser Zuordnung vorzunehmen. Evtl. dennoch

²¹ Vgl. Lünendonk (2003a) und (2003b).

an einzelnen Stellen zu identifizierende Trends sollen jedoch in die weitere Darstellung der Ergebnisse einfließen.

2.2 Unternehmensgröße und Betreuungsaufwand

Bei Betrachtung der Umsätze in Deutschland (D) (vgl. **Abb. 2**) wird deutlich, dass immerhin 30% (n=6) der teilnehmenden Unternehmen (N=20) einen Umsatz von mehr als einer Milliarde (Mrd.) EUR erwirtschaften. Von den kleineren und mittleren Dienstleistern erwirtschaften mindestens 25% (n=5) Umsätze unter 100 Millionen (Mio.) EUR bzw. mindestens 30% (n=6) Umsätze zwischen 100 Mio. und 1 Mrd. EUR in Deutschland.

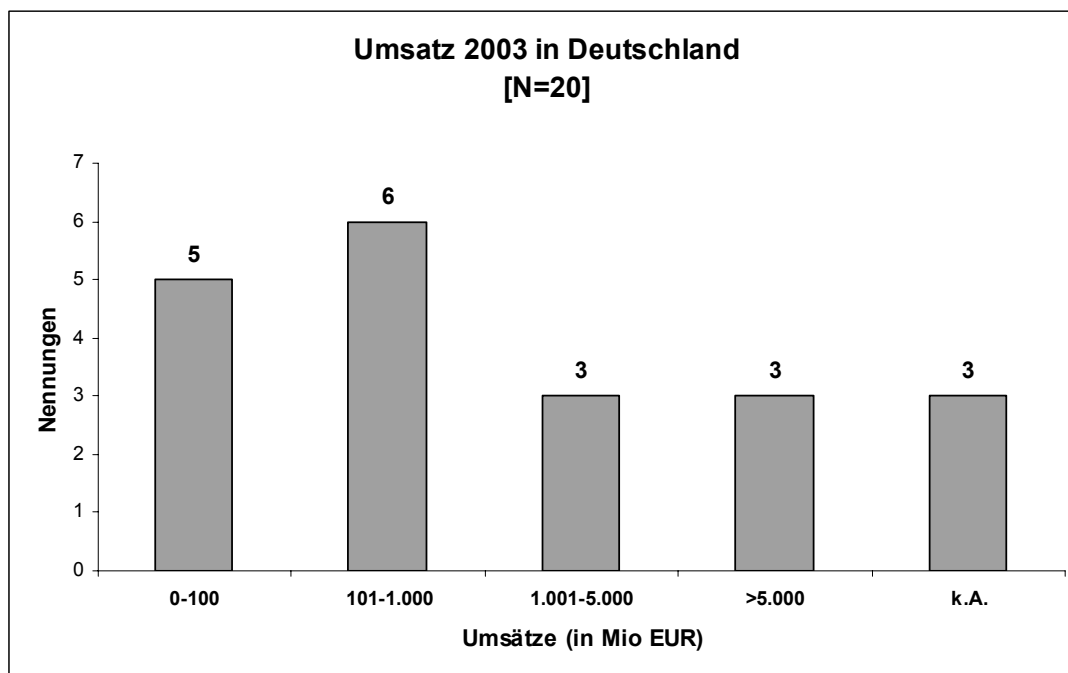


Abbildung 2: Gruppierung nach Umsätzen

Betrachtet man die Umsätze außerhalb Deutschlands, so zeigt sich bei den Werten für Europa (einschl. D), dass zwei Unternehmen europaweit Umsätze von weniger als 100 Mio. EUR und fünf zwischen 100 Mio. EUR und 1 Mrd. EUR im Jahr 2003 aufweisen. Vier Teilnehmer erwirtschafteten zwischen 1 und 5 Mrd. EUR und drei mehr als 5 Mrd. EUR Umsatz. Weltweit (einschl. Europa) geben sieben der Unternehmen weniger als 1 Mrd. EUR Umsatz und zwei zwischen 1 und 5 Mrd. EUR an. Je drei Unternehmen erwirtschafteten Umsätze zwischen 5 und 25 Mrd. EUR bzw. über 25 Mrd. EUR weltweit.

Um einen Eindruck des Betreuungsaufwands zu erhalten, den eine Datenschutzorganisation zu erbringen hat, wurde ferner die Anzahl der Beschäftigten sowie die Anzahl der Standorte, auf die sich diese verteilen, erhoben. Auch hier zeigt sich ein ähnlich ausgeglichenes Bild (vgl. **Abb. 3** und **4**). Erwartungsgemäß nimmt der Anteil der kleineren Unternehmen mit zunehmender geografischer Ausdehnung ab. Die angegebenen Werte spiegeln die jeweils ermittelte absolute Anzahl der Nennungen wider. Bei den Mitarbeiterzahlen für Europa befinden sich in der Gruppe ohne Angaben zwei Unternehmen mit mindestens 1000 bzw. 5000 Beschäftigten allein in Deutschland sowie beide mit mehr als 25.000 Beschäftigten weltweit.

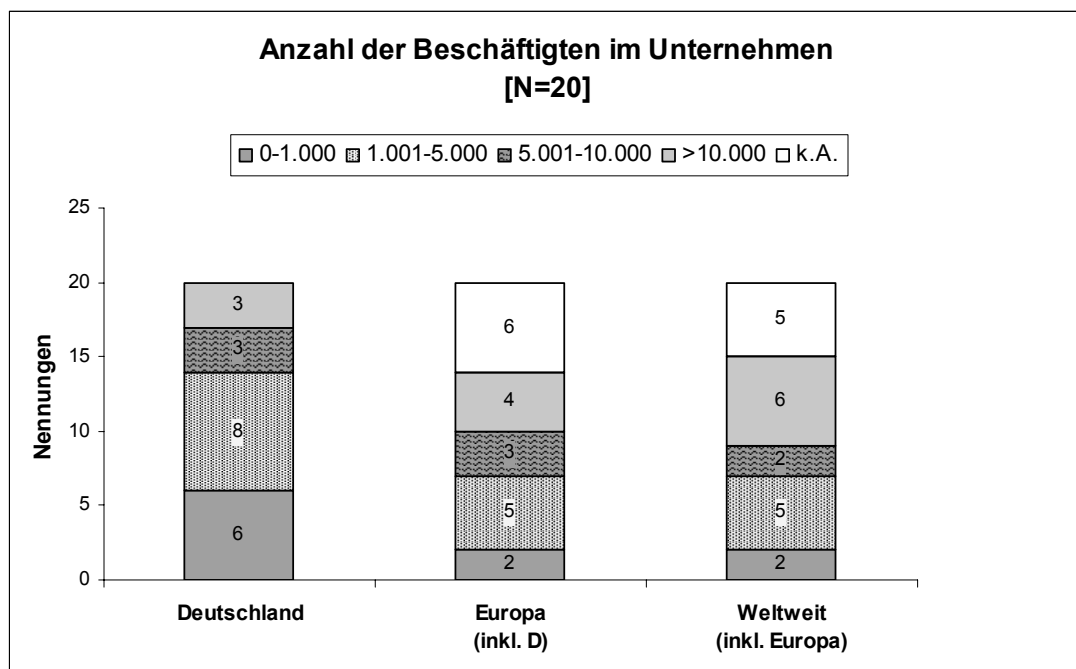


Abbildung 3: Anzahl der Beschäftigten im Unternehmen

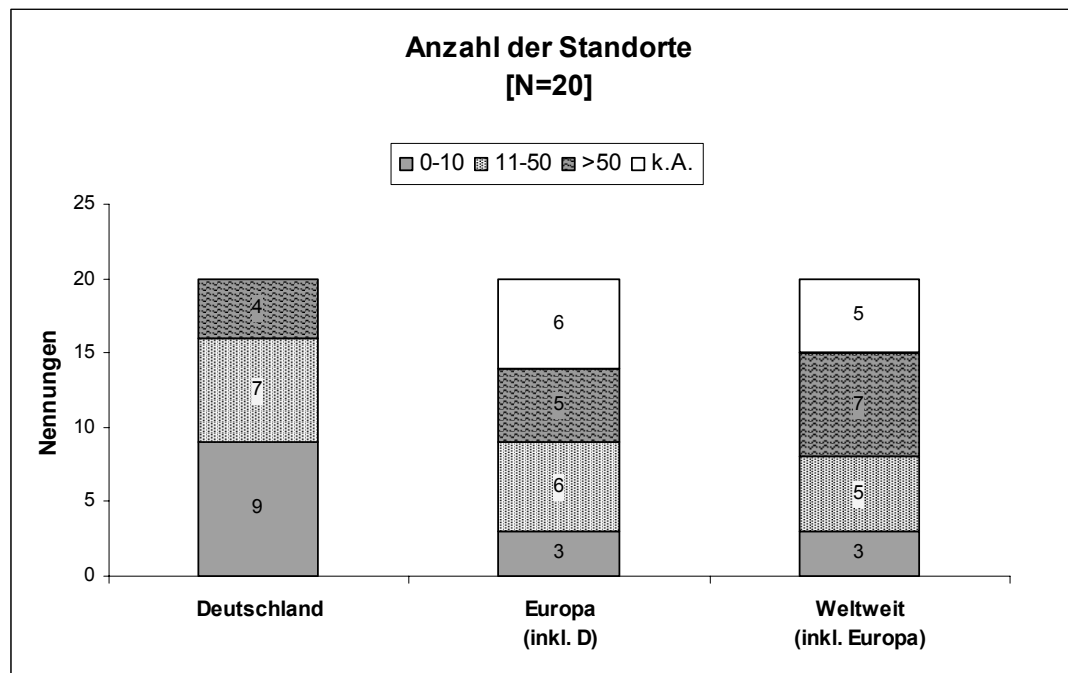


Abbildung 4: Anzahl der Standorte

Die Auswertung der erhobenen Daten zeigt damit eine ausgewogene Beteiligung unterschiedlich großer Unternehmen, die grob auch die Verteilung in der Ursprungsauswahl widerspiegelt.

2.3 Primary Business

Zur weiteren Analyse der Teilnehmerstruktur wurden verschiedene zusätzliche Kriterien erhoben, nach denen sich die Unternehmen klassifizieren lassen. So wurde zunächst gefragt, ob ein Unternehmen mehr als 50 Prozent seines Umsatzes mit Dienstleistungen entweder im Bereich des sog. Business Process Outsourcing (BPO) oder des sog. Application Service Providing (ASP) erwirtschaftet.²² Ferner wurde gefragt, ob es sich primär um einen Telekommunikationsdiensteanbieter i.S. von § 85 TKG handelt, d.h., das Unternehmen dem Fernmeldegeheimnis unterliegt sowie ob ein Unternehmen Anbieter von Auftragsdatenverarbeitungsleistung i.S. von § 11 BDSG ist.

Die Auswertung lieferte unterschiedliche Kombinationen von Nennungen (auch Mehrfachnennungen) deren absolute Häufigkeiten der **Abbildung 5**

²² Die Begriffe wurden an entsprechender Stelle durch Hilfetexte im Fragebogen definiert.

entnommen werden können. Die jeweiligen Kombinationsmöglichkeiten schließen sich dabei zwar grundsätzlich nicht aus (man denke an integrierte Dienstleistungen), so dass durchaus denkbar ist, dass ein Anbieter z.B. angibt, primär sowohl ASP- als auch BPO-Dienstleister zu sein. Da jedoch auf diese Möglichkeit bei der entsprechenden Befragung nicht explizit hingewiesen wurde und somit nicht mit hinreichender Sicherheit eine unterschiedliche Auslegung durch die Befragten ausgeschlossen werden kann, wird auf eine Gegenüberstellung dieser Klassifikationskriterien mit anderen Daten im Rahmen der weiteren Untersuchung verzichtet.

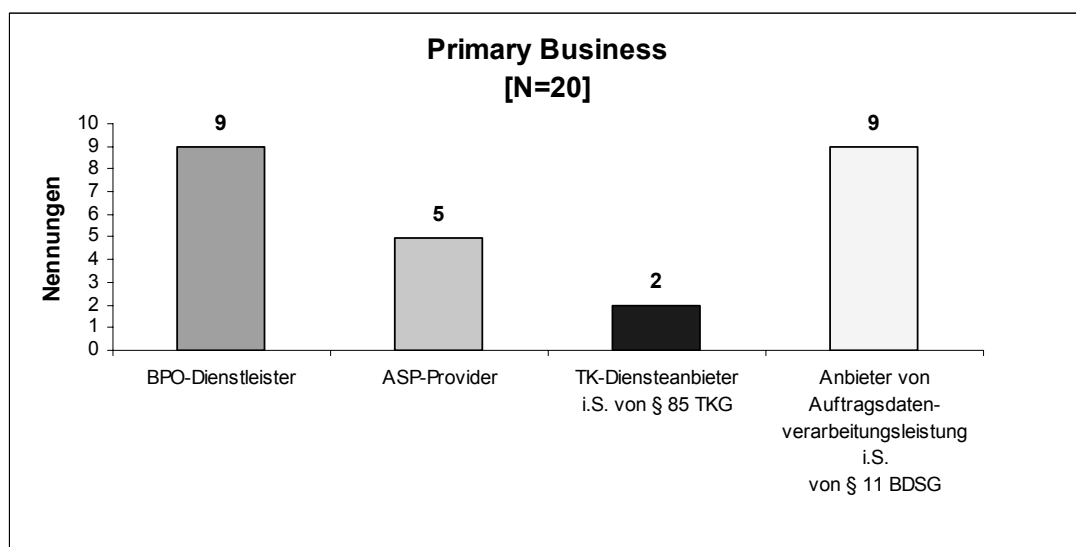


Abbildung 5: Primary Business

2.4 Zertifizierung

Zum Abschluss der Klassifikation wurde erhoben, ob die teilnehmenden Unternehmen nach den Normen ISO 9001 und/oder dem britischen Standard für IT-Security-Management BS 7799/ISO 17799 zertifiziert sind bzw. nach keiner der genannten. Zwei Unternehmen machten hierzu keine Angaben.

Wie das Ergebnis zeigt, sind immerhin knapp 78% (n=14) der antwortenden Unternehmen (N=18) nach ISO 9001 zertifiziert. Drei davon haben sich ferner einer Prüfung nach Standard BS 7799/ISO 17799 unterzogen. Vier Unternehmen geben an, nach keiner der beiden Normen geprüft zu sein (vgl. **Abb. 6**).

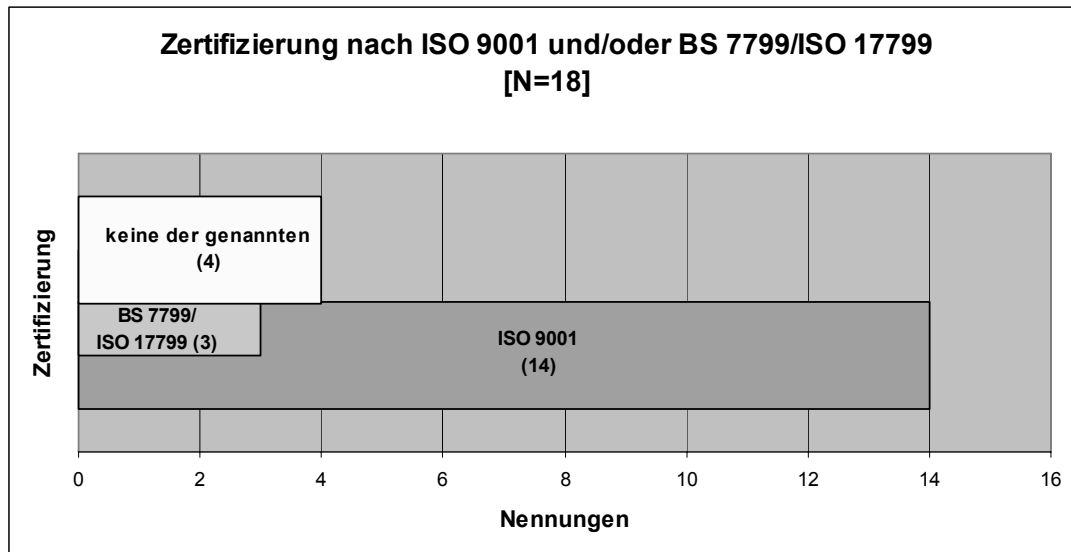


Abbildung 6: Zertifizierung

3 Strategie und Funktion des Datenschutzes

3.1 Beauftragter für den Datenschutz

Der folgende Abschnitt widmet sich der Funktion des betrieblichen Datenschutzbeauftragten (DSB). Dieser ist in 90% (n=18) der teilnehmenden Unternehmen intern bestellt. Lediglich zwei Unternehmen haben gemäß § 4f (2) BDSG eine externe Person mit dieser Aufgabe betraut. Dabei handelt es sich in einem Fall um den intern bestellten DSB der Konzernmutter; im anderen Fall um eine unternehmensfremde Person außerhalb des Unternehmensverbundes.

3.1.1 Ressourcen

Untersucht wurde zunächst, wie es mit der Ressourcenausstattung der an der Befragung teilnehmenden DSB bestellt ist. Der DSB ist gemäß BDSG „bei der Erfüllung seiner Aufgaben zu unterstützen.“²³ Ihm sind dabei „soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal [...] und Mittel zur Verfügung zu stellen“.²⁴ Wenn also im Rahmen der Wahrnehmung gesetzlicher Aufgaben durch den DSB die Rede ist, schließt dies etwaiges Hilfspersonal ausdrücklich mit ein. Aus Gründen der Lesbarkeit umfasst dieser Terminus daher, sofern nicht anders angegeben, im weiteren Verlauf der Untersuchung i.d.R. die gesamte Datenschutzorganisation.

Ein DSB eines großen Unternehmens (>10.000 Mitarbeiter in D) konnte keine exakten Aussagen zu den Ressourcen machen, da ihm zwar, wie er angibt, eine größere Anzahl an Mitarbeitern direkt bzw. indirekt fachlich für den Datenschutz zugeordnet ist, diese aber größtenteils auch andere Aufgaben wahrnehmen. Er wird daher sowohl im Rahmen der Personal- und Budgetauswertung ausgeklammert. Ferner konnten hier aufgrund fehlender Daten auch zwei weitere Teilnehmer nicht berücksichtigt werden.

Bei einem der im Folgenden berücksichtigten Teilnehmer umfasst die Personalressource und das Budget neben der Aufgabe Datenschutz auch die Unternehmenssicherheit. Der Einsatz der Ressourcen erfolgt aber nach eigener Angabe variabel je nach Arbeitsanfall in den beiden Themengebiete-

²³ BDSG § 4f (5).

²⁴ Ebd.

ten, hält sich aber ungefähr die Waage. Mannjahre und Budgetwerte wurden vom Befragten daher bereits halbiert und fließen so in die Auswertung ein. Ein weiterer DSB ist Vollzeit für den gesamten Konzern tätig; aber nur ca. 10% seiner Tätigkeit entfallen speziell auf das untersuchte Unternehmen. Somit entsprechen aus Gründen der Vergleichbarkeit auch hier die in die Auswertung einfließenden Angaben nur einem Zehntel seiner tatsächlichen Ressourcen.

(1) Personelle Ausstattung

Von insgesamt 17 der befragten Unternehmen liegen Angaben über die dem DSB zur Wahrnehmung seiner Funktion zur Verfügung stehende Zeit in Mannjahren sowie der Anzahl der Beschäftigten in Deutschland (D) vor.²⁵ Um die Anonymität zu wahren, musste hier eine starke Verdichtung der vorliegenden Daten erfolgen. **Abbildung 7** veranschaulicht daher dieses Verhältnis, das im Folgenden als *Betreuungsintensität* bezeichnet wird. Dabei wurde nach der Anzahl der Beschäftigten im Unternehmen gruppiert²⁶ sowie auf 1.000 Beschäftigte normiert. Ferner wurde die Balkendarstellung aus Gründen der Vergleichbarkeit um einen Extremwert je Gruppe bereinigt, auf welche weiter unten noch eingegangen wird. Somit gilt für die Betreuungsintensität zunächst N=14 (verbleibende Anzahl der Unternehmen in jeder Gruppe ≥ 4).

²⁵ Ein Unternehmen gibt ca. fünf bis zehn Personentage für spezifische Tätigkeiten durch Mitarbeiter aus dem Rechtsbereich sowie rund 25 Personentage des unternehmensfremden extern bestellten DSB an. Daraus ergeben sich in Summe und aufgerundet ca. 0,14 Mannjahre für die Datenschutzorganisation. Die bei der Umrechnung der Personentage zugrunde gelegte Basis für ein Mannjahr sind 260 Arbeitstage.

Bei einem anderen Unternehmen kommen weitere nicht genau zu beziffernde Mannjahre durch eine nicht genannte Anzahl an Datenschutzkoordinatoren hinzu, die hier somit nicht berücksichtigt werden konnten.

²⁶ unter 1.000 Mitarbeiter = kleine Unternehmen, 1.001 bis 5.000 Mitarbeiter = mittlere Unternehmen, mehr als 5.000 Mitarbeiter = große Unternehmen.

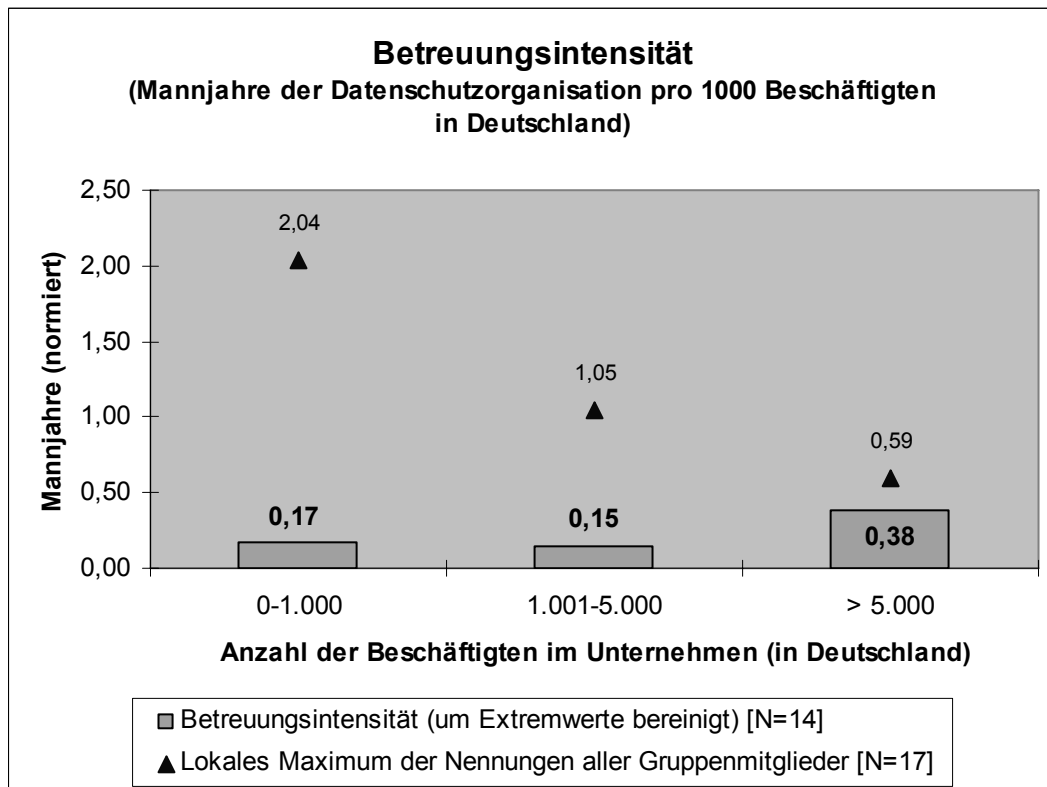


Abbildung 7: Personelle Ausstattung (Betreuungsintensität)

Während bei den kleinen und mittleren Unternehmen nur geringfügige Abweichungen zu verzeichnen sind, zeigt sich, dass bei den großen Unternehmen die Betreuungintensität sprunghaft zunimmt. Dies überrascht insofern an dieser Stelle, da hier ggf. Skaleneffekte zu vermuten wären. Anders interpretiert würde dies bedeuten, dass der Effizienzgrad der Datenschutzorganisationen in sehr großen Unternehmen abnimmt, was sich z.B. durch Überkompensation potentieller Skaleneffekte aufgrund steigender Koordinationskosten erklären ließe. Nahe liegender bzw. schwerwiegender scheint jedoch – und dies wird von den im weiteren Verlauf gemachten Angaben auch untermauert, dass größere Unternehmen tendenziell überdurchschnittlich in den Datenschutz investieren können und/oder wollen. Die daraus resultierend entsprechend größeren Datenschutzorganisationen haben dadurch auch deutlich mehr Möglichkeiten, was die inhaltliche Ausgestaltung ihrer Aufgabenwahrnehmung betrifft, als dies den DSB mit oftmals deutlich weniger als absolut 0,5 Mannjahren neben anderen Aufgaben im Tagesgeschäft möglich ist.

Dieses Bild spiegeln auch die normierten Höchstwerte (N=14) in den Gruppen der kleineren und mittleren Unternehmen wider, welche jeweils nur rund 0,3 Mannjahre pro 1.000 Beschäftigten betragen (nicht abgebildet). Demge-

genüber liegt das lokale Maximum in der Gruppe der großen Unternehmen mit immerhin 0,59 Mannjahren rund doppelt so hoch (vgl. erneut **Abb. 7**). Wie im weiteren Verlauf der Untersuchung jedoch deutlich wird, sind es nicht ausschließlich die Datenschutzorganisationen der kleineren und mittleren Unternehmen, die den gesetzlichen Anforderungen z.T. nicht im gebotenen Umfang nachkommen.

Erweitert man die Betrachtung um die oben bereinigten Unternehmen, erscheint an dieser Stelle interessant, dass selbst bei Berücksichtigung aller hier antwortenden Unternehmen (also $N=17$) die lokalen Minima (nicht abgebildet) in allen drei Gruppen bei normiert $\leq 0,1$ Mannjahren liegen. Der DSB eines mittelgroßen Unternehmens gibt dabei als absoluten Wert für die verfügbare Zeit sogar Null an, obwohl er mehr als 3.000 Beschäftigte zu betreuen hätte.

Betrachtet man hingegen die lokalen Maxima aller Nennungen zeigen sich zwei deutliche Ausreißer nach oben. So liegt das normierte Maximum, welches überraschenderweise durch ein sehr kleines Unternehmen erreicht wird, bei 2,04 Mannjahren. Der zweite Extremwert wird durch ein mittleres Unternehmen mit 1,05 Mannjahren pro 1.000 Beschäftigten erreicht. Der höchste absolute Wert aller antwortenden Teilnehmer wird von dem Unternehmen mit der größten Beschäftigtenanzahl aller teilnehmenden Unternehmen angegeben und beträgt 21 Mannjahre (nicht abgebildet), wobei hier nur ein sehr geringer normierter Wert erreicht wird.

Somit lässt sich zusammenfassend festhalten, dass die teilnehmenden Unternehmen pro 1.000 Beschäftigten im Mittel ca. 0,37 Mannjahre ($N=17$) bzw. um die Extremwerte bereinigt ca. 0,22 Mannjahre ($N=14$) für Ihre Datenschutzorganisation aufwenden.

(2) Finanzielle Mittel

Untersucht wurde hier das für Personal-, Sach- und sonstige Kosten ausgewiesene Gesamt-Budget sowie die speziell für Fortbildung, Öffentlichkeitsarbeit und Repräsentationszwecke zur Verfügung stehenden Mittel.

Auch hier musste zur Wahrung der Anonymität der Teilnehmer eine starke Verdichtung und Clusterung der Daten nach der Anzahl der Beschäftigten im Unternehmen vorgenommen werden. Dabei konnten aufgrund fehlender oder mangelhafter Daten nur 13 der oben untersuchten Unternehmen in diese Auswertung aufgenommen werden. Im Gegenzug ist jedoch das Unterneh-

men mit dem konzernintern bestellten externen DSB neu hinzugekommen. Die Darstellung wurde auch hier aus Gründen der Vergleichbarkeit um Extremwerte bereinigt. Dies betrifft zwei Teilnehmer aus den Gruppen der mittleren und großen Unternehmen. Somit gilt zunächst N=12 (mit jeweils vier Unternehmen in jeder Gruppe).

Die errechneten durchschnittlichen Budgetwerte sind in **Abbildung 8** abgetragen; sie müssen jedoch zur Interpretation in den Kontext eines geeigneten Bezugswertes gesetzt werden. Als eine der interessantesten Fragestellungen dieser Untersuchung bieten sich in diesem Zusammenhang sicherlich die Kosten der Datenschutzorganisation pro Mitarbeiter der betrachteten Unternehmen an. Diese wurden auf Basis des angegebenen Gesamt-Budgets und der Anzahl der Mitarbeiter in Deutschland errechnet. Hier ist anzumerken, dass es sich bei einigen der zugrunde gelegten Gesamtbudgets um von Teilnehmern geschätzte Werte der anfallenden Kosten handelt, da sie über kein eigenständig ausgewiesenes Budget verfügen bzw. dieses nach eigenen Angaben nicht ausgeschöpft werden sollte.

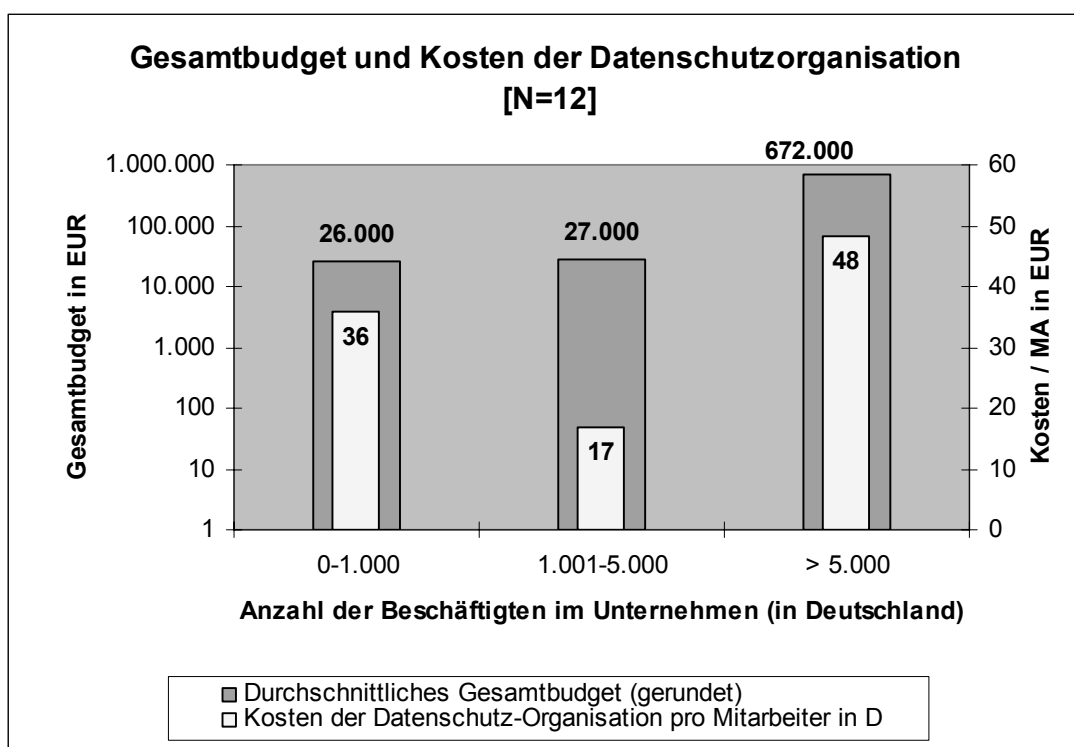


Abbildung 8: Gesamtbudget und Kosten der Datenschutzorganisation

Auffallend ist zunächst, dass sich hinsichtlich der durchschnittlichen Gesamtbudgets mit 26.000 bzw. 27.000 EUR auch in dieser Auswertung kaum nennenswerte Unterschiede zwischen den betrachteten kleineren und mittleren

Unternehmen zeigen. Demgegenüber springt der Wert bei den großen Unternehmen mit im Schnitt ca. 672.000 EUR extrem nach oben (logarithmische Skalierung der entsprechenden Achse).

Betrachtet man nun die Kosten der Datenschutzorganisation pro Mitarbeiter zeigt sich überraschenderweise bei den mittleren Unternehmen mit durchschnittlichen Kosten von nur 17 EUR ein deutlicher Einbruch, da die kleinen wie auch die großen Unternehmen mit 36 EUR bzw. 48 EUR pro Mitarbeiter hier deutlich höher liegen. Die Spannweite reicht dabei in der Gruppe der kleineren Unternehmen von 10 EUR bis knapp 57 EUR und in den großen Unternehmen von 12,50 EUR bis unter 93 EUR; in den mittleren Unternehmen jedoch nur von 4 EUR bis etwas über 31 EUR.

Bezieht man auch hier die bereinigten Unternehmen in die Analyse mit ein (also N=14), ist zunächst festzustellen, dass die jeweils niedrigsten Kosten pro Mitarbeiter in allen drei Gruppen auch hier bei relativ geringen Werten von z.T. deutlich unter 10 EUR liegen. Den absoluten Spitzenplatz belegt ein mittleres Unternehmen mit rund 95 EUR pro Mitarbeiter. Insgesamt sind zwei Unternehmen festzuhalten, die ein vergleichsweise hohes Datenschutz-Budget von rund 2 Mio. EUR aufweisen.

Zusammenfassend lässt sich feststellen, dass die Kosten der Datenschutzorganisation der 14 antwortenden Unternehmen im Schnitt bei rund 36 EUR pro Mitarbeiter im Jahr liegen (bereinigt rund 34 EUR). Es sei dabei jedoch an dieser Stelle ausdrücklich darauf hingewiesen, dass diese Ergebnisse sehr vorsichtig zu interpretieren sind. Es ist dabei eine Relativierung der Kosten aus zwei Blickwinkeln vorzunehmen: Einerseits ist zu berücksichtigen, dass einzelne der betrachteten Datenschutzorganisationen ggf. auch einen internationalen Auftrag zu erfüllen haben. D.h., es ergeben sich Verzerrungen durch die Tatsache, dass die Beschäftigten im Ausland in dieser Gegenüberstellung explizit nicht enthalten sind, für diese aber womöglich ebenfalls Leistungen erbracht werden. Andererseits sind die Kosten auch hinsichtlich des Umfangs der letztendlich überhaupt erbrachten Leistungen sowie weiterer relevanter Faktoren zu relativieren.

Die Notwendigkeit, diese Werte im richtigen Kontext des jeweils eigenen Unternehmens zu interpretieren, zeigt sich z.B. bei Betrachtung der beiden absoluten Extremwerte mit 4 EUR bzw. 95 EUR pro Mitarbeiter und Jahr. So weist das Unternehmen mit 4 EUR zwar die niedrigsten mitarbeiterbezogenen Kosten auf, dem DSB sind hier aber nach eigenen Angaben null Mannjahre für seine Aufgabe zugeordnet. Dies lässt dementsprechende Rück-

schlüsse auf die Möglichkeiten hinsichtlich der Aufgabenwahrnehmung zu, wohingegen das Unternehmen mit 95 EUR bei der Betreuungsintensität – also der personellen Ausstattung relativ zur Beschäftigtenanzahl – einen der Spitzenplätze belegt.

Abschließend ist hinsichtlich der für Fortbildung, Öffentlichkeitsarbeit und Repräsentationszwecke zur Verfügung stehenden Mittel festzustellen, dass sich diese größtenteils im Bereich bis zu 10.000 EUR bewegen. Lediglich die beiden größten Datenschutzorganisationen verfügen hierfür über höhere Summen im mittleren bis oberen fünfstelligen Bereich.

(3) Zugriff auf externes Know-How

Im Zusammenhang mit den Ressourcen wurde ferner die Frage gestellt, welche Möglichkeiten der DSB hat, um im Rahmen seiner Tätigkeit fundiertes Know-How z.B. aus den Bereichen Technik oder Recht einzuholen. Mehrfachnennungen waren hier möglich.

Dabei ist festzustellen, dass die Experten aus dem eigenen Hause allen Befragten (N=20) unentgeltlich zur Verfügung stehen. In drei der Unternehmen (15%) kann der DSB diese zudem auch gegen Entgelt konsultieren. Die Möglichkeit, externen Rat in Anspruch zu nehmen, steht dagegen nur 70% (n=14) der Befragten DSB offen.

3.1.2 Qualifikation

Zur Entwicklung moderner Datenschutzkonzepte bedarf es Akteure, die diese fördern, tragen und vor dem Hintergrund sich rapide weiterentwickelnder IKT zukunftsorientiert gestalten. Die Häufigkeit der Fortbildung eines DSB zum Thema Datenschutz liefert dabei ein Indiz, welche Strategie in einem Unternehmen mit dem Datenschutzmanagement verfolgt wird.²⁷

Hinsichtlich des beruflichen Hintergrundes lässt sich zunächst wertungsfrei feststellen, dass die Hälfte aller befragten DSB eine technische Ausbildung absolviert hat. Betriebswirtschaftler und Juristen sind dagegen nur mit je 20% vertreten. Zwei Befragte (10%) gaben eine andere Ausbildungsart bzw. eine interdisziplinäre Ausbildung an. Interessant hierbei ist, dass von den zehn DSB mit technischem Hintergrund die Mehrzahl (80%) eine Zusatzausbil-

²⁷ Angelehnt an Büllesbach, A. (2003), S.20.

dung zum DSB abgeschlossen hat, während dieser Anteil bei den anderen beiden großen Gruppen nur je 50% beträgt.

Betrachtet man die Häufigkeit der Fortbildung der DSB zum Thema Datenschutz, lässt sich eine Spannweite von gar nicht (drei Nennungen) bis zu sechs mal im Jahr (eine Nennung) beobachten. Wie sich somit zeigt, bildet sich die Hälfte der Befragten zwei bis drei mal im Jahr fort. Im Fall des außerhalb des Unternehmensverbundes extern bestellten DSB blieb diese Frage unbeantwortet. Die aggregierten Ergebnisse sind der **Abbildung 9** zu entnehmen.

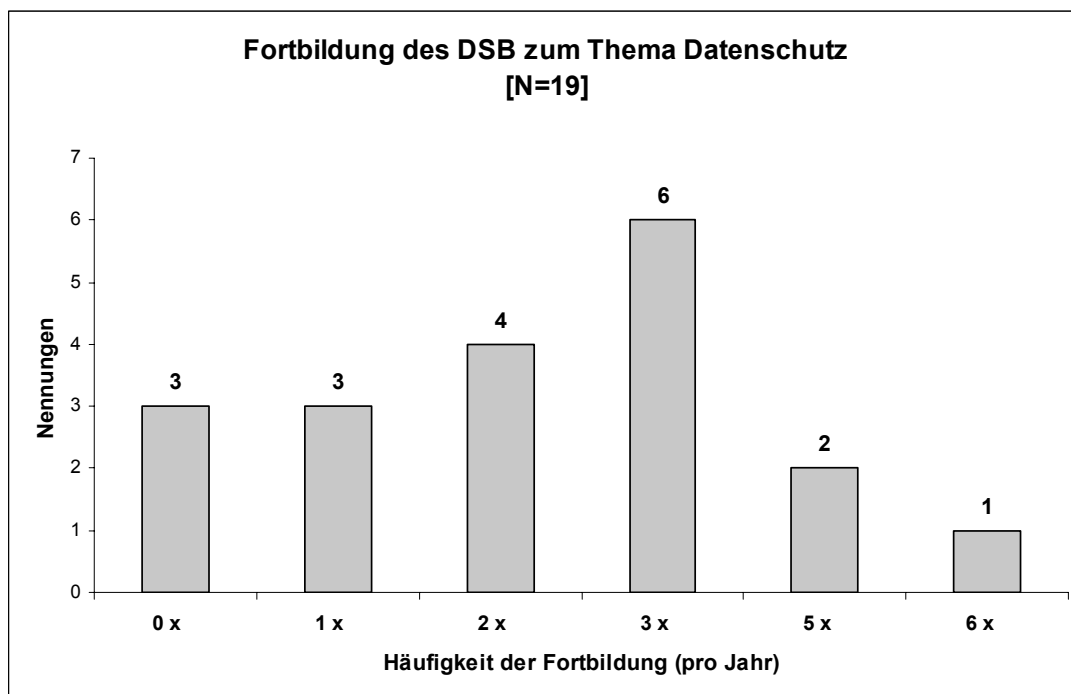


Abbildung 9: Fortbildung des DSB zum Thema Datenschutz

3.1.3 Schnittstellen

Bei der Untersuchung der Funktion des DSB interessiert – insbesondere im Zusammenhang mit der Ausübung der betrieblichen Selbstkontrolle – die Einschätzung der Zusammenarbeit bzw. der Kontakte mit verschiedenen aus Sicht des Datenschutz besonders relevanten Schnittstellen.

(1) *Datenschutz-Aufsichtsbehörden*

Kontakte der Unternehmen mit den Aufsichtsbehörden können ihrem Charakter nach grundsätzlich danach unterschieden werden, ob sie im Rahmen

von Kontrollen (z.B. wenn konkrete Anhaltspunkte für eine Rechtsverletzung vorliegen) oder aus anderem Grund erfolgen. Dabei interessiert vor allem, wie diese Kontakte von den DSB im Allgemeinen beurteilt werden und wie häufig sie stattfinden. Um der Sensibilität dieses Untersuchungsgegenstandes Rechnung zu tragen, konnten hier alternativ oder ergänzend zu einer Bewertung mit Schulnoten auch offene Angaben gemacht werden. Von fünf Unternehmen bleibt die Frage dennoch unbeantwortet; ein DSB weist darauf hin, dass diesbezügliche Kontakte über die Konzernmutter erfolgen.

Kontrollbezogene Kontakte werden von sieben Unternehmen angegeben. Davon berichten vier Befragte je von einem Fall und zwei Befragte von je drei Fällen. In sechs Unternehmen wurden den Angaben zufolge noch keine Kontrollen durchgeführt. Kontakte anderer Natur pflegen elf Unternehmen. Konkret benannt wurden Arbeitstreffen, Besprechungen datenschutzrechtlicher Fragestellungen sowie Statusgespräche. Sechs der Befragten geben dabei an, dass derartige Kontakte zwei- bis dreimal im Jahr stattfinden; vier Teilnehmer pflegen derartige Kontakte sogar sechs bis zwölfmal im Jahr. Eines der Unternehmen machte zu den jeweiligen Häufigkeiten keine Angaben, gibt jedoch an, zu Zeiten des BDSG-1990 regelmäßig von den Aufsichtsbehörden kontrolliert worden zu sein. Aus diesen Zeiten sei die Zusammenarbeit und das Verhältnis mit dem Bundesbeauftragten für den Datenschutz (BfD) bzw. mit den Aufsichtsbehörden bestens. Ähnliches spiegeln auch die offenen Angaben der anderen Teilnehmer wider. Der Kontakt wird darin als kompetent, konstruktiv und kooperativ eingestuft. Die Bewertungen der Kontakte durch Schulnoten (1-5) untermauern dieses positive Bild (vgl. **Abb. 10**). Die Kontakte werden dabei von der überwiegenden Mehrheit der DSB mit *sehr gut* (1) bzw. *gut* (2) bewertet. Die Durchschnittsnote beträgt in beiden Fällen 1,7 (*gut*).

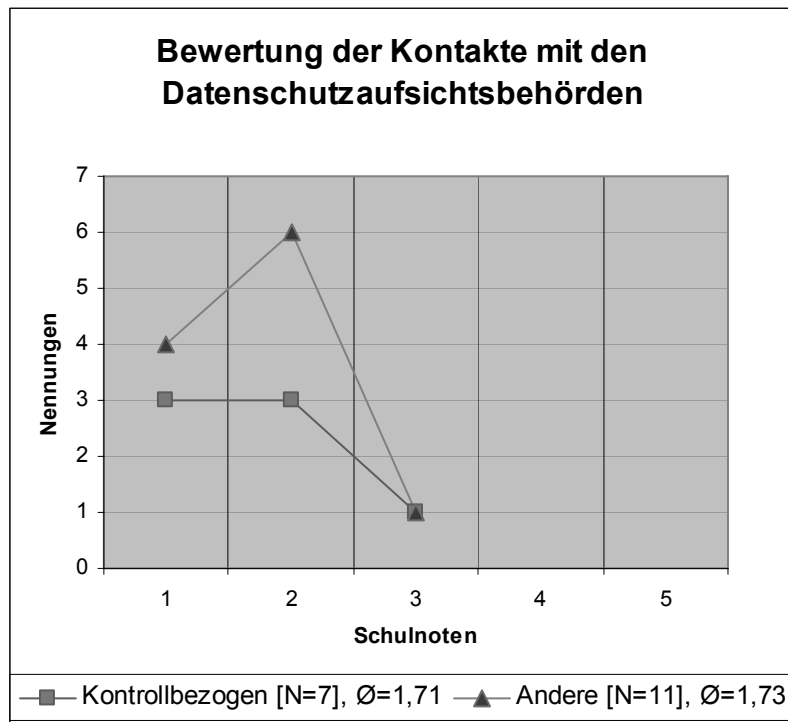


Abbildung 10: Bewertung der Kontakte mit den Datenschutzaufsichtsbehörden

(2) Andere Funktionsträger im Unternehmen

An dieser Stelle soll die Zusammenarbeit der Datenschutzorganisation mit anderen Funktionsbereichen im Unternehmen betrachtet werden. Der DSB ist zwar gemäß BDSG in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei,²⁸ die beste Voraussetzung für die Umsetzung eines umfassenden und effizienten Datenschutzes ist jedoch eine konstruktive Zusammenarbeit der verschiedenen Funktionsträger bei gemeinsamen Aufgabenstellungen.²⁹

Dem DSB ist durch das BDSG die Aufgabe zugewiesen, auf die Einhaltung der gesetzlichen Vorschriften über den Datenschutz hinzuwirken. Von elementarer Bedeutung in dieser Hinsicht ist daher zunächst die grundsätzliche Kooperation der Geschäftsführung. Der DSB ist insbesondere rechtzeitig über Vorhaben der automatisierten Verarbeitung personenbezogener Daten zu unterrichten.³⁰ Dies ist einerseits Voraussetzung, um die ordnungsgemäße

²⁸ Vgl. BDSG § 4f (3).

²⁹ Vgl. BfD (2004b), Nr. 3.7; TSI (2004).

³⁰ Vgl. BDSG § 4g (1) Satz 3 Nr. 1.

Anwendung der betreffenden Datenverarbeitungsprogramme zu überwachen. Andererseits kann der DSB die Beteiligten nur durch frühzeitige Einbindung bereits auch im Vorfeld bspw. durch eine unabhängige Beratung bei der Gewährleistung des Datenschutzes unterstützen.

Regelmäßig zu den Beteiligten zählen die IT-Abteilung, die solche Vorhaben umsetzt, sowie im Rahmen der Daten- und Informationssicherheit auch der Bereich Unternehmenssicherheit. Ferner beeinflussen im Fall von Arbeitnehmerdaten auch betriebsverfassungsrechtliche Vorschriften, Regelungen und Vereinbarungen die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung.³¹ Insofern hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen weit reichende Mitbestimmungsrechte³² und ist entsprechend zu beteiligen.

Selbst wenn das BDSG oder auch das Betriebsverfassungsgesetz (BetrVG) keine expliziten Aussagen über das Miteinander der verschiedenen Funktionsträger machen, liegt es nahe, dass diese im Interesse von Kunden und Mitarbeitern zusammenarbeiten und sich gegenseitig unterstützen. Zur Gewährleistung eines effizienten Datenschutzes muss die inhaltlich gebotene Zusammenarbeit vorausgesetzt werden.³³

Die befragten DSB sollten daher die Qualität der Zusammenarbeit mit den vier zuvor genannten sowie einem weiteren für sie wichtigen Partner anhand von Schulnoten (1-5) aus ihrer Sicht bewerten. Die Ergebnisse der vier vorgegebenen Partner können der **Abbildung 11** entnommen werden. Auf die verschiedenen Einzelnennungen der erfassten weiteren Partner wird weiter unten eingegangen.

³¹ Eine Verarbeitung von Arbeitnehmerdaten unterliegt der Mitbestimmung des Betriebsrates, dem ebenfalls eine Datenschutzkontroll-Aufgabe gesetzlich zugewiesen wird: Er hat sowohl den Auftrag, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen als auch die Aufgabe darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze und Betriebsvereinbarungen eingehalten und durchgeführt werden. Vgl. Gola, P./Jaspers, A. (2001), S. 37ff. sowie BetrVG § § 75 (2) und 80 (1) Nr. 1.

³² Diese Mitbestimmungsrechte greifen v.a. dann, wenn diese Einrichtungen dazu geeignet sein können, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Vgl. hierzu Gola, P./Jaspers, A. (2001), S. 39 sowie BetrVG § 87 (1) Nr. 6.

³³ Vgl. TSI (2004).

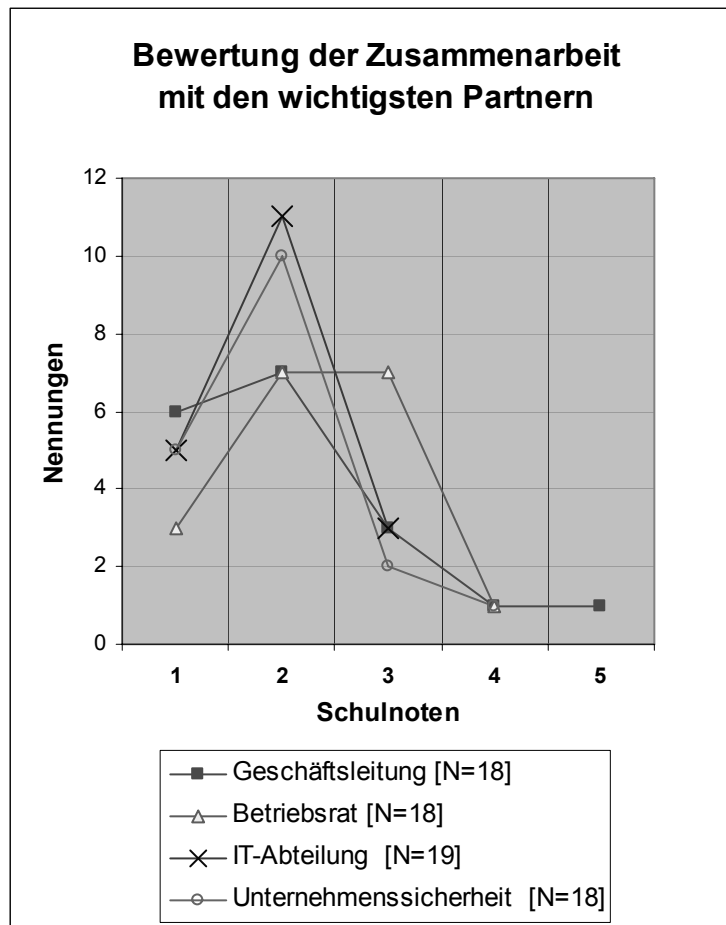


Abbildung 11: Bewertung der Zusammenarbeit mit den wichtigsten Partnern

Dabei zeigt sich, dass die überwiegende Mehrheit der befragten DSB die Kooperation mit den Partnern als durchweg gut einschätzt. Im Mittel am besten wird dabei die Zusammenarbeit mit den IT-Abteilungen (1,89) und der Unternehmenssicherheit (1,94) bewertet. Aber auch Geschäftsführung (2,11) und Betriebsrat (2,33) schneiden immerhin noch gut ab.

Ferner konnten folgende Einzelnennungen verschiedener Teilnehmer registriert werden: Jeweils mit *sehr gut* (1) wird die Zusammenarbeit mit der Produktkonzeption, der ‚Product Security‘ und dem Koordinator vor Ort (der Teilnehmer ist externer DSB) bewertet. Mit einem *Gut* (2) schneiden eine Rechts- sowie eine Personalabteilung ab. Zweimal genannt wurden nicht näher spezifizierte Fachabteilungen, sie erhalten lediglich die Note 3.

Somit zeigt sich hier ein ähnlich gutes Bild, wie im Bereich der Zusammenarbeit mit den Aufsichtsbehörden. Dies lässt einerseits auf eine hohe Akzeptanz gegenüber den Behörden schließen. Andererseits ist eine konstruktive

Zusammenarbeit der innerbetrieblichen Funktionsträger auch notwendige Voraussetzung einer gut funktionierenden Selbstkontrolle durch die Unternehmen. Ist diese Voraussetzung erfüllt, können die nachgewiesenermaßen guten Bewertungen in diesem Zusammenhang gleichermaßen als ein Indiz hierfür gewertet werden.

3.2 Aufgaben des Beauftragten für den Datenschutz

Wie bereits angemerkt, weist das BDSG dem DSB in § 4g die Aufgabe zu, auf die Einhaltung des BDSG und anderer datenschutzrechtlicher Bestimmungen hinzuwirken.³⁴ Unbeschadet der fortbestehenden Verantwortlichkeit der Geschäftsleitung trägt er damit maßgeblich zur Einhaltung der Vorschriften des Datenschutzes in seiner Organisation bei.³⁵ Er hat insbesondere bei den mit der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen das nötige Bewusstsein für den Datenschutz zu schaffen und die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme zu überwachen.³⁶ Diese Aufgaben erfüllt er in Form von Information, Schulung, Beratung und Kontrolle sowie durch Schaffung von Transparenz in der Datenverarbeitung.³⁷

3.2.1 Tätigkeitsschwerpunkt

Das Handlungsfeld des DSB ergibt sich einerseits direkt aus dem § 4g (s.o.) sowie andererseits aus dem § 9 BDSG. Hiernach sind alle „technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften [über den Datenschutz] [...] zu gewährleisten.“³⁸ Insbesondere „ist die innerbetriebliche Organisation [durch aufbau- und ablauforganisatorische Maßnahmen] so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.“³⁹

³⁴ Vgl. BDSG § 4g (1).

³⁵ Vgl. BfD (2004b), Nr. 3.

³⁶ Vgl. BDSG § 4g (1) Satz 3.

³⁷ Vgl. z.B. BfD (2004b), Nr. 3.

³⁸ BDSG § 9. Einfügung durch den Verfasser. Vgl. zu den technischen und organisatorischen Maßnahmen die Anlage zu § 9 Satz 1 BDSG (vgl. Anhang B).

³⁹ BDSG, Anlage zu § 9 Satz 1. (Siehe Anhang B).

Somit lassen sich, abgeleitet aus § 4g und § 9 BDSG, nachfolgende Tätigkeits- und Mitwirkungsfelder des DSB identifizieren:

- Mensch (z.B. Schulung, Information, Unterweisung),
- Technikgestaltung (z.B. Datensicherheitskonzepte),
- Organisationsgestaltung (z.B. Prozessberatung, Vertragsgestaltung).

In der entsprechenden Befragung wurden daher die Prozentsätze erhoben, die in etwa den Anteil der Tätigkeiten in diesen Bereichen beschreiben. Die Ergebnisse der Auswertung und die entsprechenden Mittelwerte sind in **Abbildung 12** dargestellt. Den im Mittel größten Anteil nehmen dabei mit 44% die Tätigkeiten im Rahmen der Organisationsgestaltung ein, es folgt der Tätigkeitsbereich Mensch mit 34% sowie mit deutlichem Abstand die Technikgestaltung (22%).

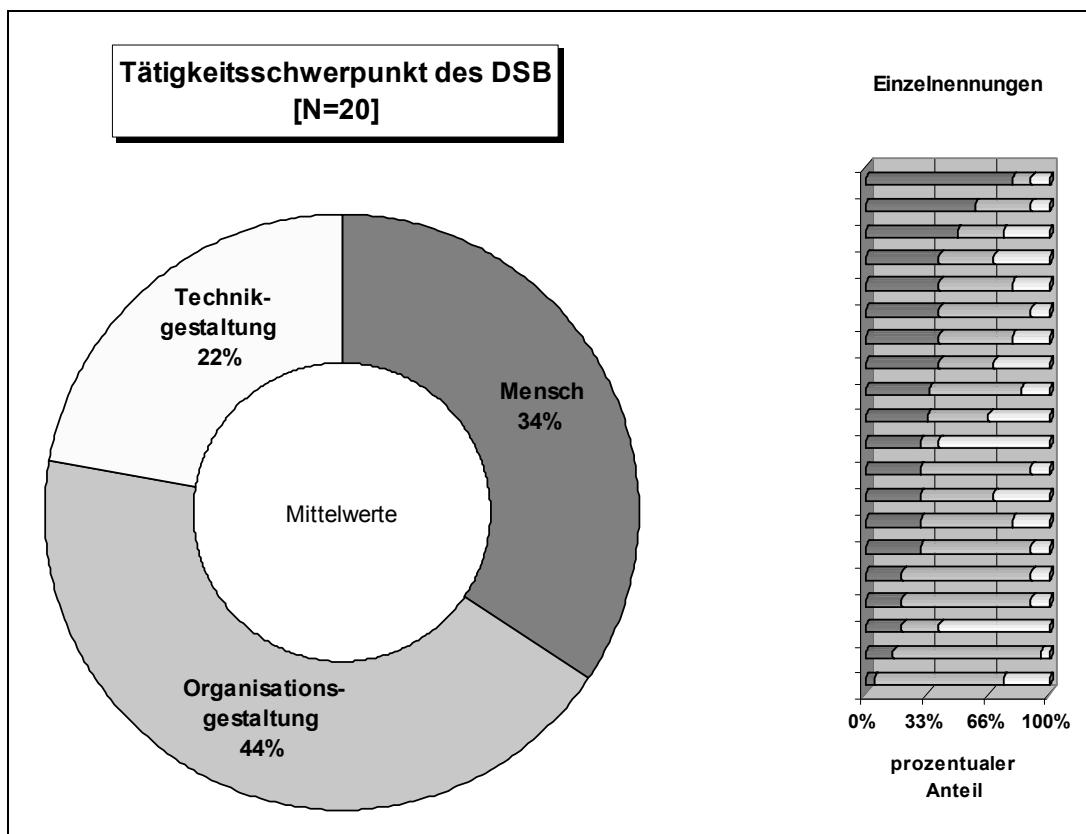


Abbildung 12: Tätigkeitsschwerpunkt des DSB

Im Rahmen einer Clusteranalyse ist auffällig, dass bei den IT-Beratungs- und Systemintegrations-Unternehmen der Tätigkeitsschwerpunkt Mensch mit 41,4% deutlich höher als im allgemeinen Durchschnitt ausfällt. Dieser Zu-

wachs geht größtenteils zu Lasten der Organisationsgestaltung, die hier nur mit 36,8 % beziffert wird. Aufgrund zahlreicher Einflussfaktoren und denkbar komplexer Wirkungszusammenhänge entzieht sich diese Abweichung jedoch der Interpretation. Auch eine Analyse z.B. der Größe der Datenschutzorganisation oder des beruflichen Hintergrunds der DSB lieferte keine Hinweise.

3.2.2 Schulung

Die Aufgabe des DSB ist es insbesondere, die in der Datenverarbeitung beschäftigten Personen mit den datenschutzrechtlichen Vorschriften sowie „den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.“⁴⁰ Dieser Abschnitt widmet sich daher einer eingehenden Untersuchung von Datenschutzschulungsmaßnahmen.

Hier gilt, dass Schulungen unterschiedliche Zielgruppen auf allen Hierarchieebenen haben, die in geeigneter Weise durch speziell auf sie abgestimmte Methoden zu erreichen sind.⁴¹ Aufgrund des breiten Spektrums denkbarer Ausprägungen, Zielgruppen und potentieller Leistungsindikatoren entsprechender Schulungsmaßnahmen musste im Rahmen des standardisierten Fragebogens eine Reduzierung des Beantwortungsfeldes derart vorgenommen werden, dass dennoch sinnvolle aggregierte Aussagen zu treffen sind. Dabei wurde schrittweise vorgegangen.

(1) Analyse der Schulungsmaßnahmen

Eingangs ist anzumerken, dass es hier im Fall des unternehmensfremden externen DSB zu Missverständnissen kam. Die Daten konnten jedoch durch telefonische Rücksprache mit dem Unternehmen präzisiert werden; sie passen jedoch nicht zur allgemeinen Struktur und fließen daher erst weiter unten in die Analyse ein (somit zunächst N=19).

Fokus der Schulungsmaßnahmen

In einem ersten Schritt wurde zunächst geprüft, ob der DSB überhaupt Schulungen durchführt und ob dadurch alle bzw. nur die Mitarbeiter in der Datenverarbeitung erfasst werden. In Unternehmen, deren primärer Geschäftszweck die Informationsverarbeitung ist, muss dabei regelmäßig davon aus-

⁴⁰ BDSG § 4g (1) Satz 3 Nr. 2.

gegangen werden, dass prinzipiell alle Mitarbeiter direkt oder indirekt mit der Verarbeitung personenbezogener Daten befasst sind.⁴² Wie daher zu erwarten war, geben 63% (n=12) – und damit die deutliche Mehrheit – der in der Auswertung befindlichen Unternehmen an, Datenschutzs Schulungen grundsätzlich für alle Mitarbeiter durchzuführen. Zwei Teilnehmer merken dabei an, dass dies in Form eines webbasierten Selbststudienkurses bzw. eines Online-Trainings erfolgt, was aber in ähnlicher Form schon aufgrund der hohen Mitarbeiterzahlen auch bei einigen anderen Unternehmen zumindest partiell zu vermuten ist. Nur 11% (n=2) der Befragten beschränken sich explizit auf die Mitarbeiter in der Datenverarbeitung. In immerhin vier Unternehmen (21%) finden gar keine Schulungen statt (darunter auch jenes mit dem über die Muttergesellschaft bestellten externen DSB). Ein anderer DSB (5%) führt ebenfalls selbst keine Schulungen durch; er weist darauf hin, dass Schulungen nur sporadisch und nach Bedarf über die Konzernmutter erfolgen.

Art der Schulungsmaßnahmen

Im nächsten Schritt wurden die Schulungsmaßnahmen hinsichtlich ihrer Art in die Bereiche *Grundschulungen für alle Mitarbeiter* bzw. *S Schulungen spezieller Zielgruppen*⁴³ unterschieden. Weiterhin konnten, um die Befragung nicht zu sehr einzuschränken, *sonstige Schulungen* durch offene Angaben näher spezifiziert werden. Als Leistungsindikatoren wurden jeweils die Häufigkeit, mit der sie angeboten werden sowie der erreichte Abdeckungsgrad erhoben. Dabei zeigt sich ein uneinheitliches Bild.

Grundschulungen für alle Mitarbeiter

Insgesamt werden in 58% (n=11)⁴⁴ der berücksichtigten Unternehmen Grundschulungen für alle Beschäftigten angeboten. Hinsichtlich der Leistungsparameter ist dabei festzustellen, dass in fünf Unternehmen, darunter die beiden mit den netzgestützten Lösungen, eine jährliche Schulung der Mitarbeiter erfolgt. Der Teilnehmer mit dem Online-Training und ein weiterer

⁴¹ Vgl. BfD (2004b), Nr. 3.4. Vgl. zu einem Schulungs- und Sensibilisierungskonzept Büllesbach, A. (2001).

⁴² Vgl. z.B. DTAG (2004), S. 16, Nr. 2.2.1.1.

⁴³ Denkbare spezielle Zielgruppen stellen z.B. Beschäftigte in datenschutzrechtlich besonders sensiblen Bereichen dar (z.B. System-Administratoren, Mitarbeiter der Personaldatenverarbeitung).

⁴⁴ Im Vergleich zu den vorhergehenden Ergebnissen ist dies ein Teilnehmer weniger. Dieser gibt zwar im ersten Schritt an, Schulungen für alle Mitarbeiter anzubieten, präzisiert hier jedoch explizit nur zielgruppenspezifische Schulungen.

geben dabei einen Abdeckungsgrad von je 80% an. Zwei weitere DSB erreichen durch alle zwei Jahre stattfindende Schulungen einen Abdeckungsgrad von 73% bzw. 75%. In einem anderen Unternehmen erfolgen nur alle zehn Jahre Grundschulungen; es überrascht daher nicht, dass hier nur ein Abdeckungsgrad von 5% erzielt wird. Trotz der wenigen Nennungen wird bereits deutlich, dass die Häufigkeit, mit der die Schulungen angeboten werden, positiv mit dem erreichten Abdeckungsgrad korreliert ist. Zwei weitere Befragte geben an, Grundschulungen nur einmalig für jeden Mitarbeiter durchzuführen und damit einen Abdeckungsgrad von 100% zu erreichen. Demnach kann hier in beiden Fällen die Vermutung aufgestellt werden, dass die Teilnahme an derartigen Grundschulungen durch einen Prozess verbindlich vorgeschrieben wird. Ein weiterer DSB führt zwar Grundschulungen durch, nennt jedoch keine Häufigkeiten.

Schulungen spezieller Zielgruppen

Es zeigt sich, dass in ebenfalls 58% (n=11) der berücksichtigten Unternehmen speziell auf die Bedürfnisse bestimmter Zielgruppen zugeschnittene Datenschutzeschulungen angeboten werden. Wiederum drei DSB führen derartige Schulungen jährlich durch; nur ein Befragter gibt dabei einen konkreten Abdeckungsgrad in Höhe von 95% an. In zwei Unternehmen erfolgt dies alle zwei Jahre mit einem Abdeckungsgrad von 10% bzw. 30%. In einem weiteren alle drei Jahre mit einem Abdeckungsgrad von 70%.

Auch hier erfolgen in zwei Unternehmen solche Schulungen nur einmalig für jede Zielgruppe. Hier wird in einem Fall ein Abdeckungsgrad von 90% und im anderen Fall von nur 5% erreicht. Ein weiterer Befragter führt zielgruppenorientierte Schulungen unregelmäßig nach Bedarf durch. In einem anderen Unternehmen finden ca. zehn spezielle Schulungen pro Jahr statt. Ein DSB gibt zwar wiederum derartige Schulungen an, nennt jedoch auch hier keine Häufigkeiten. Zusätzlich konnte im Rahmen der Befragung als Einzelnennung registriert werden, dass ein DSB über die zielgruppenspezifischen Schulungen hinaus bei Bedarf auch projektbezogene Schulungen durchführt.

Im Fall des unternehmensfremden externen DSB konnte durch telefonische Rücksprache mit dem Unternehmen festgehalten werden, dass für die *Mitarbeiter in der Datenverarbeitung* mindestens einmalig Grundschulungen durchgeführt werden. Bei Bedarf (z.B. durch Änderung von Rahmenbedingungen) erfolgt dies flexibel, d.h. möglicherweise für einige auch jährlich und ggf. auch für *alle Mitarbeiter*. Hierbei wird ein Abdeckungsgrad von ca. 60%

erreicht. Spezielle Zielgruppen in sensiblen Bereichen werden grundsätzlich jährlich geschult. Der Abdeckungsgrad beträgt hier 90%.

Analyse

Betrachtet werden nun die jeweils sieben Unternehmen, die im jeweiligen Bereich paarweise Antworten zur Häufigkeit und dem Abdeckungsgrad der Schulungen übersandten. Dabei sticht bei der Gegenüberstellung dieser beiden Merkmale im Bereich der zielgruppenspezifischen Schulungen die im Gegensatz zu den Grundschulungen außerordentlich breite Streuung des Abdeckungsgrades innerhalb gleicher oder ähnlicher Schulungsintervalle (Häufigkeit alle x Jahre) und insbesondere die dazu festzustellende Unkorreliertheit heraus (vgl. **Tabelle 1**).

Grundschulungen für alle MA		Schulungen spezieller Zielgruppen	
Häufigkeit (alle x Jahre)	Abdeckungsgrad	Häufigkeit (alle x Jahre)	Abdeckungsgrad
einmalig	100%	einmalig	90%
einmalig	100%	einmalig	5%
1	80%	1	95%
1	80%	1(*)	90%(*)
2	75%	2	30%
2	73%	2	10%
10	5%	3	70%

Tabelle 1: Analyse der Schulungsmaßnahmen⁴⁵

Eine formale Ursache hierfür könnte darin zu sehen sein, dass einige der Befragten möglicherweise entweder den Abdeckungsgrad nicht wie intendiert

⁴⁵ Im Rahmen der Analyse der zielgruppenspezifischen Schulungen wurde die Angabe des unternehmensfremden externen DSB nun zur Auswertung hinzugezogen. Sie ist durch einen (*) gekennzeichnet.

An dieser Stelle ist ferner anzumerken, dass sowohl die identische Anzahl von je elf Unternehmen in den beiden Bereichen bzw. von sieben Unternehmen in der Analyse, wie auch die überwiegend identische Anzahl jeweils gleicher Häufigkeitsausprägungen in den beiden Tabellen zufällig ist. Die entsprechenden Angaben stammen größtenteils von verschiedenen Unternehmen.

auf die Zielgruppe bezogen, sondern hinsichtlich der Gesamtzahl der Mitarbeiter interpretiert haben und/oder dass die Häufigkeit hier vereinzelt nicht dahingehend ausgelegt wurde, wie oft der einzelne Mitarbeiter einer Zielgruppe geschult wird, sondern wie häufig der DSB überhaupt zielgruppenspezifische Schulungen durchführt.

Unter pragmatischen Überlegungen ist dies wohl aber auch darauf zurückzuführen, dass bei der entsprechenden Befragung nicht explizit definiert wurde, welche Personengruppen unter die *speziellen Zielgruppen* fallen. Es wurden zwar die auch bereits oben angeführten Beispiele genannt; jedoch ist zu berücksichtigen, dass die tatsächlich erreichte Abdeckung letztendlich erheblich von der Anzahl der wirklich betrachteten Personen abhängt.

(2) *Bestandteil der fachlichen Fortbildung*

Abschließend interessiert in diesem Zusammenhang, welcher Stellenwert dem Datenschutz generell im Rahmen der allgemeinen fachlichen Fortbildung der Mitarbeiter außerhalb der Datenschutzorganisation beigemessen wird. Dabei zeigt sich, dass nur 35% (n=7) der Befragten (N=20) angeben, dass Datenschutzthemen integraler Bestandteil der fachlichen Fortbildung in ihren Unternehmen sind.

Fasst man nun dieses Bild mit dem oben ermittelten Ergebnis zusammen, demgemäß jeder vierte bis fünfte der befragten DSB auch keine Schulungen durchführt, stellt sich die Frage, inwieweit diese Untersuchung womöglich repräsentativ ist und ob sie die Situation in der ganzen Branche widerspiegelt. Immerhin sind Datenschutzeschulungen ein unmittelbar aus dem BDSG abzuleitender Auftrag. Dieses Ergebnis ist daher als äußerst kritisch zu beurteilen.

Vor dem Hintergrund des eingeschränkten Beantwortungsfeldes kann hier keine abschließende Beurteilung erfolgen. Dieser Aufgabenbereich sollte daher einer umfassenderen und insbesondere qualitativen Analyse unterzogen werden, um hier zu belastbaren Aussagen zu kommen.

3.2.3 Beratung und Kontrolle

Der Gesetzgeber hat die Institution des betrieblichen DSB geschaffen, um in weiten Bereichen die Überwachung der Einhaltung des Datenschutzes sozusagen im Rahmen der betrieblichen Selbstkontrolle durchzuführen: „An die Stelle einer ansonsten üblichen bürokratischen, staatlichen Kontrolle tritt eine

innerbetriebliche Kontrollinstanz. Der Datenschutzbeauftragte kennt das Unternehmen, die Prozesse, die Menschen und kann [somit] noch am ehesten beurteilen, wie Datenschutz angemessen sichergestellt werden kann.“⁴⁶ Dass sich dieses Konzept bewährt, bestätigen auch die positiven Ergebnisse der Bewertung der Zusammenarbeit unter den Funktionsträgern im Bereich des Datenschutzes (vgl. Abschnitt 3.1.3 (2)).

(1) Interne Kontrollen

Es ist nicht Aufgabe des DSB dafür zu sorgen, dass möglichst wenig personenbezogene Daten verarbeitet werden, sondern dass die Verarbeitung dieser Daten in Einklang mit den gesetzlichen Vorgaben und dem informationellen Selbstbestimmungsrecht steht.⁴⁷ Seine vorrangige Aufgabe ist daher die Beratung, um die Datenverarbeitung für die Betroffenen so transparent wie möglich zu gestalten und Schwachstellen von vornherein zu vermeiden oder konstruktiv zu lösen.⁴⁸ Er „hat jedoch auch nachträglich die Einhaltung der datenschutzrechtlichen Vorschriften zu überprüfen.“⁴⁹

Zu diesem Zweck kann der DSB interne Kontrollen durchführen. Derartigen Kontrollen kann dabei ein konkreter Anlass zugrunde liegen, sie können aber auch stichprobenartig (nicht anlassbezogen) oder in Form von Auditierungen erfolgen. Im Rahmen der Befragung wurde daher erhoben, ob und wie oft derartige Kontrollen pro Jahr stattfinden.

Um dabei auch dem Gedanken von Datenschutz als Qualitätsmerkmal gerecht zu werden, wurde ferner die z.B. auch im Sinne der ISO 9000⁵⁰ allgemein für Qualitätsmerkmale geforderte Implementierung eines kontinuierlichen und verbindlichen Verbesserungsprozesses sowie das Selbstverständnis der DSB im Rahmen ihrer Kontrollfunktion untersucht.

⁴⁶ Kern, H. (2004).

⁴⁷ Vgl. Kern, H. (2004).

⁴⁸ Vgl. z.B. auch BfD (2004b), Nr. 3.

⁴⁹ BfD (2004b), Nr. 3.3.

⁵⁰ Es sei darauf hingewiesen, dass die ISO 9000 weder die Einhaltung von Datenschutzrecht, noch eine kontinuierliche Verbesserung speziell des Datenschutzes fordert. Sie ist vielmehr darauf ausgerichtet, dem Kunden eine bestimmte Qualität oder Qualitätsprüfung eines Gutes, das man ihm liefert, zu garantieren. Vgl. BMWI (1999), hier den Beitrag von Roßnagel, A.

Art und Umfang der Kontrollen

Zunächst ist hinsichtlich der Art der Kontrollen festzustellen, dass insgesamt 80% (n=16) der befragten DSB anlassbezogene Kontrollen durchführen. Demgegenüber wurden Audits bzw. nicht anlassbezogene Kontrollen nur je neun mal (45%) genannt. Mehrfachnennungen wurden zugelassen, da sich die verschiedenen Kontrollen nicht ausschließen. Vier Teilnehmer (20%) führen dagegen keine internen Datenschutzkontrollen durch.

Betrachtet man nun den Umfang⁵¹ der Kontrollen, lässt sich feststellen, dass dies in drei Unternehmen flexibel bzw. je nach Bedarf, unabhängig von der Art der Kontrollen gehandhabt wird; in einem Fall wird dabei einmal pro Jahr das gesamte Unternehmen (>10.000 Mitarbeiter in D) auditiert. Ferner gibt ein Großkonzern an, pro Jahr bis zu 300 Audits sowie 50 anlassbezogene bzw. 250 nicht anlassbezogene Kontrollen durchzuführen. Ein weiteres Unternehmen führt ebenfalls 50 anlassbezogene, ein anderes 25 nicht anlassbezogene Kontrollen pro Jahr durch. In den verbleibenden Fällen führen fünf DSB zwischen ein und vier Audits, elf DSB zwischen ein und zwölf anlassbezogene und vier DSB nur ein bzw. zwei nicht anlassbezogene Kontrollen pro Jahr durch.

Werden Schwachstellen aufgedeckt, vereinbart die überwiegende Mehrheit der DSB mit den verantwortlichen Personen bzw. den betroffenen Stellen entsprechende Maßnahmen zur Beseitigung der festgestellten Defizite. Dies wird i.d.R. auch überwacht. Lediglich zwei DSB, die nur anlassbezogene Kontrollen durchführen, verzichten auf Maßnahmen und/oder das Monitoring. Der unternehmensfremde externe DSB macht ähnlich eines Audits eine Art Bestandsaufnahme anhand der eine ToDo-Liste abgeleitet wird, die den konkreten Handlungsbedarf an den einzelnen Stellen aufzeigt. Im darauf folgenden Jahr wird dies wiederholt. Insofern findet auch hier ein (überjähriges) Monitoring der vorgeschlagenen Maßnahmen statt.

⁵¹ Fehlende Angaben sowohl zu Umfang als auch Maßnahmen und Monitoring wurden aufgrund der Konstruktion der entsprechenden Frage als „trifft nicht zu“ für die entsprechende Kontrollart interpretiert. Wurden hingegen Maßnahmen und Monitoring markiert, der Umfang jedoch nicht bzw. durch entsprechende Erläuterungen in Textform angegeben, wird dies als flexibel/bei Bedarf angeführt.

Beratung oder „harte Kontrolle“?

Soviel zur Wahrnehmung der Kontrollaufgabe. Die Frage ist nun, wie es dabei mit dem Selbstverständnis der DSB aussieht, denn zweifelsfrei haben diese in den Unternehmen einen Kontrollauftrag mit dem Ziel, die Einhaltung gesetzlicher Vorgaben zu überwachen. Aber sehen sie sich dabei tatsächlich nur als reine Kontrolleure oder mehr als Berater zur Verbesserung des Datenschutzes? Die Ausübung dieser Aufgabe lässt erheblichen Gestaltungsspielraum zu. Die Untersuchung zeigt, dass der Schwerpunkt bei der Durchführung der zuvor genannten Datenschutzkontrollen mit im Mittel 66,25% deutlich bei der Beratung liegt. Der Großteil der DSB will sich somit mehr als Partner im Unternehmen verstanden wissen. Dennoch finden sich neben den ‚Beratern‘ mit in einem Fall sogar bis zu 100 Prozent Beratungsanteil auch drei ‚harte Kontrolleure‘ mit 60 bis 90 Prozent Kontrollanteil.

Die abschließende Beurteilung, ob die Verfolgung spezifischer Datenschutzziele dabei vornehmlich durch eine stark kontrollierende Instanz oder aber im Sinne einer partnerschaftlichen Beratung umzusetzen ist, hängt letztendlich von kulturellen Aspekten ab und muss daher individuell erfolgen.

Es genügt dabei jedoch nicht, nur im Einzelfall tätig zu werden. Vielmehr sollte eine unterstützende Beratung in jedem Fall unter Einbeziehung der Leitungsebene präventiv auf entsprechende Organisationsstrukturen ausgerichtet sein. Die Beratung setzt dabei bereits bei der Datenerhebung an und betrifft alle Bereiche über die Datenverarbeitung, die Institutionalisierung von Unterrichtungspflichten (Schaffung von Transparenz) bis zur Sicherung des Datenschutzrechts durch Technik sowie der Löschung von Daten.⁵²

(2) Auftragsdatenverarbeitung – Kontrolle nach § 11 BDSG

Wenden wir nun den Blick nach außerhalb des Unternehmens. Im Falle der sog. Auftragsdatenverarbeitung ist der Auftraggeber für die Einhaltung des BDSG und anderer Datenschutzvorschriften verantwortlich. Auch wenn die betrachteten Unternehmen zu einem großen Teil selbst Auftragsdatenverarbeiter und somit Auftragnehmer ihrer Kunden sind, ist es doch nicht ungewöhnlich, dass sie ihrerseits ebenfalls bestimmte Tätigkeiten an Dritte auslagern. Und in ihrer Rolle als Auftraggeber haben sie sich wiederum selbst „von der Einhaltung der beim Auftragnehmer getroffenen technischen und

⁵² Vgl. BfD (2004b), Nr. 3.1.

organisatorischen Maßnahmen [zur Gewährleistung des Datenschutzes] zu überzeugen.“⁵³

Untersucht wurde daher, wie häufig und auf welche Art (schriftlich bzw. vor Ort) die Befragten bei ihren Auftragnehmern tatsächlich Datenschutzkontrollen durchführen. Nur in rund zwei Drittel (N=13) der Unternehmen werden dabei überhaupt „personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt“⁵⁴. Deutlich wird, dass davon aber nur rund 15% (n=2) regelmäßig sowohl schriftliche als auch vor Ort Kontrollen bei den Auftragnehmern durchführen. Zwei Unternehmen geben an, die Auftragnehmer nie zu kontrollieren. Dabei ist jedoch anzumerken, dass es sich hierbei in einem Fall beim einzigen Auftragnehmer um die Gehaltsabteilung der Konzernmutter handelt. Die Ergebnisse im Einzelnen können der **Abbildung 13** entnommen werden. Die in der enthaltenen Tabelle angeführten Zahlen in Klammern geben dabei die absolute Anzahl der Nennungen an.

In diesem Zusammenhang erscheint auch interessant, inwieweit die betreffenden Verträge zur Auftragsdatenverarbeitung überhaupt mit dem DSB abgestimmt werden. Leider erweisen sich die Angaben zu der betreffenden Frage in diesem Kontext als nicht eindeutig interpretierbar, da die Fragestellung nicht explizit auf Verträge mit den Auftragnehmern fokussierte. Dennoch sollen die Ergebnisse an dieser Stelle nicht verschwiegen werden (vgl. **Tabelle 2**). Die Aussagekraft ist jedoch dahingehend zu relativieren, dass sich die Antworten ggf. auch auf Verträge mit den Kunden der betrachteten Unternehmen beziehen. Auch hier geben die Zahlen in Klammern die absolute Anzahl an Nennungen an.

Alles in allem wird deutlich, dass bei den Auftragnehmern tendenziell eher selten oder nie kontrolliert wird. Demgegenüber fällt jedoch auf, dass die Situation bei den internen Kontrollen gerade gegenläufig ist. Diese finden der Grundtendenz nach wesentlich häufiger statt, wie der vorausgehende Abschnitt gezeigt hat.

⁵³ BDSG § 11 (2). Einfügung durch den Verfasser.

⁵⁴ BDSG § 11 (1).

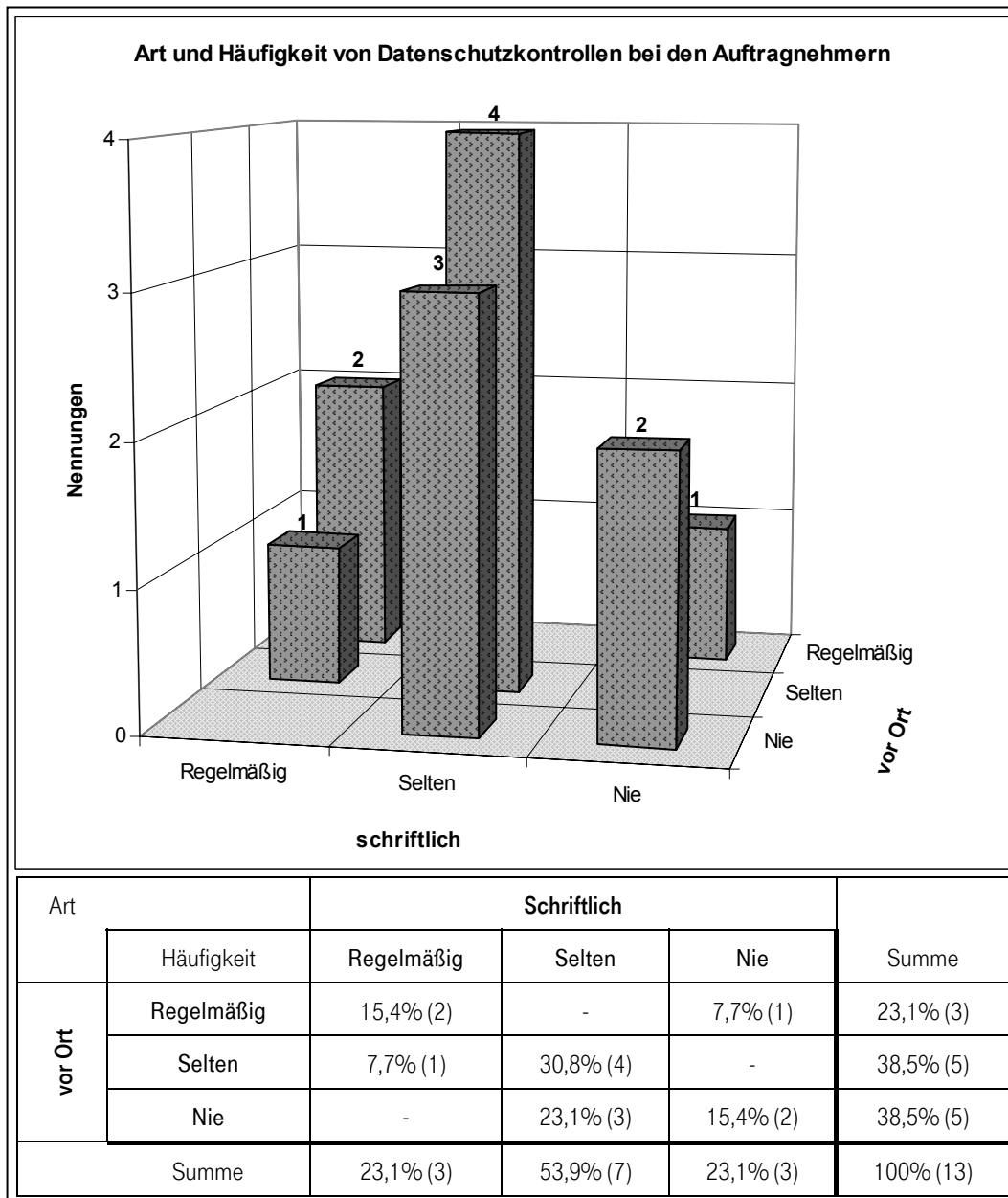


Abbildung 13: Art und Häufigkeit von Datenschutzkontrollen bei den Auftragnehmern

Grundsätzlich	Meistens	Selten	Nie	Summe
38,5% (5)	46,2% (6)	15,4% (2)	-	100% (13)

Tabelle 2: Abstimmung von Verträgen zur Auftragsdatenverarbeitung mit dem DSB

Obwohl ein direkter Vergleich zwar schon allein aufgrund der nominalen Skalierung und aufgrund fehlender qualitativer Daten zu den Kontrollen nicht möglich ist, stellt sich dennoch die grundsätzliche Frage, ob hier ggf. eine Kontrolllücke besteht. Gerade vor dem Hintergrund des Trends zum strategischen IT-Outsourcing⁵⁵ und der damit auch weiterhin zunehmenden Auftragsdatenverarbeitung sollte dieser Bereich einer detaillierteren und insbesondere qualitativen Analyse unterzogen werden, um umfassend zu beurteilen, ob hier tatsächlich eine Lücke be- bzw. entsteht und sich möglicherweise an dieser Stelle zukünftig ein Problem im Datenschutzrecht entwickelt.

3.2.4 Informationspolitik

Eine weitere Aufgabe des DSB ist es, im Unternehmen das nötige Bewusstsein für den Datenschutz zu schaffen. Im Rahmen der Untersuchung wurde daher erhoben, inwieweit von den DSB Informationen zum Thema Datenschutz verbreitet werden, in welcher Form dies erfolgt und wie häufig.

Dabei ist zunächst festzustellen, dass insgesamt 16 (80%) der Befragten (N=20) angeben, überhaupt regelmäßige Informationen zum Datenschutz herauszugeben. Als Formen der Verbreitung wurden Webseiten (Intra-/ Internet), e-Mail, Newsletter sowie Printmedien vorgegeben. Darüber hinaus wurde in einem offenen Feld nach sonstigen Medien gefragt. Bei allen Formen wurde jeweils zwischen interner und externer Veröffentlichung unterschieden.

Das entsprechende Auswertungsergebnis für den Bereich der unternehmensinternen Informationen kann der **Tabelle 3**⁵⁶ entnommen werden. Am häufigsten genannt werden dabei die Webseiten im Intranet (n=15). 13 DSB geben hier absolute Werte an; sie stellen demnach im Mittel knapp sechs Mal im Jahr Informationen ins Intranet ein. Der höchste Wert wurde mit 24 angegeben, was eine durchschnittliche regelmäßige Informationsversorgung im Abstand von rund zwei Wochen bedeutet. Die beiden anderen DSB geben hier in Textform ‚ständig‘ bzw. ‚bei Bedarf‘ an. Den Webseiten folgen im Mittel rund drei bis vier e-Mails bzw. Newsletter im Jahr (ein DSB gibt hier ebenfalls in beiden Fällen ‚bei Bedarf‘ an), während die Printmedien mit nur

⁵⁵ Vgl. Huber, A. (2004); einen Überblick über häufige Gründe zum IT-Outsourcing geben Mauch, C./Wildemann, H. (2004), S. 33f.

vier Nennungen aufgrund des größeren Aufwands erwartungsgemäß das Schlusslicht bilden.

Über die vorgegebenen Formen hinaus konnten die beiden Einzelnennungen Mitarbeiter-Info (einmal jährlich) und Anweisungen (sechs Mal pro Jahr) registriert werden.

Form der Verbreitung	Anzahl der Nennungen	Maximale Häufigkeit (pro Jahr)
Webseiten (Intranet)	13 (+2)	24
e-Mail	6 (+1)	6
Newsletter	5 (+1)	8
Printmedien	4	6

Tabelle 3: Form und Häufigkeit der internen Informationsverbreitung⁵⁷

Externe Informationen werden dagegen nur von wenigen DSB veröffentlicht. So geben fünf Befragte an, einmal jährlich auch Informationen auf Webseiten ins Internet einzustellen. Zwei DSB versenden einen bzw. zwölf Newsletter im Jahr. Ein weiterer veröffentlicht zwei Mal im Jahr in Printmedien.

3.2.5 Verfahrensverzeichnis

Dem DSB sind durch die verantwortliche Stelle bestimmte Angaben über die Informationsverarbeitungsverfahren im Unternehmen zu machen. Grundlage hierfür ist eine Vorgabe des BDSG, wonach dem Beauftragten für den Datenschutz von der verantwortlichen Stelle eine Übersicht der Verfahren⁵⁸

⁵⁶ Die an den Stichprobenumfang von N=16 jeweils fehlenden Teilnehmer trugen entweder eine Null ein oder machten keine Angaben im entsprechenden Feld. Dies wurde hier aufgrund der Konstruktion der entsprechenden Frage als „trifft nicht zu“ interpretiert.

⁵⁷ Die bei der Anzahl der Nennungen in Klammern angeführten Werte kennzeichnen verbale Nennungen, die nicht in die statistischen Berechnungen der Abweichungen mit einfließen.

⁵⁸ Der Begriff des „Verfahrens“ wird im Gesetz selbst nicht definiert. „Abgeleitet aus Art. 18 Abs. 1 der EU-Richtlinie 95/46 EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 hat sich die folgende Definition durchgesetzt: „Unter Verfahren ist die

automatisierter Verarbeitungen sowie über zugriffsberechtigte Personen zur Verfügung zu stellen ist.⁵⁹ Das Führen eines sog. Verfahrensverzeichnisses setzt diese Anforderungen des BDSG um. Es stellt eine wichtige Übersicht für den DSB dar und dient zugleich der Schaffung von Transparenz in der Datenverarbeitung.⁶⁰ Aufgabe des DSB ist es, den öffentlichen Teil dieser Angaben auf Antrag jedermann in geeigneter Weise verfügbar zu machen.

Umsetzung

Im Rahmen der Untersuchung wurde dabei zunächst erhoben, ob und in welcher Form (elektronisch, manuell oder anders) ein Verfahrensverzeichnis geführt wird.⁶¹ Nur 70% (n=14) aller befragten Unternehmen geben an, ein elektronisches Verfahrensverzeichnis implementiert zu haben. Dementsprechend haben manuell geführte Verzeichnisse, die sich in 25% (n=5) der Unternehmen finden, erwartungsgemäß eine untergeordnete Bedeutung. Drei (15%) der Unternehmen, erfüllen die Anforderung des BDSG zum Zeitpunkt der Erhebung nicht, zwei davon planen bzw. untersuchen jedoch die Einführung eines Verfahrensverzeichnisses. Da Mehrfachnennungen möglich waren, pflegen zwei Unternehmen somit offensichtlich beide Varianten. In einem weiteren Unternehmen ist die Umstellung bereits angedacht. Die Möglichkeit, eine andere Form durch offene Antwort zu spezifizieren, wurde nicht genutzt. Interessant wäre an dieser Stelle, den Abdeckungsgrad des Verfahrensverzeichnisses zu untersuchen, wie von einem Teilnehmer im Fragebogen vorgeschlagen wurde.

Gesamtheit an Verarbeitungen zu verstehen, mit denen eine oder mehrere miteinander verbundene Zweckbestimmung(en) realisiert werden sollen. Ein Verfahren kann danach eine Vielzahl von Datenverarbeitungsdateien umfassen“. Als Beispiele für Verfahren können danach Personalverwaltungs-, Betreuungs- und Abrechnungssysteme, Verfahren zur Abwicklung von Kundenaufträgen, Telekommunikationssysteme, Teledienste und sonstige Systeme, die eine geschlossene Struktur von Verarbeitungen umfassen, genannt werden.“ BfD (2004b), Nr. 3.5.

⁵⁹ Vgl. BDSG § 4g (2). Den Inhalt dieser Angaben regelt § 4e Satz 1 Nr.1 bis 9 BDSG.

⁶⁰ Vgl. BfD (2004b), Nr. 3.5.

⁶¹ An dieser Stelle ist anzumerken, dass die beiden Formen ‚elektronisch‘ bzw. ‚manuell‘ nicht trennscharf gewählt wurden. Unter der berechtigten Annahme, dass nicht mehr zeitgemäße Formen wie z.B. Karteikartensysteme in den untersuchten Unternehmen ausgeschlossen werden dürfen, wird im Kontext dieser Befragung unter einem manuellen Verfahrensverzeichnis daher z.B. die Pflege einer Excel-Liste verstanden, wohingegen unter einem elektronischen Verfahrensverzeichnis eine dezentrale Erfassung der Angaben verstanden wird.

Akzeptanz

Ferner wurde die grundsätzliche Akzeptanz dieser gesetzlichen Vorgabe untersucht. Gefragt wurde dabei, wie der DSB das Führen eines Verfahrensverzeichnis einschätzt. Dabei sehen 79% der 19 Antwortenden das Verfahrensverzeichnis für *sinnvoll* an. Als *praktikabel* bzw. *verhältnismäßig* wird es hingegen nur zu je 58% eingestuft. Nur ein Befragter machte hier keine konkreten Angaben. Er nutzte jedoch die ebenfalls angebotene Möglichkeit, eine offene Einzeleinschätzung abzugeben, verwies dort aber lediglich darauf, dass alle Angaben von der Unternehmensgröße und -struktur abhingen. Die absoluten Häufigkeiten der einzelnen Nennungen sind der **Abbildung 14** zu entnehmen.

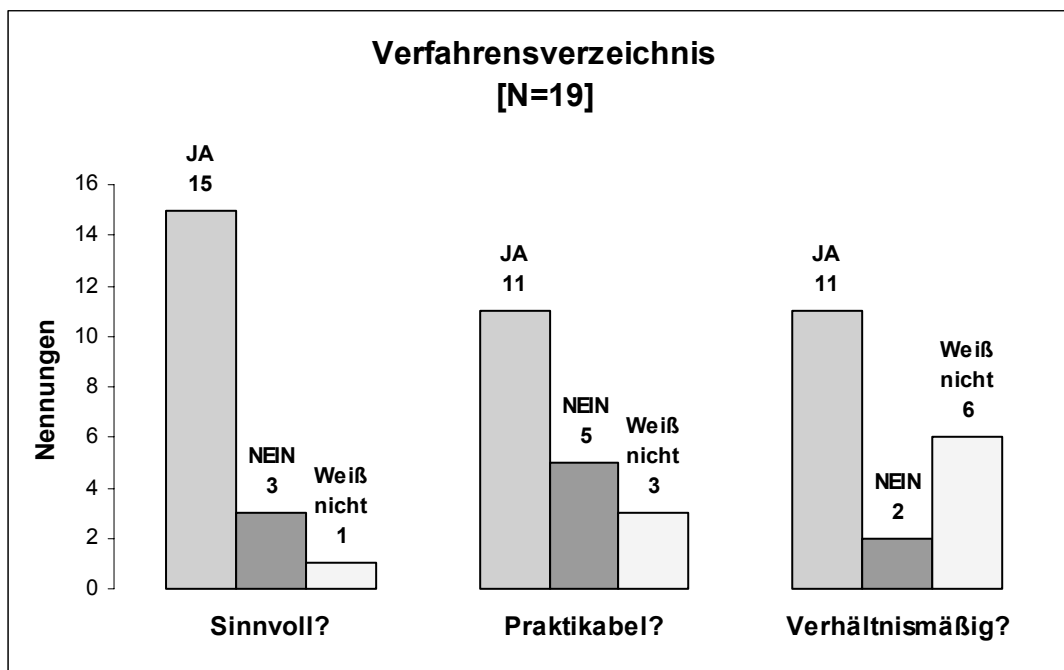


Abbildung 14: Verfahrensverzeichnis

Während zum Sinn dieser Einrichtung noch eine breite Zustimmung zu verzeichnen ist, hält nur eine knappe Mehrheit das Führen des Verfahrensverzeichnisses auch für praktikabel bzw. verhältnismäßig. Dies spiegeln auch die offenen Angaben wider. So stellt das Verfahrensverzeichnis für einen Befragten die erste Möglichkeit dar, um überwachend und steuernd auf die Verarbeitung personenbezogener Daten im Unternehmen einzuwirken. Nur so könnten frühzeitig die datenschutzrechtliche Zulässigkeit eines Datenverarbeitungsverfahrens und die zur Datensicherheit getroffenen Maßnahmen beurteilt werden. Für einen anderen DSB ist das Verfahrensverzeichnis allein

schon deshalb wichtig, um überhaupt Informationen darüber zu erhalten, in welchen Systemen personenbezogene Daten verarbeitet werden. Dabei ist er aber auf die Unterstützung in den Fachabteilungen angewiesen, die das mitunter eher als lästig empfinden.

Ein Verfahrensverzeichnis macht nur dann Sinn, wenn es den DSB in seiner Arbeit unterstützt. Dazu müsste es nach Meinung einiger Befragter jedoch mehr und detailliertere Informationen enthalten, als es im Gesetz vorgeschrieben ist. Da es sich um stark zusammengefasste und dadurch auch verkürzte Informationen handle, lieferten diese Daten letztlich keinerlei tiefere Erkenntnisse. Sinnvoller erscheint es daher manchem Teilnehmer, den Schwerpunkt auf die rechtzeitige Information über die Einführung oder Veränderung von Verarbeitungen personenbezogener Daten zu legen - und ggf. deren Dokumentation.

Die DSB der beiden Unternehmen, die die Einführung eines Verfahrensverzeichnisses planen bzw. untersuchen, stehen diesem Vorhaben zwar grundsätzlich positiv gegenüber, einer der Befragten stuft jedoch insbesondere den Anfangsaufwand dabei als unverhältnismäßig hoch ein. In einem anderen Unternehmen ist zu verzeichnen, dass die Anwendung einer elektronischen Variante die Akzeptanz und Praktikabilität des Verfahrensverzeichnisses allgemein erhöhen konnte.

Praktische Probleme anderer Art sieht ein DSB besonders darin, in einem weltweit agierenden Unternehmen, dessen Schwerpunkt und Richtlinienkompetenz nicht in Deutschland liegt, ein Verfahrensverzeichnis zu führen. Dies gelte insbesondere bei Verfahren, die Kundendaten betreffen.

Zusammengefasst lässt sich feststellen, dass lediglich ein DSB dem Verfahrensverzeichnis gänzlich ablehnend gegenübersteht und es für zu bürokratisch hält. Im Übrigen lässt sich eine positive Grundtendenz ausmachen, jedoch mit z.T. deutlichen Defiziten in der praktischen Umsetzung.

3.3 Unternehmenspolitischer Auftrag

Um die strategische Ausrichtung des Datenschutzes in den Unternehmen nicht nur auf Basis der gesetzlichen Regelungen beurteilen zu können, wurden verschiedene weitere Indikatoren identifiziert, die Anhaltspunkte dafür liefern können, wie ernst es ein Unternehmen mit dem Datenschutzmanagement nimmt. Logische Konsequenz eines als Corporate Value Factor verstandenen Datenschutzes, wie er einleitend dargestellt wurde, ist dabei insbesonde-

re ein im Einzelfall auch über die gesetzlichen Anforderungen hinausgehender unternehmenspolitischer Auftrag der Datenschutzorganisation. Die Frage, wie der Datenschutz und damit auch der DSB im Unternehmen verankert ist, hängt daher letztendlich eng mit der Existenz eines solchen unternehmenspolitischen Auftrags durch ein Mandat der Geschäftsführung zusammen.

3.3.1 Institutionalisation

Ein Indiz, inwiefern der Datenschutz Bestandteil der internen Kommunikation und der Querschnittsprozesse ist, liefert daher dessen Institutionalisation im Unternehmen. Wie bei der Untersuchung deutlich wird, ist der Datenschutz in immerhin 65% (n=13) der befragten Unternehmen (N=20) durch ein Fachkonzept bzw. einen Beschluss der Geschäftsleitung konzeptionell beschrieben.

Der DSB ist gemäß BDSG der Geschäftsführung als Leitung der verantwortlichen Stelle unmittelbar unterstellt⁶² und verfügt jederzeit über ein direktes Vortragsrecht.⁶³ Im Rahmen der Befragung wurde daher untersucht, ob die DSB auch tatsächlich direkt an ihre Geschäftsleitung berichten und wie oft.

Dies wird in immerhin 85% (n=17) der untersuchten Unternehmen (N=20) gemäß BDSG umgesetzt. Während die Hälfte (n=10) der DSB jedoch nur zwischen ein und vier mal pro Jahr berichtet, liefert in knapp über einem Drittel (n=7) der Unternehmen der DSB dem Management mindestens im Abstand von zwei Monaten bzw. in einem Fall sogar wöchentliche Berichte (vgl. **Abb. 15**).

Wenngleich hier auch keine qualitative Unterscheidung, d.h. in welcher Form (z.B. schriftlich oder durch ein persönliches Gespräch) die Berichte erfolgen, vorgenommen wurde, zeigt sich dennoch eine massive Streuung der Aufmerksamkeit, die dem Datenschutz durch das Management entgegengebracht wird.

⁶² Wie bereits angemerkt, ist der DSB dabei allerdings in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Vgl. BDSG § 4f (3).

⁶³ Vgl. BfD (2004b), Nr. 2.2; BDSG § 4f (3).

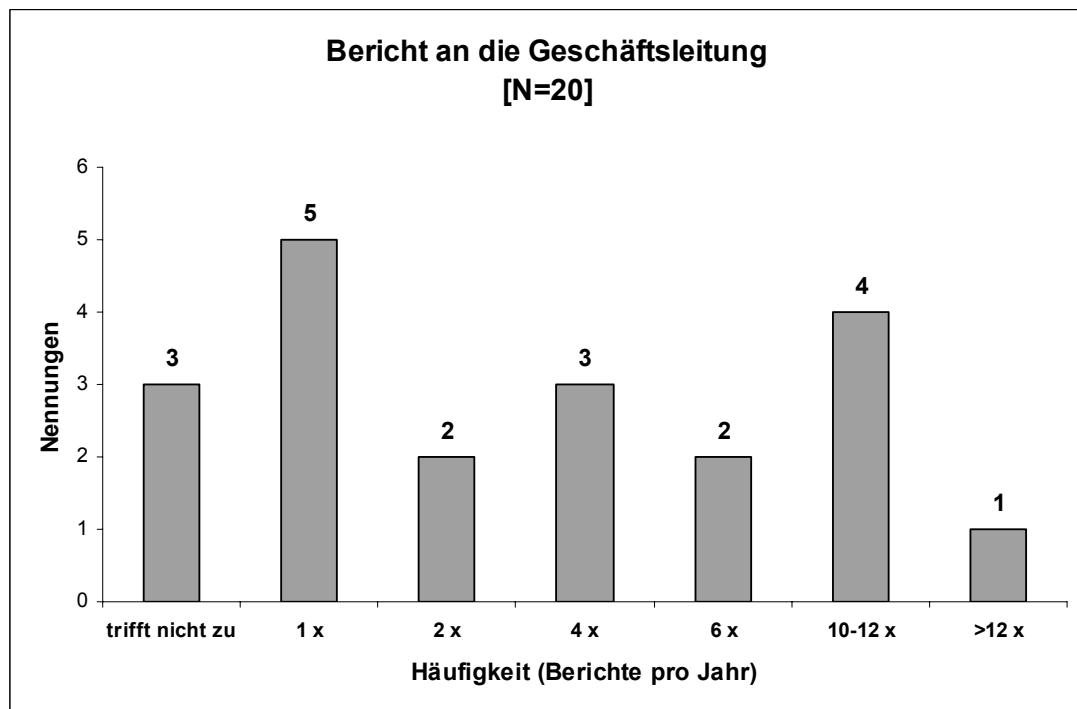


Abbildung 15: Bericht an die Geschäftsleitung

Jahresbericht

Einen Jahresbericht an die Geschäftsführung liefern 80% (n=16) der befragten DSB, wobei hier keine Korrelation zur direkten Berichterstattung festzustellen ist. Untersucht wurde hier auch, welche Art von Informationen die Jahresberichte an die Geschäftsleitung enthalten. Bei den im Folgenden angeführten, vorgegebenen Ausprägungen wurden Mehrfachnennungen akzeptiert. Die Zahlen in Klammern geben dabei die absoluten Häufigkeiten der Nennungen an:

- Tätigkeitsbericht (12),
- Allgemeine Beschreibung der Lage des Datenschutzes im Unternehmen (11),
- Einschätzung der Umfeldentwicklung bzw. Ausblick (7).

Außerdem konnten über die vorgegebenen Antwortmöglichkeiten hinaus noch zusätzliche Angaben gemacht werden. Genannt wurden von zwei DSB laufende Berichte und Involvierung in Projekte und eine sofortige Information der Geschäftsleitung über aktuelle Probleme per e-Mail. Ein DSB klärt die Geschäftsleitung im Jahresbericht nur über Aufgaben und Risiken auf. Da er

jedoch im Abstand von zwei Monaten direkt berichtet, lässt dies detailliertere Informationen an dieser Stelle vermuten.

Der DSB eines großen Unternehmens liefert hingegen keinen Jahresbericht. Er hält die Geschäftsleitung durch regelmäßige schriftliche und mündliche Information auf dem aktuellen Stand. Ebenso der extern über die Konzernmutter bestellte DSB, der nur von Fall zu Fall berichtet.

3.3.2 Leistungen

Der folgende Abschnitt widmet sich den durch den DSB bzw. die Datenschutzorganisation der befragten Unternehmen erbrachten Leistungen. Dabei ist anzumerken, dass es auch hier im Fall des unternehmensfremden externen DSB zu Missverständnissen kam, die jedoch auch durch telefonische Nachfrage nicht restlos aufgeklärt werden konnten. Die Beantwortung der diesbezüglichen Fragen erfolgte bei diesem Teilnehmer z.T. aus Sicht des externen DSB. Gefragt wurde jedoch nach Leistungen, die durch das befragte Unternehmen am Markt erbracht werden. Um das Ergebnis nicht zu verfälschen, fließen die Angaben dieses Teilnehmers im Rahmen der Untersuchung der Leistungen nicht mit ein (somit N=19).

(1) Leistungsdefinition

Im Rahmen der Untersuchung der Leistungen wurde einleitend gefragt, ob es eine Richtlinie gibt, welche die Aufgaben des DSB beschreibt⁶⁴ und ob die Leistungen in einem Datenschutz-Dienstleistungsangebot (Service Offering Portfolio) definiert sind. Die Mehrheit von 63% der befragten DSB (n=12) gibt dabei an, dass es eine derartige Richtlinie gibt; auf ein definiertes Service Offering Portfolio trifft man in diesem Zusammenhang dagegen nur in knapp 37% der Unternehmen (n=7).

Ferner ist dabei von Interesse, in welchem Umfang die Datenschutzorganisation auch Kundenprojekte betreut. Zwar ist es Aufgabe des DSB, im Rahmen der Auftragsdatenverarbeitung Beratungsleistung *für das eigene Unternehmen* auch in Kundenprojekten zu erbringen (z.B. Vertragsgestaltung und -prüfung im Hinblick auf § 11 BDSG).⁶⁵ Diese Frage zielte jedoch auf den

⁶⁴ Eine solche Richtlinie ergibt sich potentiell aus der Operationalisierung der Vorgaben des BDSG für die Anwendung im Unternehmen und/oder einem erweiterten unternehmenspolitischen Auftrag.

⁶⁵ Vgl. BfD (2004b), Nr. 3.1.

Umstand ab, dass es dagegen nicht zu den gesetzlichen Aufgaben des DSB gehört, Beratungsleistungen *für Kunden* des Unternehmens zu erbringen (z.B. die Erstellung von Datenschutzkonzepten oder Schulungen). Denn wie bereits an anderer Stelle dargestellt wurde, ist für die Sicherstellung der ordnungsgemäßen Verarbeitung personenbezogener Daten im Rahmen der Auftragsdatenverarbeitung der DSB des Kunden zuständig. Vor diesem Hintergrund ist festzustellen, dass insgesamt 42% (n=8) der untersuchten Unternehmen ihre Kunden in dieser Hinsicht unterstützen und Beratungsleistungen auch über den gesetzlichen Auftrag hinaus erbringen.

Interessant erscheint an dieser Stelle, das Ergebnis einer Clusteranalyse zu unterziehen. Das auf die einzelnen Branchenbereiche aufgeschlüsselte Auswertungsergebnis kann der **Abbildung 16** entnommen werden.

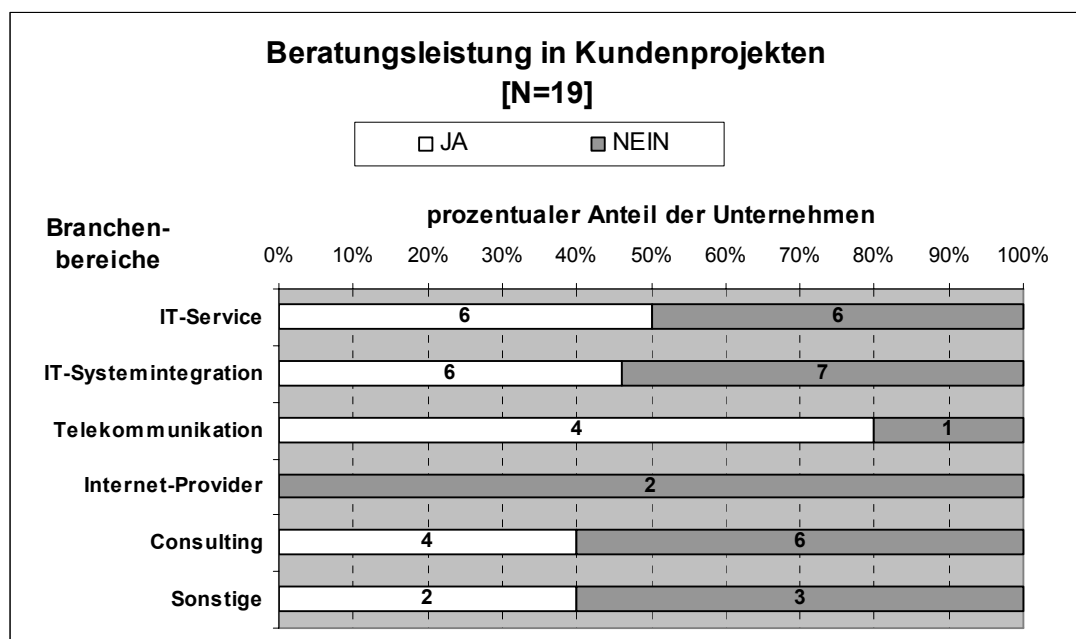


Abbildung 16: Beratungsleistung in Kundenprojekten

Die in den Balken angetragenen Werte spiegeln dabei die jeweilige absolute Anzahl der Nennungen wider. Deutliche Abweichungen vom prozentualen Gesamtwert sind jedoch nur bei den Telekommunikations-Unternehmen nach oben bzw. den Internet-Providern nach unten zu beobachten. Aufgrund der geringen Anzahl an Nennungen dieser beiden Marktsegmente können hieraus jedoch keine weiteren Schlüsse gezogen werden.

(2) Leistungen am Markt

Ferner wurde untersucht, ob und zu welchem Preis Leistungen auf dem Markt angeboten bzw. erbracht werden und ggf. um welche Art von Leistungen es sich dabei handelt. Von sechs der 19 berücksichtigten Unternehmen bleibt diese Frage unbeantwortet und sieben weitere geben an, dass sie keine Leistungen am Markt anbieten. Somit verbleiben in dieser Auswertung letztendlich nur sechs Unternehmen. Dabei wurden die im Folgenden angeführten möglichen Leistungen vorgegeben. Die Zahlen in Klammern geben die absoluten Häufigkeiten der jeweiligen Nennungen an, da Mehrfachnennungen akzeptiert wurden:

- Beratung (5),
- Schulungen (4),
- Datenschutzfreundliche Produkte bzw. Technologien (4),
- Bestellung zum externen DSB (2).

Außerdem konnten weitere sonstige Leistungen durch offene Angaben näher spezifiziert werden. Dies wurde nur von einem Teilnehmer genutzt. Er konkretisierte darin den einzigen von ihm genannten Punkt *Beratung* hinsichtlich Beratung von Projektteilnehmern. Marktpreise für die angebotenen Leistungen wurden nur von zwei Unternehmen genannt. Sie berechnen Stundensätze in Höhe von 120 bzw. 123 EUR.

Interessant an dieser Stelle ist, dass hier ein deutlicher Zusammenhang zwischen der personellen Ausstattung der Datenschutzorganisation und der Häufigkeit der Nennungen o.g. Leistungen erkennbar ist. Mit dem erweiterten Aufgabengebiet geht regelmäßig auch eine personelle Ausstattung mit mehr als 1,5 Mannjahren einher. Bezüglich der Zuordnung der angebotenen Leistungen zu den Branchenbereichen zeigt sich dabei, dass die betreffenden Unternehmen nahezu ausschließlich aus den Bereichen IT-Service, Beratung und IT-Systemintegration kommen.

(3) Datenschutzfreundliche Produkte bzw. Technologien

Datenvermeidung und Datensparsamkeit spielen bei der Entwicklung und der Anwendung von IKT bisher nur eine untergeordnete Rolle.⁶⁶ Einen hinsicht-

⁶⁶ Vgl. Ernestus, W. et al. (1997), S. 14, Nr. 6.

lich des Leistungsportfolios bisher eher akademisch-abstrakten Gegenstand der Diskussion in Datenschutzfachkreisen stellt in diesem Zusammenhang die Entwicklung sog. datenschutzfreundlicher Produkte bzw. Technologien⁶⁷ dar. Nicht klar definiert ist dabei, ob es sich hier ausschließlich um bereits im Einsatz befindliche praktische Anwendungsfälle bzw. technische Systeme handeln soll oder ob der Begriff vielmehr auch innovative Entwicklungen umfasst, die z.B. jedem Bürger die Ausübung seines informationellen Selbstbestimmungsrechts im Einzelfall gewährleisten sollen. Zumindest von letzteren sind bislang keine oder kaum Produkte auf dem Markt zu finden.

Erhoben wurde daher, wie die Sicht der Praxis dazu ist und ob die Unternehmen tatsächlich eigene datenschutzfreundliche Produkte bzw. Technologien entwickeln. Die Frage wurde dabei bewusst sehr allgemein gehalten, um zu sehen, ob hier überhaupt nennenswerte Aktivitäten stattfinden. Wie sich dabei zeigt, wird immerhin von rund einem Drittel der Unternehmen angegeben, eigene datenschutzfreundliche Produkte bzw. Technologien zu entwickeln. Die Clusteranalyse liefert auch hier vorwiegend IT-Service-, Beratungs- und IT-Systemintegrationsunternehmen. Dieses Thema sollte daher ggf. im Rahmen einer zukünftigen Untersuchung näher beleuchtet werden.

Im Gegensatz zum Ergebnis der vorhergehenden Auswertung zeigt sich hier überraschenderweise kein eindeutiger Zusammenhang zur personellen Ausstattung. Denn sowohl zwei Datenschutzorganisationen mit weniger als 0,5 Mannjahren als auch drei mit mehr als 1,5 Mannjahren bejahen diese Frage und entwickeln also entsprechende Produkte bzw. Technologien.

(4) Leistungsverrechnung

Abschließend wurde erhoben, wie die von der Datenschutzorganisation erbrachten Leistungen dem Leistungsempfänger letztendlich berechnet werden bzw. wie die Finanzierung erfolgt. Im Rahmen der innerbetrieblichen Leistungsverrechnung wurden lediglich allgemein *Verrechnungspreise*⁶⁸ und/oder *Umlagefinanzierung* unterschieden. Darüber hinaus konnten offene Angaben gemacht werden. Mehrfachnennungen wurden ausdrücklich zugelassen, falls Leistungen ggf. nur teilweise verrechnet werden. Denkbar wäre dies etwa bei Beratungsleistungen in internen Projekten, wohingegen Basisleistungen wie

⁶⁷ Vgl. für einen Überblick zu diesem Thema z.B. Ernestus, W. et al. (1997) sowie Jandach, T. et al. (1997).

⁶⁸ Vgl. zur Funktion von Verrechnungspreisen z.B. Coenenberg, A. G. (1999), S. 523ff.

z.B. Grundschulungen für alle Mitarbeiter durch Schlüssel umgelegt werden könnten.

Sieben der 19 in der Auswertung befindlichen Unternehmen übersandten hierzu keine Antworten. Zwei Befragte machen nur die Angabe ‚keine Verrechnung‘ bzw. ‚anders‘; ein weiterer trifft widersprüchliche Aussagen und kann daher nicht mit einbezogen werden. Von den verbleibenden neun Unternehmen verrechnen sieben (78%) die Leistungsbeziehungen der Datenschutzorganisation mit anderen Organisationseinheiten durch Umlage und nur vier (44%) über Verrechnungspreise. Deren Höhe wird von drei der Befragten mit einem Stundensatz in Höhe von 70, 95 und 100 EUR beziffert. Wie aus den Ergebnissen bereits ersichtlich wird, kommen somit in zwei der betrachteten Unternehmen beide Verfahren zum Einsatz. Die zuvor angestellte Überlegung, dass womöglich beide Varianten zum Einsatz kommen, wird somit durch die empirischen Ergebnisse bestätigt. Ein Zusammenhang zur Frage, ob Leistungen am Markt erbracht werden, lässt sich nicht feststellen. Im Übrigen beträgt der Tagessatz des unternehmensfremden externen DSB 1.350 EUR.

3.3.3 Lobbying

Das Verständnis und die Fortentwicklung von Datenschutz und Informationssicherheit als Wettbewerbs- und Qualitätsbestandteil verlangt die Interessen von Unternehmen, Mitarbeitern, Kunden und Geschäftspartnern in die politische Diskussion einzubringen, um so eine vernünftige Verzahnung zwischen gesellschaftspolitischen und wirtschaftlichen Anforderungen zu gewährleisten.⁶⁹ Die Analyse der strategischen Ausrichtung des Datenschutzes erfordert daher auch eine Untersuchung der politischen Interessensvertretung durch die DSB.

Dabei zeigt sich, dass immerhin in rund 63% (n=12) der berücksichtigten Unternehmen (N=19) der DSB versucht, die Interessen des Unternehmens in die Gestaltung von Datenschutzrechtsnormen einzubringen. Knapp 37% (n=7) der Befragten verneinen dagegen derartige Versuche. Nur im Fall des unternehmensfremden externen DSB lag hierzu keine Angabe vor.

In diesem Zusammenhang erscheint auch die Mitgliedschaft des DSB bzw. des Unternehmens in spezifischen Interessensverbänden und Organisatio-

nen interessant. Insgesamt am häufigsten genannt wurde dabei die Gesellschaft für Datenschutz und Datensicherung e.V. (GDD). Vier DSB sind eigenen Angaben zufolge nicht Mitglied eines Interessensverbandes. Einer der Befragten gibt seine GDD-Mitgliedschaft über die Konzernmutter an; ein weiterer verweist ohne konkrete Nennungen ebenfalls auf die Muttergesellschaft. Ferner konnte eine Einzelnennung der Organisation „SAVE“ registriert werden. Die Ergebnisse der entsprechenden Befragung können der **Tabelle 4** entnommen werden.

Name der Organisation	Nennungen
Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)	12
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)	6
Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)	2
eco Electronic Commerce Forum - Verband der deutschen Internetwirtschaft e.V.	1
Sonstige: SAVE	1

Tabelle 4: Mitgliedschaft in Interessensverbänden

3.3.4 Verpflichtung auf das Datengeheimnis

Die Verpflichtung zur Einhaltung des Datengeheimnisses ergibt sich aus § 5 BDSG: Hiernach ist es den „bei der Datenverarbeitung beschäftigten Personen [...] untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind [...] bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.“⁷⁰ Die Pflicht zur Wahrung des Datengeheimnisses besteht auch über die Beendigung ihrer Tätigkeit hinaus.

⁶⁹ Vgl. Büllesbach, A. (2002), S. 54f.

⁷⁰ BDSG § 5.

Unbefugt ist die Datenverarbeitung oder sonstige Nutzung personenbezogener Daten, wenn kein Erlaubnistatbestand vorliegt, d.h. wenn diese Vorgänge nicht erforderlich sind oder außerhalb des ursprünglichen Zwecks der jeweiligen rechtmäßigen Aufgabenerfüllung vollzogen werden.

Im Rahmen der Untersuchung wurde die Häufigkeit bzw. die zeitlichen Abstände erhoben, mit der bzw. in denen die Beschäftigten auf das Datengeheimnis verpflichtet werden. Nur ein Teilnehmer machte hier keine Angabe. Zunächst kann festgestellt werden, dass alle verbleibenden 19 Unternehmen der Verpflichtung der Beschäftigten auf das Datengeheimnis nachkommen. In der überwiegenden Mehrheit (68%, n=13) der betrachteten Unternehmen (N=19) erfolgt dies jedoch nur einmalig zu Beginn des Anstellungsverhältnisses. Lediglich ein Viertel (n=5) der Unternehmen verpflichten ihre Beschäftigten wiederholt und in regelmäßigen Abständen auf das Datengeheimnis. Die genannten Ausprägungen reichen dabei von der jährlichen bis zur alle fünf Jahre erfolgenden Verpflichtung. Im Fall des unternehmensfremden externen DSB werden alle Beschäftigten grundsätzlich mindestens zu Beginn des Anstellungsverhältnisses verpflichtet, wohingegen Mitarbeiter in speziellen Bereichen wie z.B. in der Datenverarbeitung auch hier jährlich erneut verpflichtet werden.

Vor dem Hintergrund der Schlüsselfunktion, die der Schutz von Informationen und personenbezogenen Daten für die Unternehmen in den umkämpften ITK-Märkten einnimmt, zeigt dieses Ergebnis Raum für Verbesserungen. Es reicht hier eben nicht, sich auf die Einhaltung gesetzlicher Minimalanforderungen zu beschränken.

Wie schon an anderer Stelle angeführt, ist in den Unternehmen dieses Sektors regelmäßig davon auszugehen, dass nahezu alle Mitarbeiter unmittelbar oder mittelbar Umgang mit personenbezogenen Daten haben. Im Sinne einer auf permanente Verbesserung des Datenschutzes ausgerichteten Unternehmenspolitik ist es daher angebracht, sämtliche Beschäftigten nachweislich und regelmäßig in periodischen Abständen auf das Datengeheimnis zu verpflichten. Eine entsprechende Unterweisung kann dabei aus unternehmenspolitischen Erwägungen mit einer Grundschulung verbunden und so die gesetzlich vorgesehene Verpflichtung⁷¹ als Sensibilisierungsmaßnahme für alle Mitarbeiter ausgestaltet werden.⁷²

⁷¹ Eine besondere Form der Verpflichtung ist im Gesetz nicht vorgeschrieben. Aber schon aus Beweiszwecken empfiehlt sich eine persönliche, schriftliche Verpflichtung des Mitarbeiters. Vgl. Glossner, S. (2004), S. 345, Rdnr. 26.

⁷² Vgl. DTAG (2004), S. 16, Nr. 2.2.1.1; Königshofen, T. (2002), S. 58.

4 Übermittlung personenbezogener Daten ins Ausland

Gemeinsame Märkte und globalisierte Wirtschaftsbeziehungen führen auch zu einer erheblichen Zunahme grenzüberschreitender Datenübermittlungen sowohl innerhalb als auch zwischen weltweit operierenden Organisationen. Insbesondere beim Outsourcing ist dabei eine Verlagerung der Datenverarbeitung an Stellen im Ausland (z.B. in Niedriglohnländer) immer häufiger anzutreffen.⁷³

In diesem Kontext interessiert vor dem Hintergrund der besonderen datenschutzrechtlichen Herausforderungen⁷⁴ bei der Übermittlung personenbezogener Daten ins Ausland, wo in den hier untersuchten Unternehmen eine Datenübermittlung stattfindet. Grundsätzlich sind dabei verschiedene Szenarien und Anlässe für derartige Übermittlungen denkbar (z.B. Austausch von Kunden- oder Personaldaten zwischen einzelnen Standorten oder zur Durchführung von Kundenprojekten). Ein Szenario, dem besonders im IT-Sektor aktuell große Bedeutung zukommt, ist das Offshoring⁷⁵, da sich der Anteil

⁷³ Vgl. z.B. Glossner, S. (2004), S. 346, Rdnr. 29; Mauch, C./Wildemann, H. (2004), S. 32.

⁷⁴ Eine zentrale Herausforderung für global agierende Unternehmen stellen in diesem Zusammenhang die Artikel 25 und 26 der EG-Datenschutzrichtlinie dar. Diese regeln die Frage der Zulässigkeit von der EU und damit auch von Deutschland ausgehender Datenübermittlungen. Insbesondere eine Datenübermittlung an sog. Drittstaaten, also an Stellen außerhalb der EU, ist dabei nur dann zulässig, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist oder der Betroffene einwilligt bzw. die Übermittlung im Rahmen einer Vertragsabwicklung erfolgt. Diese Regelungen vermögen jedoch weite Bereiche der unternehmensinternen Kunden- und Personaldatenverarbeitung nicht zu erfassen. Eine weitere Möglichkeit stellen hier bestimmte Schutzgarantien in Form von speziellen Vertragsklauseln oder verbindliche Unternehmensrichtlinien (Code of Conduct) dar. Vgl. dazu sowie zu den Rechtsgrundlagen und den Handlungsoptionen globaler Unternehmen bei der Datenübermittlung Büllsbach, A./Höss-Löw, P. (2001), BfD (2003), Nr. 3.2.4 sowie EG (1995), Art. 25f.

Einen Sonderweg hat man für den Datenverkehr mit den USA geschaffen. Dabei handelt es sich um die sog. „Safe Harbor Principles“. Für US-Unternehmen, die sich freiwillig entscheiden, diese von der US-Regierung und der EU-Kommission entwickelten Standards verbindlich zu befolgen, erkennt die EU-Kommission das angemessene Datenschutzniveau im Sinne der EG-Datenschutzrichtlinie an. Das US-Handelsministerium überwacht die Einhaltung dieser Prinzipien und ahndet Verstöße. Vgl. dazu EG (2000), S.10; Glossner, S. (2004), S. 348; kritisch: Karstedt-Meierrieks, A. (2001), S. 288. Weitere Informationen zu Safe Harbor finden sich auf der Website des U.S. Department of Commerce unter: <http://www.export.gov/safeHarbor/>, 13.10.2005.

⁷⁵ Unter Offshoring wird hier das Outsourcing von IT-Dienstleistungen an einen geografisch entfernten Standort verstanden. Vgl. A.T. Kearney (2004).

von IT-Offshoring-Prozessen in deutschen Unternehmen in den kommenden Jahren voraussichtlich vervielfachen wird.⁷⁶

Einleitend wurde daher zunächst gefragt, ob es im jeweiligen Unternehmen Offshore-Aktivitäten gibt und ob ggf. ein Konzept zur datenschutzkonformen Gestaltung solcher Projekte existiert. Im weiteren Verlauf wurde ohne Beschränkung auf ein konkretes Anlass-Szenario erhoben, wo eine Datenübermittlung stattfindet. Dabei wurde aus Gründen der Vereinfachung nur unterschieden zwischen Kunden- und/oder Mitarbeiterdaten. Hinsichtlich des Bestimmungsorts wurde differenziert zwischen Übermittlungen

1. innerhalb Deutschlands,
2. innerhalb der EU (einschl. sicherer Drittländer i.S. der EG-Richtlinie),
3. außerhalb der EU (d.h. in Drittstaaten i.S. der EG-Richtlinie).

Ferner wurde erhoben, wie sich im Fall, dass tatsächlich personenbezogene Daten in Drittstaaten übermittelt werden, die Rechtsgrundlage gestaltet. Dabei wurden Mehrfachnennungen akzeptiert, da sich die entsprechenden Regelungen nicht ausschließen.

4.1 Ergebnisse

Die Auswertung innerhalb Deutschlands liefert zehn Unternehmen, die Kunden- und Mitarbeiterdaten, sowie vier weitere, die nur Mitarbeiterdaten übermitteln. Ebenfalls zehn Unternehmen übermitteln Kunden- und Mitarbeiterdaten innerhalb der EU einschließlich sicherer Drittländer i.S. der EG-Richtlinie (vgl. **Abb. 17**).

Von besonderem Interesse sind die Unternehmen, in denen es Offshore-Aktivitäten gibt. Dies trifft den Angaben zufolge zwar in elf Unternehmen zu, im Folgenden betrachtet werden aber nur neun Fälle, in denen auch tatsächlich *personenbezogene* Daten in Länder außerhalb der EU, also in Drittstaaten i.S. der EG-Richtlinie, übermittelt werden (vgl. erneut **Abb. 17**).⁷⁷ Weltweit

⁷⁶ Vgl. A.T. Kearney (2004).

⁷⁷ Sieben dieser Unternehmen übermitteln Kunden- *und* Mitarbeiterdaten. Zwei weitere entweder nur Kunden- *oder* Mitarbeiterdaten. Somit sind je Datenart zwar nur acht; insgesamt jedoch neun Unternehmen zu verzeichnen.

verfügen zwei davon über mehr als 50 Standorte⁷⁸ und sechs über mehr als 10.000 Beschäftigte.⁷⁹

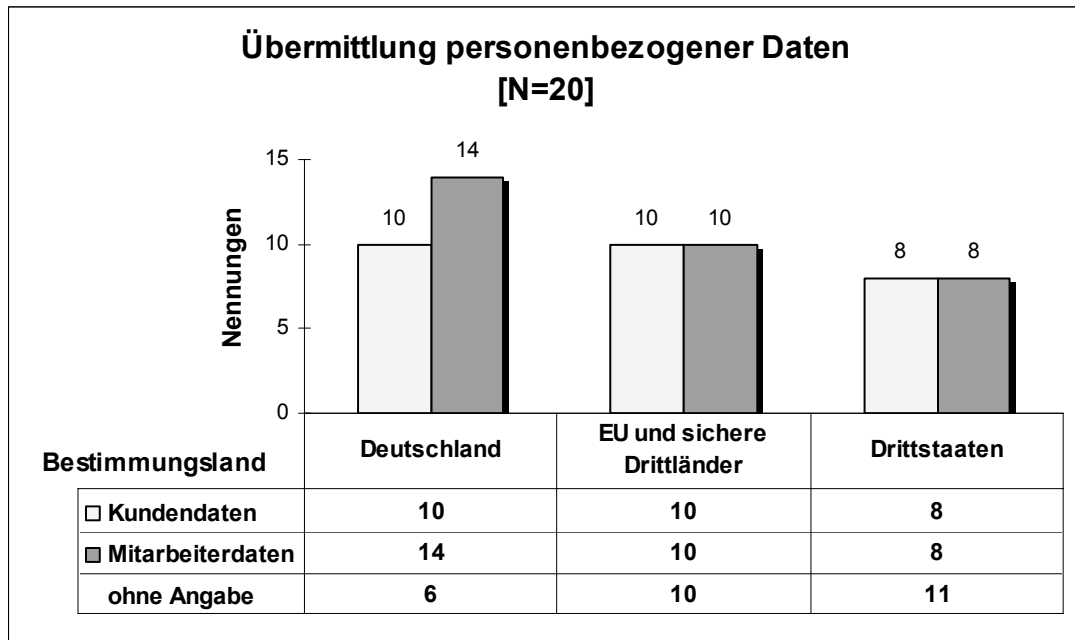


Abbildung 17: Übermittlung personenbezogener Daten

Erstaunlich ist, dass nur zwei Drittel der Datenübermittlungen in Drittstaaten durch ein Datenschutzkonzept begleitet werden. Vier dieser sechs Konzepte finden sich dabei in den großen Unternehmen mit mehr als 10.000 Beschäftigten weltweit.

4.2 Rechtsgrundlage der Datenübermittlung in Drittstaaten

Betrachtet man die Rechtsgrundlagen⁸⁰, auf denen die Übermittlung in Drittstaaten (N=9) erfolgt (vgl. **Abb. 18**), dominieren mit 77,8% (n=7) deutlich Regelungen durch einschlägige Klauseln in *bilateralen Verträgen* vor den *Safe Harbor Principles* mit 55,6% (n=5). Auffällig ist dagegen die vergleichsweise geringe Anzahl von nur vier mit den Aufsichtsbehörden abgestimmten

⁷⁸ Von den restlichen Teilnehmern liegen zwar hierzu keine Angaben vor; von vier weiteren darf dies aber aufgrund ihrer internationalen Ausdehnung zumindest vermutet werden.

⁷⁹ Eines dieser Unternehmen übermittelt den Angaben zufolge zwar Kundendaten in Drittstaaten, verfügt jedoch selbst über keinen eigenen Standort außerhalb Europas.

⁸⁰ Vgl. zu den Rechtsgrundlagen erneut Büllsach, A./Höss-Löw, P. (2001), BfD (2003), Nr. 3.2.4 sowie EG (1995), Art. 25f.

Unternehmensrichtlinien (44,4%). Letztere sind gerade für große global operierende Konzerne wesentlich einfacher zu handhaben, da sie den Vorteil bieten, ein einheitliches Datenschutzkonzept in allen Unternehmensbereichen zu etablieren, so dass Unterschiede in den nationalen Rechtsordnungen weniger zum Tragen kommen.⁸¹ Sie passen somit besser zu ihrer Struktur als die im Fall von Änderungen der situativen Bedingungskonstellationen mit komplexen und unübersichtlichen Anpassungsmechanismen verbundenen Vertragsklauseln.⁸² In dieses Bild passt daher, dass drei der vier Unternehmensrichtlinien in den großen Unternehmen mit mehr als 10.000 Beschäftigten weltweit anzutreffen sind.

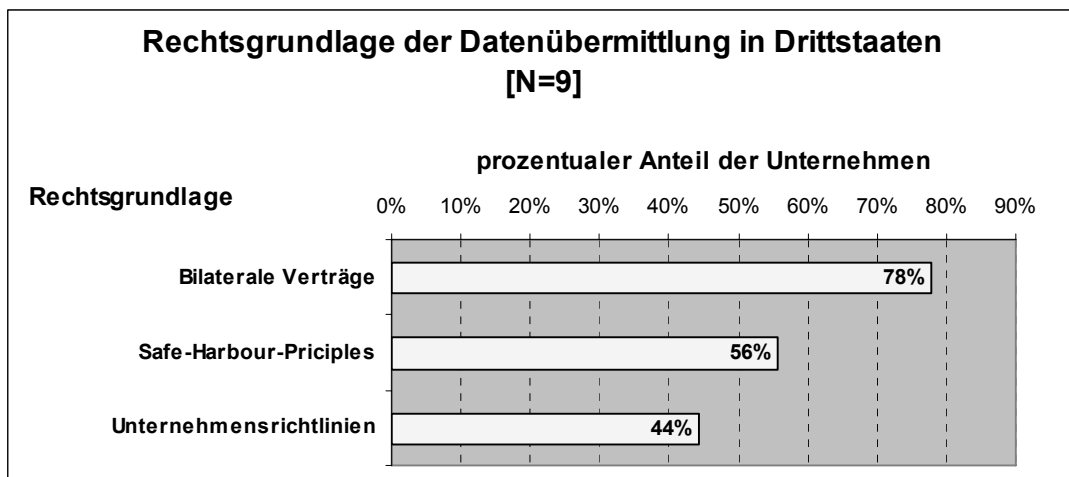


Abbildung 18: Rechtsgrundlage der Datenübermittlung in Drittstaaten

⁸¹ Vgl. Büllsbach, A. (2002), S. 54 sowie BfD (2003), Nr. 3.2.4.2.

⁸² Vgl. ebd.

5 Allgemeine Einschätzung

Zum Abschluss der Untersuchung wurden die DSB gebeten, aus ihrer Sicht zum nicht unumstrittenen⁸³ Thema *Gütesiegel als Wettbewerbselement im Datenschutz* Stellung zu nehmen sowie eine allgemeine Einschätzung zum Regelungsgrad im Geltungsbereich des BDSG abzugeben.

5.1 Gütesiegel im Datenschutz

Zu den zentralen Elementen privater Selbstregulierung durch die Unternehmen und insbesondere zum Aufbau von Vertrauen gehören Gütesiegel.⁸⁴ Das BDSG sieht dabei zur Verbesserung des Datenschutzes und der Datensicherheit das sog. Datenschutzaudit vor: Hiernach können Anbieter von Datenverarbeitungssystemen und -programmen sowie datenverarbeitende Stellen ihr Datenschutzkonzept und ihre technischen Einrichtungen durch vertrauenswürdige Instanzen prüfen und bewerten lassen und das Ergebnis dieser Prüfung veröffentlichen.⁸⁵

Das Datenschutzaudit ist freiwillig. Die Vergabe von Gütesiegeln im Datenschutz stellt dabei eine Form des Datenschutzaudits dar⁸⁶ und „dient [...] dazu, Datenschutz zum Wettbewerbsfaktor für miteinander konkurrierende Unternehmen [...] werden zu lassen“⁸⁷. Hierdurch „wird der hohen Bedeutung der Förderung des Datenschutzes durch den Einsatz von Technik und von datenschutzgerechten Gesamtkonzepten Rechnung getragen, in dem diese auch ökonomisch als Wettbewerbsvorteil über das Gütesiegel belohnt werden.“⁸⁸

Das in § 9a BDSG angekündigte Ausführungsgesetz zum Datenschutzaudit liegt jedoch bisher noch nicht vor,⁸⁹ so dass die betroffenen Institutionen keine Klarheit über dessen Auswirkungen haben.⁹⁰ Eine Darstellung des

⁸³ Vgl. z.B. Vossbein, R. (2002), S.150; BMWI (1999).

⁸⁴ Vgl. zur Selbstregulierung Schaar, P. (2003), hier insbesondere Nr. 2.2.3 „Gütesiegel“, S. 423.

⁸⁵ Vgl. BDSG § 9a. Zum Datenschutzaudit grundlegend Roßnagel, A. (2000).

⁸⁶ Vgl. Diek, A. C. (2002), S. 157.

⁸⁷ BfD (2004b), Nr. 3.6.

⁸⁸ BfD (2004a), Nr. 2.11.

⁸⁹ Vgl. BfD (2004b), Nr. 3.6.

⁹⁰ Vgl. Vossbein, R. (2002), S. 150.

Diskussionsstandes⁹¹ würde den Rahmen dieses Beitrags sprengen; erwartungsgemäß gehen daher auch die im Rahmen dieser Befragung erhobenen Meinungen auseinander. Untersucht wurde, wie gerade die Teilnehmer der ITK-Branche den Nutzen solcher Gütesiegel einschätzen und wie sie diese allgemein beurteilen.

Die Auswertung der Ergebnisse (vgl. **Abb. 19**) macht auf der einen Seite deutlich, dass ein großer Teil der Befragten (40%, n=8) Gütesiegeln im Datenschutz nur einen geringen Nutzen beimisst und diesen gegenüber eine eher ablehnende Haltung einnimmt. Die veranschlagten Kosten seien nicht nur zu hoch, es werde gar ein neues „Geldgrab“ geschaffen, wenn eine ähnliche Entwicklung wie bei bereits existierenden Zertifizierungen (wie z.B. den ISO-Normen) eintritt und eine Datenschutzkonformität nur „vorgegaukelt“ würde. So wird hier der allgemeine Nutzen von Gütesiegeln dauerhaft also eher angezweifelt: Wenn erst alle ein Gütesiegel haben, brauche man wieder etwas Neues um aus der Masse herauszuragen.

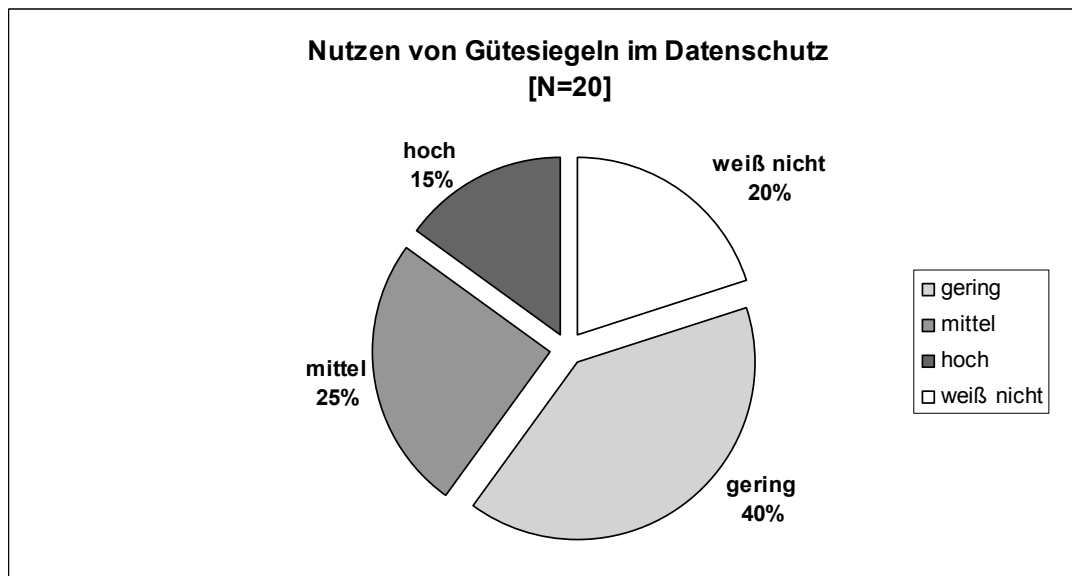


Abbildung 19: Nutzen von Gütesiegeln im Datenschutz

⁹¹ Vgl. zur Diskussion z.B. BMWI (1999). Vgl. auch Hladjk, J. (2002) und Karstedt-Meierrieks, A. (2001).

Hladjk gibt eine Übersicht über nationale und internationale Angebote sowie über die Qualität und Effektivität von Gütesiegeln.

Karstedt-Meierrieks weist in ihrem Beitrag auf Chancen und Risiken der Datenschutz-Selbstregulierung im Internet hin und unterwirft v.a. die Möglichkeit des Datenschutzaudits einer kritischen Kosten-Nutzen-Analyse aus Unternehmenssicht.

Moderatere Stimmen (25%, n=5) sind der Meinung, es hänge sehr stark von der Branche ab, ob ein Datenschutz-Gütesiegel sinnvoll ist und auch vom Markt angenommen wird. Ferner komme es auf die Ausgestaltung an. Denn ständig besser zu werden, könne allein auch kein Anspruch sein. Der gängige Vergleich mit Umweltrecht würde insofern hinken, da totaler Datenschutz letztlich bedeutet, gar keine personenbezogenen Daten zu verarbeiten.

Auf der anderen Seite sehen einige DSB (15%, n=3) in Gütesiegeln einen durchaus hohen Nutzen und erwarten, dass die Bedeutung der Gütesiegel erheblich zunehmen wird. Jedoch wird hier die Akzeptanz auf der Unternehmensseite mitunter noch als (zu) gering bezeichnet. Als größtes Hindernis einer wirksamen Verbreitung von Gütesiegeln werden dabei insbesondere uneinheitliche Standards gesehen. In diesem Zusammenhang werden auch EU-weit einheitliche Regelungen als Voraussetzung eines flächendeckenden Einsatzes gefordert. Demgegenüber ist ein Teilnehmer der Meinung, dass Risiken und Erfordernisse sehr stark von Unternehmensstruktur und Geschäftsorganisation abhängig sind, so dass eine Vereinheitlichung von Zertifizierungsmaßnahmen somit auch kontraproduktiv wirken könne.

Dieses Ergebnis zeigt, dass zu den Gütesiegeln nach wie vor eine gewisse Grundskepsis besteht. Doch gerade vor dem Hintergrund, dass der Datenschutz, wie einleitend kurz skizziert, zum zentralen Technologieakzeptanzfaktor avanciert, bieten sie mittelfristig idealtypisch die Möglichkeit, den Datenschutz als Qualitätsmerkmal zu kommunizieren. Langfristig wird es im zukünftigen Allgegenwärtigkeitsparadigma moderner ITK beim Gütesiegel dann auch nicht mehr darum gehen, aus der Masse hervorstechen, wie einer der Teilnehmer angemerkt hat, sondern damit dem Kunden zu signalisieren, dass seine elementarsten (Basis-)Anforderungen⁹² vollständig erfüllt werden und ein bestimmtes (Mindest-)Datenschutzniveau gewährleistet wird.

Wird daher von mehreren Unternehmen der Datenschutz erst als Qualitätsbestandteil entdeckt, werden auch die Datenschutzauditierung und damit die Gütesiegel als Differenzierungskriterium an Bedeutung gewinnen.⁹³ Führende Unternehmen u.a. aus der Telekommunikationsbranche haben dies bereits erkannt. Insbesondere ist dabei auch an eine mögliche Verbindung mit der britischen Norm für Sicherheitsmanagement BS 7799/ISO IEC 17799-1 zu denken. Dieser als offener Standard konzipierte Zertifizierungsprozess er-

⁹² Vgl. dazu auch die Ausführungen zum KANO-Modell im einleitenden Kapitel.

⁹³ Vgl. zum Folgenden Vossbein, R. (2002), S.153ff.

laubt auch die Berücksichtigung nationaler gesetzlicher Bestimmungen als Prüfobjekte. Der Datenschutz wäre hier als Teilsystem des gesamten IT-Sicherheitsmanagement zu definieren und entsprechend abzugrenzen. Das Datenschutzaudit wäre so als Bestandteil einer umfassenden IT-Sicherheitszertifizierung quasi „en passant“ durchzuführen. Wie die Ergebnisse des Klassifikationsteils zur Zertifizierung zeigen, besteht hier aber noch großes Potential.

5.2 Datenschutzrechtsnormen

Abschließend wurde gefragt, wie die DSB den Regelungsgrad insbesondere im Geltungsbereich des BDSG einschätzen. Ferner sollten die Befragten durch eine offene Antwort die geltenden Datenschutzrechtsnormen im Allgemeinen beurteilen, wovon ebenfalls reger Gebrauch gemacht wurde.

Mit drei Viertel aller Befragten (N=20) hält die überwiegende Mehrheit (75%, n=15) den bestehenden Regelungsgrad für angemessen. Nur ein DSB hält den Regelungsgrad für zu gering, während drei (15%) ihn als zu hoch einschätzen (vgl. **Abb. 20**).

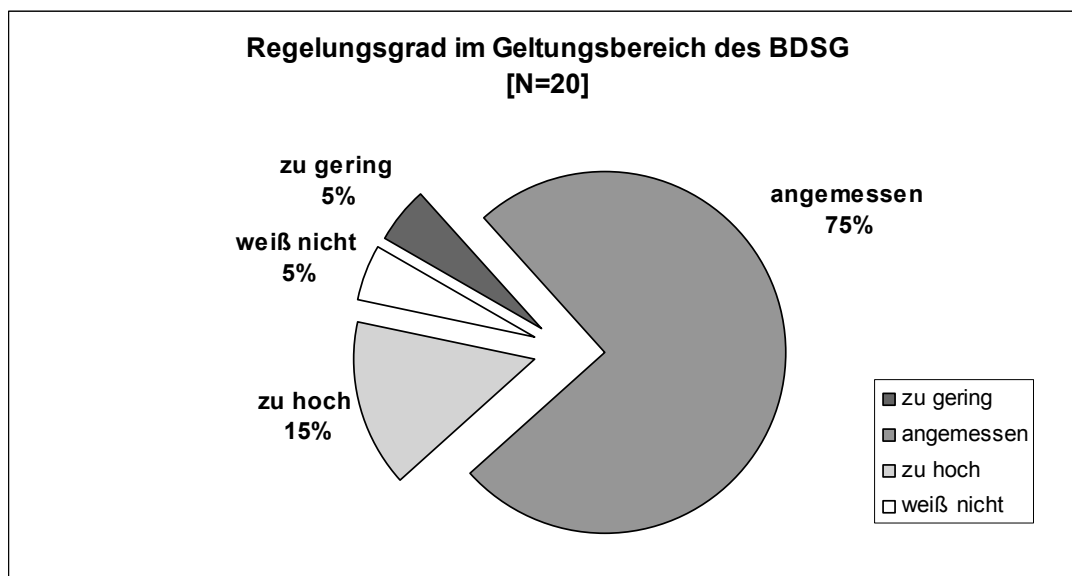


Abbildung 20: Regelungsgrad im Geltungsbereich des BDSG

Bei der allgemeinen Beurteilung der geltenden Datenschutzrechtsnormen zeigt sich hingegen ein anderes Bild. Hier zeichnen sich zwei Lager ab: Nur eine Minderheit hält dabei die Gesamtheit der geltenden Regelungen als insgesamt überwiegend angemessen, fair, sinnvoll oder notwendig. Während

hier nur vereinzelt kritische Stimmen zu verzeichnen sind, wird von der deutlichen Mehrheit der DSB v.a. die Unübersichtlichkeit aufgrund der Vielzahl an gesetzlichen Bestimmungen kritisiert. Die Regelungen seien insbesondere zu umfangreich bei gleichzeitig zu hohem Detaillierungsgrad.

Große Probleme bereitet der Umstand, dass die gesetzlichen Vorgaben den aktuellen technischen Möglichkeiten bzw. Entwicklungen nicht nachkommen. Gerade junge Rechtsgebiete wie z.B. das Teledienstegesetz seien dabei noch nicht ausgereift genug.

In Folge werden die Bestimmungen als nicht sachgerecht, in großen Teilen zu statisch und praxisfern eingestuft. Besonders kritisiert werden die hohen Anforderungen an Einwilligungen des Betroffenen (Schriftlichkeit) sowie Regelungen, die Randgebiete des Datenschutzes betreffen. Hier wird neben dem TKG auch auf den schmalen Grat im Bereich der Auftragsverarbeitung von Sozialdaten bzw. im Hinblick auf § 203 StGB verwiesen. Neben offenen Wertungswidersprüchen, Regelungsüberschneidungen und unklaren Zuständigkeiten im Allgemeinen stoßen auch politisch motivierte Zuordnungen (wie z.B. e-Mail zur Telekommunikation) auf harsche Kritik und sind in der Praxis kaum vermittelbar.

Ferner wird beklagt, in der Praxis die tatsächlich Verantwortlichen über das BDSG und seine Anwendung oft nicht zu erreichen sowie der unangemessen hohe Aufwand für einen Nichtjuristen, diese abstrakten Normen zu interpretieren. Gefordert werden daher klarere gesetzliche Vorgaben, eine Vereinheitlichung des Datenschutzrechtes – zumindest innerhalb der EU – und eine generell häufigere Anpassung bzw. Novellierung zur Berücksichtigung aktueller Entwicklungen.

6 Zusammenfassung und Ausblick

6.1 Ergebnis der Untersuchung und Handlungsempfehlungen

Das Privacy Benchmarking gibt einen ersten Überblick über Entwicklungen im Datenschutz und den Stand der Umsetzung des novellierten BDSG in einigen ausgewählten Unternehmen der ITK-Branche. Wie die Ergebnisse der Auswertungen zeigen, bestehen über die verschiedenen Beurteilungskriterien hinweg regelmäßig erhebliche Spannweiten hinsichtlich der im Einzelnen erbrachten Leistungen sowie den sicherlich nicht erschöpfend erfassten Praktiken, die z.T. als Indikatoren für einen unternehmenspolitischen Auftrag der Datenschutzorganisation identifiziert wurden.

Die Anwendung des Benchmarking-Instruments endet aber nicht mit der Darstellung der Ergebnisse. Ausgangspunkt der weiteren Überlegungen sollte daher zunächst die individuelle Standortbestimmung der eigenen Datenschutzorganisation darstellen. Dies schafft zunächst die Voraussetzung, um die Lücken zwischen den eigenen und den Leistungen der (besten) Wettbewerber zu identifizieren. In den Unternehmen, in denen Kostentransparenz bezüglich der Datenschutzorganisation gegeben ist, wird daran regelmäßig die wirtschaftliche Betrachtung des eigenen Leistungsniveaus anknüpfen. Wichtig dabei ist, die zugrunde liegenden Prozesse und Methoden zu verstehen,⁹⁴ die zu diesen Kosten führen, um diese vor dem Hintergrund des eigenen unternehmerischen Qualitätsanspruchs unter Effizienzgesichtspunkten zu analysieren; nicht um sie im Einzelnen in Frage zu stellen, sondern um Anhaltspunkte für Verbesserungspotentiale zu identifizieren.

Die gewonnenen Erkenntnisse können dann zusammen mit den Ergebnissen des Privacy Benchmarking als Argumentationsgrundlage dienen, um Zustimmung für eine Verbesserung der Rahmenbedingungen zu erhalten. Im Management bietet sich dabei die Gelegenheit, das Verständnis von Datenschutz als Wettbewerbsbestandteil und Corporate Value Factor zu schaffen bzw. zu festigen. Besonders in Unternehmen, welche die strategische Bedeutung des Datenschutz noch nicht erkannt haben, kann dies zu einer Neuausrichtung der gesamten Datenschutzorganisation und infolge ggf. auch zu einem unternehmenspolitischen Mandat führen.

⁹⁴ Vgl. Horváth, P./Herter, R. N. (1992), S. 5.

Das einleitend im Rahmen der Darstellung des Datenschutzes als Erfolgspotential skizzierte Allgegenwärtigkeitsszenario zukünftiger IKT gibt dabei Richtung und Maßstab zukünftiger Spitzenleistungen vor und stellt damit den Denkraum der Strategieentwicklung dar, um das im Rahmen der Implementierung notwendige Ausmaß der internen Verbesserungen zu quantifizieren.

Ein erfolgreiches Benchmarking sollte jedoch nicht einmalig sein, denn das volle Potential des Instruments entfaltet sich erst durch seine wiederholte Anwendung.⁹⁵ Durch die erstmalige Durchführung des Privacy Benchmarking steht hierfür nun ein Arbeitsmodell zur Verfügung, das auf Basis der damit gewonnenen Erfahrungen weiterentwickelt werden kann.⁹⁶ Das Benchmarking ist daher vor dem Hintergrund der im Rahmen der Implementierung gemachten Erfahrungen und der damit realisierbaren Veränderungen in den Fachkreisen zu diskutieren. Dabei ist zu erwägen, ob ggf. auch der Teilnehmerkreis erweitert werden sollte.

Es wird somit vorgeschlagen, das Privacy Benchmarking regelmäßig durchzuführen und z.B. durch einen Verband zu institutionalisieren. Durch eine Modifikation und Aktualisierung der Benchmarks bietet sich zum einen die Möglichkeit, einige der Untersuchungsgegenstände, die hier aufgrund der Breite der Untersuchung nicht abschließend beurteilt werden konnten, umfassender zu behandeln und durch qualitative Analysen zu ergänzen. Zum anderen können dabei aktuelle Entwicklungen und Diskussionen berücksichtigt werden. Denkbare Schwerpunkte könnten dabei z.B. innovative datenschutzfreundliche Produkte bzw. Technologien oder auch das in dieser Untersuchung nur angeschnittene Thema der Transparenz in der Datenverarbeitung sein. Ein gewisses Entwicklungspotential zeigte die Untersuchung auch hinsichtlich der Schulungsmaßnahmen, der service- und marktorientierten Aufstellung der Datenschutzorganisationen sowie der Datenschutzaudits. Auch hier können sicherlich noch Impulse gegeben werden.

Gerade für Unternehmen, die generell den Anspruch haben, nur Spitzenleistungen zu erbringen, könnte ein institutionalisiertes Privacy Benchmarking im Einzelfall auch einem befürchteten Dilemma⁹⁷ von Datenschutzaudit und Gütesiegeln Abhilfe verschaffen: Denn beim Benchmarking braucht man

⁹⁵ Vgl. Karlöf, B./Östblom, S. (1994), S. 192.

⁹⁶ Vgl. ebd.

⁹⁷ Vgl. dazu die Äußerungen der Teilnehmer in Abschnitt 5.1.

eben nicht ständig Neues, um aus der Masse hervorzustechen. Vielmehr besteht durch den regelmäßigen Vergleich ein fortwährender Anreiz zur ständigen Leistungsverbesserung.

Im Gegensatz zu Datenschutzaudits geht es beim Benchmarking nicht vordergründig darum, ein hohes Datenschutzniveau zu bescheinigen. Interessant wäre zwar zu diskutieren, ob und wie ein derartig institutionalisierter Prozess z.B. durch Entwicklung eines geeigneten Scoring-Modells über bestimmte Beurteilungskriterien hinweg zu einer Art freiwilligem Ranking von Unternehmen der ITK-Branche ausgebaut und damit zum öffentlichkeitswirksamen Wettbewerbsbestandteil werden könnte. Gerade vor dem Hintergrund der Weisungsfreiheit des DSB ist dabei jedoch mit Widerständen zu rechnen. Schließlich würde dies doch bedeuten, zumindest teilweise die Beurteilung der Effektivität, d.h. die Eignung der von einer Datenschutzorganisation getroffenen Maßnahmen für einen angestrebten Zweck, an externe Stellen zu übergeben.

Im Zentrum eines institutionalisierten Privacy Benchmarking steht daher vielmehr das gegenseitige Lernen zur kontinuierlichen Verbesserung des Datenschutzes im Interesse von Unternehmen und Bürgern. Denn die Determinanten und das Verständnis von Datenschutz und Informationssicherheit unterliegen nicht nur technischen, sondern auch sozialen Veränderungsprozessen.⁹⁸ Nur wer diese Herausforderungen rechtzeitig erkennt und fähig ist, die daraus resultierenden Anforderungen systematisch zu Bestleistungen zu adaptieren, wird sich im Ringen um das Vertrauen der verschiedenen Anspruchsgruppen⁹⁹ auf einem der vorderen Plätze halten.

6.2 Trends und Entwicklungen

Die heutige Wissens- und Informationsgesellschaft ist geprägt durch die vielfältigen Möglichkeiten effizienter Kommunikations- und Rechnerinfrastrukturen, die den einfachen Zugang zu Daten und Informationen sowie deren Weitergabe bzw. wechselseitigen Austausch erleichtern. Die weiter zunehmende Leistungsfähigkeit moderner IKT¹⁰⁰ erschließt aber auch ein breites

⁹⁸ Vgl. dazu z.B. Eggs, H./Englert, J. (2000); Eggs, H./Müller, G. (2002), S. 215. Vgl. auch Eggs, H. (2001).

⁹⁹ Vgl. Roßnagel, A. (2002), S. 124.

¹⁰⁰ Vgl. zu den Entwicklungstendenzen der IKT Picot, A./Reichwald, R./Wiegand R. T. (1998), S.136ff.

Spektrum innovativer und auf Effizienzsteigerung gerichteter neuer Anwendungen: Die Technologie der Zukunft heißt Grid-Computing¹⁰¹ und umfasst die Virtualisierung und die gemeinsame Nutzung geographisch verteilter IT-Ressourcen durch deren intelligente Vernetzung.

Im Gegensatz zu den heutigen verteilten Umgebungen, in denen die technischen Details und der Ort jeder Infrastrukturkomponente gegenüber dem Nutzer exponiert sind, treten in einer *virtualisierten* Umgebung nur noch die Eigenschaften einer Leistung bzw. einer Ressource in Erscheinung, die ihm über eine standardisierte Schnittstelle als Dienst zur Verfügung gestellt wird.¹⁰² Weiteres Schlüsselement in diesem Zusammenhang ist die *kooperative* Nutzung von Ressourcen.¹⁰³ Neben der Realisierung netzwerkübergreifender Skaleneffekte, ermöglicht die Grid-Vision dadurch insbesondere die Bildung dynamischer virtueller Organisationen zur Modellierung von Geschäftsbeziehungen.¹⁰⁴ Leistungsfähige Mechanismen zum weltweiten Auffinden und Brokern von entsprechenden Ressourcen gehen dabei weit über die heute bereits verbreiteten Informations- und Marktplatzsysteme auf Basis von Web Services hinaus.¹⁰⁵ Zukünftig wird daher nicht mehr der „Besitz“ einer IT-Ressource über die Fähigkeit entscheiden, bestimmte Probleme lösen zu können, sondern das im Bedarfsfall verfügbare Budget für den Zugriff auf eine solche Ressource am Weltmarkt.¹⁰⁶ Die Grid-Technologie schafft damit die Basis für standortverteilte und organisationsübergreifende Kernprozesse betrieblicher Wertschöpfung ohne regionale Grenzen.¹⁰⁷

Vor dem Hintergrund einer solchen globalen Vision lassen sich effektive Datenschutzmaßnahmen nicht mehr gesetzlich verordnen, denn durch das dynamische Zu- und Wegschalten von Ressourcen tritt die physikalische Ebene immer weiter in den Hintergrund. Es gibt nach dem heutigen Stand der Diskussion z.B. in einem sog. Service-Grid keine eindeutige Möglichkeit der Lokalisierung der verarbeiteten Daten mehr. Der Endnutzer weiß in einer solchen Umgebung nicht mehr, mit wem er die Infrastruktur teilt.¹⁰⁸

¹⁰¹ Vgl. zum Grid-Computing z.B. Foster, I./Kesselman, C. (1999).

¹⁰² Vgl. FZK (2003), S. 1f.; Blum, J./Geiger, A./Molzberger, U. (2004), S. 7.

¹⁰³ Vgl. FZK (2003), S. 2.

¹⁰⁴ Vgl. FZK (2003), S. 10.

¹⁰⁵ Vgl. ähnlich ebd.

¹⁰⁶ Vgl. Blum, J./Geiger, A./Molzberger, U. (2004), S. 9.

¹⁰⁷ Vgl. z.B. ähnlich auch FZK (2003), S. 1f.; a.a.O., S. 10f.

¹⁰⁸ Vgl. Blum, J./Geiger, A./Molzberger, U. (2004), S. 8f.

Datenschutz und Sicherheit werden daher sowohl Anbietern als auch Nutzern von Diensten eine noch weitaus höhere Aufmerksamkeit abverlangen als bisher, sofern wir nicht einige unserer demokratischen und menschlichen Grundrechte in Frage stellen wollen.¹⁰⁹ Denn in einem Zeitalter, in dem die Verfügungsgewalt über Ressourcen in den Hintergrund tritt und der Computer aus dem Bewusstsein verschwindet, muss der Anwender sich jederzeit voll darauf verlassen können, dass die eingesetzten Schnittstellen und Verfahren seine Vertraulichkeitsanforderungen unter allen Umständen gewährleisten.¹¹⁰

Die zentrale Herausforderung für den Datenschutz ist daher, abseits nationalstaatlicher Regelungen geeignete Strukturen zu schaffen, die den Anwender befähigen seine Interessen durch individuelle Selbstbestimmung durchzusetzen.¹¹¹ Bewusste Entscheidungen erfordern dabei aber auch ein entsprechendes Bewusstsein seitens der Betroffenen. Dieses darf durch die heute praktizierte Vorgehensweise, deren Einwilligung lediglich im Kleingedruckten einzuholen, jedoch mehr als in Frage gestellt werden.

Zukunftsauftrag des Datenschutz muss es daher sein, über die Erfüllung gesetzlicher Anforderungen hinaus den Menschen in den Mittelpunkt der Betrachtung zu rücken und als Impulsgeber die Entwicklung innovativer Lösungen im Datenschutz anzustoßen, um die Prozesse so zu gestalten, dass für die Menschen transparent wird, wie tatsächlich mit ihren Daten umgegangen wird. Denn die globale „Entwicklung einer Informationsgesellschaft braucht Vertrauen, Akzeptanz und Perspektiven für Menschen und Märkte.“¹¹²

¹⁰⁹ Vgl. Langheinrich, M./Mattern, F. (2002), S. 4f (in der Online-Version). Vgl. dazu auch Roßnagel, A. (2001).

¹¹⁰ Vgl. Blum, J./Geiger, A./Molzberger, U. (2004), S. 8; Langheinrich, M./Mattern, F. (2002), S. 5 (in der Online-Version).

¹¹¹ Vgl. auch Büllsbach, A. (1999).

¹¹² Büllsbach, A. (2003), S. 13.

Literatur

Arnaout, Ali/Hildebrandt, Jörg/Werner, Harald (1998)

Einsatz der Conjoint-Analyse im Target Costing,
in: Controlling, 10. Jg. (1998) Nr. 5, S. 306-315

A.T. Kearney (2004)

IT-Offshoring und Implikationen für den Standort Deutschland, Frankfurt am Main 2004

Bailom, Franz et al. (1996)

Das Kano-Modell der Kundenzufriedenheit,
in: Marketing-Zeitschrift für Planung, 18. Jg. (1996) Nr. 2, S. 117-126

Bäumler, Helmut/von Mutius, Albert (Hrsg., 2002)

Datenschutz als Wettbewerbsvorteil – Privacy sells: Mit modernen Datenschutzkomponenten Erfolg beim Kunden, Braunschweig/Wiesbaden 2002

BDSG

Bundesdatenschutzgesetz vom 20.12.1990, BGBl. I, S. 2954,
Neugefasst durch Bekanntmachung vom 14.01.2003, BGBl. I, S. 66,
<http://www.bfd.bund.de/information/BDSG.pdf>, 10.05.2005

Becker, Wolfgang (1999)

Begriff und Funktionen des Controlling, Bamberg 1999

Becker, Wolfgang (2001)

Strategisches Management, 5. Aufl., Bamberg 2001

Becker, Wolfgang (2002)

Kostenpolitik und Erfolgssteuerung, 2. Aufl., Bamberg 2002

BetrVG

Betriebsverfassungsgesetz vom 15.01.1972, BGBl. I, S. 13,
neugefasst durch Bekanntmachung vom 25.09.2001, BGBl. I, S. 2518,
zuletzt geändert durch Art. 5 Nr. 2 des Gesetzes vom 18.05.2004, BGBl. I, S. 974,
Online in der jeweils aktuellsten Fassung unter:
<http://bundesrecht.juris.de/bundesrecht/betrvg/>, 10.05.2005

BfD (2003)

Der Bundesbeauftragte für den Datenschutz, 19. Tätigkeitsbericht 2001 - 2002,
<http://www.bfd.bund.de/information/tb19/index.html>, 28.05.2003,

Referenzierter Abschnitt Nr. 2.3.4:

<http://www.bfd.bund.de/information/tb19/node27.html#SECTION00524000000000000000>
, 10.05.2005

BfD (2004a)

Der Bundesbeauftragte für den Datenschutz,
BfD-Info 1: Bundesdatenschutzgesetz – Text und Erläuterung,
11. Aufl., Bonn Januar 2004,
http://www.bfd.bund.de/information/pdf/info_1.pdf, 10.05.2005

BfD (2004b)

Der Bundesbeauftragte für den Datenschutz,
BfD-Info 4: Die Datenschutzbeauftragten in Behörde und Betrieb,
4. Aufl., Bonn Januar 2004,
http://www.bfd.bund.de/information/pdf/info_4.pdf, 10.05.2005

BITKOM (2005)

Kompass der IT-Sicherheitsstandards – Ein Leitfaden für mittelständische Unternehmen, Version 1.01, Berlin März 2005,
<http://www.bitkom.org/de/publikationen/1357.aspx>, 10.05.2005

Blum, J./Geiger, A./Molzberger, U. (2004)

eScience (unveröffentlichter Entwurf), ohne Ort 2004

BMWI (1999)

Bundesministerium für Wirtschaft und Technologie, Dokumentation der Fachveranstaltung „Chance für die neuen Informations- und Kommunikationsdienste - Neues Recht als Impulsgeber einer innovativen Wirtschafts- und Technologiepolitik“ zur Evaluierung des Informations- und Kommunikationsdienstegesetzes (IuKDG) vom 27. April 1999 im Wissenschaftszentrum Bonn,
Diskussionsbeiträge von Roßnagel, Alexander; Jacob, Harald; Schröder, Lothar; Neuber, Wolfgang; Hein, Werner; Greil, Peter; Elschner, Günter, Klumpp, Dieter zum Thema „Datenschutzaudit - staatliche Regulierung oder/und firmeninternes Benchmarking“,
<http://www.iukdg.de/eval/Prot270499.html>, 10.05.2005

Bräutigam, Peter (Hrsg., 2004)

IT-Outsourcing, Berlin 2004

Büllesbach, Alfred (1999)

Datenschutz in einem globalen Unternehmen, Symposium „Datenschutz – Brücke zwischen Privatheit und Weltmarkt“ bei der Internationalen Funkausstellung Berlin, 30. August 1999,
<http://www.datenschutz-berlin.de/infomat/heft27/buelles.htm>, 10.05.2005

Büllesbach, Alfred (2001)

Personal Data and Privacy Protection: The Pedagogics at Issue, Vortrag im Rahmen der 23rd International Conference of Data Protection Commissioners, Paris La Sorbonne, 24.-26.09.2001

Büllesbach, Alfred (2002)

Premium Privacy, in: Bäuml, H./Von Mutius, A. (Hrsg., 2002), S. 45-57

Büllesbach, Alfred (2003)

Premium Privacy – Datenschutz als Wettbewerbsvorteil, Vortrag am 4. Oldenburger Forum zum elektronischen Geschäftsverkehr, 13.02.2003,
<http://www.offis.de/forum/vortraege/Buellesbach%20PremiumPrivacy.ppt>, 10.05.2005

Büllesbach, Alfred/Höss-Löw, Petra (2001)

Vertragslösung, Safe Harbor oder Privacy Code of Conduct – Handlungsoptionen globaler Unternehmen; in: DuD, 25. Jg. (2001) Nr. 3, S. 135 – 138

Camp, Robert C. (1994)

Benchmarking, München/Wien 1994

Coenenberg, Adolf G. (1999)

Kostenrechnung und Kostenanalyse, 4. Aufl., Landsberg am Lech 1999

Diek, Anja Charlotte (2002)

Gütesiegel nach dem schleswig-holsteinischen Landesdatenschutzgesetz, in: Bäuml, H./Von Mutius, A. (Hrsg., 2002), S. 157-162

Diekmann, Andreas (2002)

Empirische Sozialforschung – Grundlagen, Methoden, Anwendung; 9. Aufl., Reinbek bei Hamburg 2002

DTAG (2004)

Deutsche Telekom AG, Konzern-Datenschutzhandbuch, Bonn, Stand Februar 2004

EG (1995)

Europäische Gemeinschaften, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt der Europäischen Gemeinschaften, Nr. L 281, 23.11.1995, S. 31
Abgedruckt auch in BfD (2004a), Anhang 2.

EG (2000)

Europäische Gemeinschaften, Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA;
Amtsblatt der Europäischen Gemeinschaften, Nr. L 215, 25.08.2000, S. 7-47,
<http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF>, 10.05.2005

Eggs, Holger (2001)

Vertrauen im Electronic Commerce: Herausforderungen und Lösungsansätze, Wiesbaden 2001

Eggs, Holger/Englert, Jürgen (2000)

Electronic Commerce Enquête II - Business-to-Business Electronic Commerce, Empirische Studie zum Business-to-Business Electronic Commerce im deutschsprachigen Raum, Executive Research Report, Stuttgart 2000

Eggs, Holger/Müller, Günter (2002)

Sicherheit, Vertrauen, Identität und Privatheit: Grundlagen für den „Post-Bubble Electronic Commerce“; in: Bäuml, H./Von Mutius, A. (Hrsg., 2002), S. 211-223

Ernestus, Walter et al. (1997)

Arbeitspapier „Datenschutzfreundliche Technologien“ der Arbeitsgruppe „Datenschutzfreundliche Technologien“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder, Online (ohne Seitenzahlen) auch unter: <http://www.datenschutz-berlin.de/to/datenfr.htm>, 18.11.1997

Foster, Ian/Kesselman, Carl (1999)

The Grid: Blueprint for a New Computing Infrastructure, San Francisco 1999

FZK (2003)

Forschungszentrum Karlsruhe, Strategiepapier - D-Grid: Auf dem Weg zur e-Science in Deutschland, Eggenstein-Leopoldshafen 2003,
http://iwrwww1.fzk.de/dgrid/intern2/D-Grid_Strategie_17-12-03b.pdf, 05.05.2005

Gälweiler, Aloys (1990)

Strategische Unternehmensführung, 2. Auflage, Frankfurt am Main 1990

Glossner, Silke (2004)

Datenschutz, in: Bräutigam, P. (Hrsg., 2004), S. 331-365

Gola, Peter/Jaspers, Andreas (2001)

Das neue BDSG im Überblick: Erläuterungen und Schaubilder für die Datenschutzpraxis, Frechen 2001

Hladjk, Jörg (2002)

Qualität und Effektivität von Gütesiegeln – Eine Übersicht über nationale und internationale Angebote, in: DuD, 26. Jg. (2002) Nr. 11, S. 672-678

Horváth, Péter/Herter, Ronald N. (1992)

Benchmarking – Vergleich mit den Besten der Besten,
in: Controlling, 4. Jg. (1992), Nr. 1, S. 4-11

Huber, Arthur (2004)

Strategisches IT-Outsourcing, in: ICT Kommunikation (2004) Nr. 6, S. 50f.,
http://ch.country.csc.com/de/ne/na/uploads/1566_1.pdf, 10.05.2005

Jandach, Thomas et al. (1997)

Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation“ der Arbeitsgruppe „Datenschutz in der Telekommunikation“ des Arbeitskreises “Technische und organisatorische Datenschutzfragen” der Datenschutzbeauftragten des Bundes und der Länder, Online (ohne Seitenzahlen) auch unter:
http://www.datenschutz-berlin.de/to/tk/ds_tk123.htm, 17.10.1997

Kano, Noriaki/Seraku, Nabuhiko/Tsuji, Shinichi (1984)

Attractive Quality and Must be Quality, in: Quality, 14. Jg. (1984) Nr. 2, S. 39-48

Karlöf, Bengt/Östblom, Svante (1994)

Das Benchmarking-Konzept: Wegweiser zu Spitzenleistung in Qualität und Produktivität, München 1994

Karstedt-Meierrieks, Annette (2001)

Selbstregulierung des Datenschutzes – Alibi oder Chance?,
in: DuD, 25. Jg. (2001) Nr. 5, S. 287-289

Keller, Tilo (1996)

Benchmarking – Methoden und Techniken: Mit einer kritischen Analyse des theoretischen Hintergrunds, Chemnitz 1996

Kern, Heiko (2003)

Allgemeine Beschreibung zur Sicherstellung des Datenschutz bei Mitarbeitern und Kunden, T-Systems International GmbH, Vers. 1.1, Frankfurt am Main 2003

Kern, Heiko (2004)

Global Privacy Strategy, Vortrag am International Legal Committee, T-Systems International GmbH, Frankfurt am Main 15./16.11.2004

Königshofen, Thomas (2002)

Das Datenschutzkonzept der Deutschen Telekom,
in: Bäumler, H./Von Mutius, A. (Hrsg., 2002), S. 58-67

KPMG (2001)

Information, Kommunikation, Medien 2001-2004 – Branchenprognosen aus vier europäischen Ländern, Berlin 2001, <http://www.kpmg.de/library/pdf/IKMstudieKPMG.pdf>, 10.05.2005

Küchler, Peter (2004)

Technische und wirtschaftliche Grundlagen, in: Bräutigam, P. (Hrsg., 2004), S. 51-131

Langheinrich, Marc/Mattern, Friedemann (2002)

Wenn der Computer verschwindet – Was Datenschutz und Sicherheit in einer Welt intelligenter Alltagsdinge bedeuten, in: digma – Zeitschrift für Datenrecht und Informationssicherheit, 2. Jg. (2002) Nr. 3, S. 138-142,
<http://www.vs.inf.ethz.ch/res/papers/datenschutz-langhein02.pdf>, 10.05.2005

Legner, Christine (1999)

Benchmarking informationssystemgestützter Geschäftsprozesse:
Methode und Anwendung, Wiesbaden 1999

Leibfried, Kathleen H. J./McNair, Carol Jean (1993)

Benchmarking – Von der Konkurrenz lernen, die Konkurrenz überholen;
Freiburg i. Br. 1993

Lünendonk (2004a)

Führende IT-Service-Unternehmen in Deutschland,
http://www.luenendonk.de/it_service.php, 08.06.2004

Lünendonk (2004b)

Top 25 der IT-Beratungs- und Systemintegrations-Unternehmen in Deutschland,
http://www.luenendonk.de/it_beratung.php, 19.05.2004

Mattern, Friedemann/Langheinrich, Marc (2001)

Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge,
in: Müller G./Reichenbach, M. (Hrsg. 2001), S. 7-26

Mauch, Christiane/Wildemann, Horst (2004)

Erst analysieren, dann outsourcen;
in: io new management, Zeitschrift für Unternehmenswissenschaften und Führungspraxis, 28. Jg. (2004), Nr. 9, S. 32-37,
http://www.tcw.de/tcw_V1/uploads/html/publikationen/aufsatz/files/Erst_analysieren_dann_outsourcen.pdf, 10.05.2005

Mertens, Peter/Knolmayer, Gerhard (1998)

Organisation der Informationsverarbeitung, 3. Aufl., Wiesbaden 1998

Müller, Günter/Reichenbach, Martin (Hrsg., 2001)

Sicherheitskonzepte für das Internet, Berlin 2001

Opaschowski, Horst W. (2001)

Quo vadis, Datenschutz? Die Angst der User vor dem Datenklau breitet sich aus,
in: DuD, 25. Jg. (2001) Nr. 11, S. 678 – 681

Opaschowski, Horst W. (2002)

Was will der Verbraucher?,
in: Bäumlner, H./Von Mutius, A. (Hrsg., 2002), S. 13-19

Picot, Arnold/Reichwald, Ralf/Wiegand Rolf T. (1998)

Die grenzenlose Unternehmung – Information, Organisation und Management,
3. Aufl., Wiesbaden 1998

Pieske, Reinhard (1995)

Benchmarking in der Praxis – Erfolgreiches Lernen von führenden Unternehmen, Landsberg/Lech 1995

Rau, Harald (1996)

Mit Benchmarking an die Spitze – Von den Besten lernen, Wiesbaden 1996

Reith, Heinz-Konrad (2005)

Datenschutz und Qualitätsmanagement – integriert!,
in: Computer-Fachwissen, 14. Jg. (2005) Nr. 3, S. 11-16

Roßnagel, Alexander (2000)

Datenschutzaudit – Konzeption, Durchführung, gesetzliche Regelung; Braunschweig 2000

Roßnagel, Alexander (2001)

Datenschutz in Zeiten der Terrorismusbekämpfung,
in: Fiff -Kommunikation, 18. Jg. (2001) Nr. 4, S. 10f,
<http://www.emr-sb.de/EMR/fiff2001.pdf>, 06.05.2005

Roßnagel, Alexander (2002)

Marktwirtschaftlicher Datenschutz im Datenschutzrecht der Zukunft,
in: Bäumler, H./Von Mutius, A. (Hrsg., 2002), S. 115-124

Schaar, Peter (2003)

Selbstregulierung und Selbstkontrolle – Auswege aus dem Kontrolldilemma?,
in: DuD, 27. Jg. (2003) Nr. 7, S. 421 – 426

Schnell, Rainer/Hill, Paul B./Esser, Elke (1993)

Methoden der empirischen Sozialforschung, 4. Aufl., München/Wien 1993

Smith, Scott (2003)

Wettbewerbsvorteile durch E-Business-Outsourcing, Eine Studie von Cumulus Research
Partners – in Zusammenarbeit mit PSINet Europe,
http://www.psinet.de/data/pdf/tco/TCO_Studie_DE_final.pdf, 28.10.2003

Stöber, Kathrin (2005)

Gestaltung von Outsourcing-Verträgen aus datenschutzrechtlicher Sicht,
<http://www.graeffe-rechtsanwaelte.de/docs/outsourcing-info/datenschutz.pdf>, 16.03.2005

TSI (2004)

T-Systems International GmbH, Service Center Datenschutz, Newsletter Privacy Nr. 5,
Frankfurt am Main November 2004

Ulrich, Peter (1998)

Organisationales Lernen durch Benchmarking, Wiesbaden 1998

Vossbein, Reinhard (2002)

Auditierung und Zertifizierung des Datenschutzes – erste Schritte, Möglichkeiten und
Probleme; in: Bäumler, H./Von Mutius, A. (Hrsg., 2002), S. 150-156

BBB-History

Becker, W.

Begriff und Funktionen des Controlling, Band 106, Bamberg 1995

Becker, W./Wicke, J.M

Rechtsfragen der Vermögensverwaltung, Band 107, Bamberg 1995

Becker, W./Benz, K.

Effizienz des Controlling, Band 108, Bamberg 1996

Becker, W./Benz K.

Ergebnis einer empirischen Untersuchung zur Effizienz des Controlling, Band 114, Bamberg 1996

Becker, W./Sahl, N.

Erfüllbarkeit bedeutsamer Rechenzwecke durch die Prozesskostenrechnung – dargestellt am Beispiel der Wirtschaftlichkeitskontrolle in administrativen Leistungsbereichen, Band 117, Bamberg 1997

Becker, W./Geisler, R.

Medienökonomische Grundlagen der Fernsehwirtschaft, Band 119, Bamberg 1998

Becker, W./Daniel K.

Wissensintensive Dienstleistungsbetriebe, Band 122, Bamberg 1999

Becker, W.

Begriff und Funktionen des Controlling, Band 106, Überarbeiteter Nachdruck, Bamberg 1999

Becker, W./Brinkmann F.

Gestaltungsdeterminanten von Funktionskostenrechnungen, Band 123, Bamberg 1999

Becker, W.

Wertorientierte Unternehmensführung, Band 125, Bamberg 2000

Becker, W.

Lexikon zur Kosten-, Erlös- und Ergebnisrechnung, Band 126, Bamberg 2000

Becker, W./Stephan, P.

Unternehmensnachfolge in mittelständischen Familienunternehmen, Band 127, Bamberg 2001

Becker, W./Piser, M.

Strategische Kontrolle - Ergebnisse einer empirischen Untersuchung, Band 131, Bamberg 2003

Becker, W./Piser, M.

Strategische Kontrolle - Fallstudien aus der Unternehmenspraxis, Band 132, Bamberg 2003

Becker, W./Fuchs, R.

Controlling-Informationssysteme, Band 130, Bamberg 2004

Becker, W./Moses, H.

Controlling in karitativen Nonprofit-Organisationen, Band 133, Bamberg 2004

Becker, W./Stock, C.

Strategisches Entwicklungsmanagement. Ergebnisse einer empirischen Untersuchung in der deutschen Automobilwirtschaft, Band 135, Bamberg 2004

Becker, W./Schmeken, G. M.

Integrierte Kosten- und Leistungsführerschaft als strategisches Orientierungsmuster für den E-Commerce, Band 136, Bamberg 2005

Becker, W./Stock, C.

Besonderheiten des Strategischen Entwicklungsmanagements in der Automobilindustrie am Beispiel eines europäischen Sportwagenherstellers, Band 137, Bamberg 2005

Becker, W./Brenner, F.

Sanierungsmanagement durch Kreditinstitute – Ergebnisbericht einer empirischen Untersuchung, Band 139, Bamberg 2005

Becker, W./Kunz, C.

Multiprojektmanagement in Großunternehmen – Ergebnisbericht einer empirischen Untersuchung, Band 140, Bamberg 2005

Becker, W./Fischer, S./Ostbomk, P.

Lebenszyklusorientierte Steuerung von Projekten, Band 141, Bamberg 2006

Becker, W./Fischer, S./Semmler, C.

Privacy Benchmarking 2004 – Strategie und Funktionen des Datenschutzes in der ITK-Branche, Band 142, Bamberg 2006

New Releases: www.professorwecker.de