Dirk Loomans
Manuela Matz
Michael Wiedemann

Praxisleitfaden zur Implementierung eines Datenschutz-managementsystems

Ein risikobasierter Ansatz für alle Unternehmensgrößen

Springer Vieweg

Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems

Dirk Loomans • Manuela Matz
Michael Wiedemann

Praxisleitfaden zur Implementierung eines Datenschutzmanagement-systems

Ein risikobasierter Ansatz für alle Unternehmensgrößen

Springer Vieweg

Dirk Loomans
Loomans & Matz AG
Mainz
Deutschland

Manuela Matz
Loomans & Matz AG
Mainz
Deutschland

Michael Wiedemann
SAP AG
Walldorf
Deutschland

ISBN 978-3-658-02805-3 ISBN 978-3-658-02806-0 (eBook)
DOI 10.1007/978-3-658-02806-0

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

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist eine Marke von Springer DE Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-vieweg.de

Vorwort

Mit der Veröffentlichung der „Anforderungen an ein Datenschutzmanagementsystem“ durch Dirk Loomans und Manuela Matz wurde im Jahr 2009 erstmalig ein Ansatz für ein offenes, mit bekannten Managementansätzen kompatibles Datenschutzmanagementsystem vorgestellt. Diese Bemühungen wurden vom Landesbeauftragten für den Datenschutz Rheinland-Pfalz unterstützt. Rückblickend hat sich die von Michael Wiedemann verantwortete Anwendung dieses Anforderungskataloges im globalen Support-Prozess der SAP AG im Laufe der letzten drei Jahre erfolgreich in der Praxis bewährt.

Auf Basis unserer guten Zusammenarbeit seit dem Jahr 2009 und den vielen verschiedenen Erfahrungen, die wir mit dem Datenschutzmanagementsystem in der Praxis machen konnten, haben wir Autoren uns gemeinsam zur Erstellung dieses Praxisleitfadens entschieden.

Hierin beschreiben wir den aus unserer Sicht bestmöglichen Weg zur Einführung eines Datenschutzmanagementsystems. Da bisher ein solcher strukturierter Ansatz fehlte, wird mit dem Leitfaden zugleich eine Lücke in der Managementliteratur zum Thema Datenschutz geschlossen. Großen Wert haben wir dabei darauf gelegt, sowohl die Unabhängigkeit als auch die Kompatibilität der beschriebenen Vorgehensweise zu einzelnen, fest definierten Managementstandards zu wahren und somit konsequent einen offenen Ansatz zu verfolgen, der auch die jüngsten Entwicklungen der Fachwelt auf dem Gebiet des Datenschutzmanagements zu integrieren vermag. Aus diesem Grund sehen wir den im September 2013 veröffentlichten Datenschutzstandard „Anforderungen an Auftragnehmer nach §11 BDSG“ von GDD und BVD sowie weitere Planungen zu Datenschutz-Standards von Datenschutzverbänden als eine echte Bereicherung der Praxisarbeit im Datenschutz an, die sich in die hier beschriebene Vorgehensweise ebenfalls problemlos einbinden lässt. Das genannte Beispiel und die Rückmeldungen, die wir Autoren im Laufe der Zeit zum Konzept des Datenschutzmanagementsystems bekamen, zeigen, dass darüber hinaus Bedarf für eine Handlungsanleitung besteht, die Verantwortlichen in Unternehmen praxisnah und aus einer Managementperspektive die Einführung

eines Datenschutzmanagementsystems aufzeigt. Wir freuen uns, Ihnen, liebe Leser, mit diesem Praxisleitfaden ebendies an die Hand reichen zu können und wünschen Ihnen eine erkenntnisreiche Lektüre.

Mainz/Walldorf, im Frühjahr 2014

Dirk Loomans
Manuela Matz
Michael Wiedemann

Danksagung

Ein solches Buchprojekt, das Menschen aus der Praxis für die Praxis einen Leitfaden bieten möchte, bedarf der Unterstützung einer Vielzahl von tatkräftigen Personen.

Zuallererst möchten wir uns bei Markus Kirsch bedanken, ohne dessen zuverlässige und unermüdliche Recherche- und Textarbeit dieses Werk kaum vorstellbar gewesen wäre. Wir verdanken ihm viele Einfälle zur sprachlichen Gestaltung der einzelnen Kapitel.

Außerdem möchten wir uns bei Thomas Kling für die Projektbegleitung und -koordination bedanken. Gleiches gilt für die wertvollen inhaltlichen Hinweise von Florian Gerhard und Tobias Kefelja zur praktischen Umsetzung von Datenschutzmaßnahmen in mittelständischen Unternehmen.

Die Firma SAP und ihre Mitarbeiter haben die Erstellung dieses Buches sicherlich entscheidend mitgeprägt. Hervorheben möchten wir hier Gordon Stier, der das SAP DSMS unermüdlich weiter vorantreibt, und den Datenschutzbeauftragten Hermann-Josef Schwab, dem wir für seine ausdauernde Unterstützung und seine wertvollen Anregungen danken.

Silke Herren gilt unser Dank für ihre abschließende Prüfung der Textqualität unseres Werkes.

Die Autoren möchten zudem die fruchtbare und konstruktive Zusammenarbeit hervorheben, die das Verhältnis zwischen der SAP AG und der Loomans & Matz AG im Verlauf dieses Projekts prägte.

Inhaltsverzeichnis

1 Einleitung 1
1.1 Einleitung 1
1.2 Über diesen Praxisleitfaden 3
1.3 Aufbau des Praxisleitfadens 4

2 Anforderungen an den Datenschutz 7
2.1 Bedeutung des Datenschutzes 8
2.2 Datenschutzrecht 9
2.2.1 Informationelle Selbstbestimmung 9
2.2.2 Datenschutzgrundsätze 9
2.2.3 Datenschutzgesetze 11
2.3 Auswirkungen auf die betriebliche Praxis 15
2.4 Notwendigkeit eines Datenschutzmanagementsystems 17
Literatur 19

3 Datenschutzmanagementsysteme 21
3.1 Ein Managementsystem für den Datenschutz 22
3.1.1 Das Konzept des Managementsystems 22
3.1.2 Vorteile eines DSMS 22
3.1.3 Vermeintliche Nachteile widerlegt 26
3.2 Normungen und Gütesiegel rund um den Datenschutz 28
3.2.1 Notwendigkeit eines Datenschutznachweises 28
3.2.2 Eignung für ein Datenschutzmanagementsystem 31
3.2.3 Vorgehensweise der SAP AG 34
Literatur 36

4 Voraussetzungen schaffen 39
4.1 Szenarien 40
4.2 Voraussetzungen 42
4.2.1 Anwendungsbereich festlegen 42
4.2.1.1 Einbeziehung der Verantwortlichen 44

4.2.1.2 Scoping ... 48
4.2.2 Entscheidungsvorlage für die Geschäftsleitung ... 58
Literatur ... 59

5 Implementierung ... 61
5.1 PDCA-Zyklus, KVP und DSMS ... 62
5.1.1 PDCA ... 62
5.1.2 Kontinuierlicher Verbesserungsprozess (KVP) ... 63
5.1.3 DSMS-PDCA ... 64
5.2 Implementierung anhand des DSMS-PDCA ... 67
5.2.1 Datenschutzziele festlegen und einführen ... 67
5.2.1.1 Datenschutzziele definieren ... 68
5.2.1.2 Governance Model zur Umsetzung der Ziele ... 70
5.2.1.3 Datenschutz-Policy ... 79
5.2.2 Projektstart ... 86
5.2.2.1 Inhaltliche Aspekte des Projektstartes ... 86
5.2.2.2 Beteiligte ... 88
5.2.3 Risikoanalyse ... 92
5.2.3.1 Gestufte Vorgehensweise ... 92
5.2.3.2 Risikoanalyse und -behandlung ... 95
5.2.3.3 Prozessanalyse ... 112
5.2.3.4 Einbeziehung der DSMS-Akteure in die Maßnahmenplanung ... 116
5.2.4 Dokumentation ... 119
5.2.4.1 Sinn und Zweck der DSMS-Dokumentation ... 120
5.2.4.2 Aufbau einer DSMS-Dokumentation ... 121
5.2.4.3 Aspekte der DSMS-Dokumentation ... 123
5.2.5 Roll-out ... 138
5.2.5.1 Vorbereitung ... 138
5.2.5.2 Bekanntmachung ... 140
5.2.5.3 Nachbereitung ... 141
5.2.6 Trainings ... 145
5.2.6.1 Notwendigkeit einer Datenschutz-Awareness ... 146
5.2.6.2 Grundlegende Aspekte von Datenschutztrainings ... 147
5.2.6.3 Inhalte ... 149
5.2.6.4 Methoden ... 153
5.2.6.5 Weitergehende Awareness-Maßnahmen ... 154
5.2.7 Realisierung des DSMS ... 159
5.2.7.1 Einordnung in den Kontext des DSMS-PDCA ... 160
5.2.7.2 Kommunikation ... 161
5.2.7.3 Risikoüberwachung ... 164
5.2.7.4 Veränderungen und Vorabkontrolle ... 166

5.2.7.5 Überprüfung der Dienstleister ... 168
5.2.7.6 Datenschutzvorfälle und Anfragen von außerhalb ... 172
5.2.7.7 Kontrolle der Umsetzung ... 174
5.2.7.8 Beginn mit der kontinuierlichen Verbesserung ... 177
5.2.8 Audit-Planung ... 181
5.2.8.1 Über DSMS-Audits ... 182
5.2.8.2 Audit-Cycle als systematische Abfolge der Prüfaktivitäten 188
5.2.8.3 Aspekte des Audit-Programms ... 191
5.2.9 Interne Audits ... 195
5.2.9.1 Vorbereitung ... 195
5.2.9.2 Durchführung ... 202
5.2.9.3 Nachbereitung ... 205
5.2.10 Management Review ... 211
5.2.10.1 Einordnung in den Kontext ... 211
5.2.10.2 Beteiligte ... 212
5.2.10.3 Eingaben und Ergebnisse ... 213
5.2.11 Externe Audits und Zertifizierung ... 217
5.2.11.1 Kunden-Audit (2nd-Party-Audit) ... 218
5.2.11.2 Zertifizierungs-Audit (3rd-Party-Audit) ... 219
5.2.12 Finale Anpassungen ... 223
5.2.13 Fazit zur Implementierung ... 224
5.2.13.1 Beteiligte ... 224
5.2.13.2 Agenda ... 225
5.3 Überführung in den Regelbetrieb ... 227
5.3.1 Ziele überprüfen ... 228
5.3.2 Jahresplan aufstellen ... 228
5.3.3 Risikoanalyse und Erstellung des Maßnahmenplans ... 229
5.3.4 Dokumentenrevision ... 229
5.3.5 „Re-Roll-out" ... 230
5.3.6 Umsetzung der Maßnahmen ... 230
5.3.7 Interne Audits ... 231
5.3.8 Management Review ... 231
5.3.9 Externe Audits ... 231
5.3.10 Fazit zum Status des DSMS ... 231
Literatur ... 233

6 Ausweitung des DSMS ... 235
6.1 Anpassung der Regelkreise ... 236
6.2 Besonderheiten der parallelen Aktivitäten ... 236
6.2.1 Plan-Phase ... 236
6.2.2 Do-Phase ... 238
6.2.3 Check-Phase ... 239
6.2.4 Act-Phase ... 239

7 Abschließende Bewertung 241
7.1 Das SAP-Datenschutzmanagementsystem im dritten Jahr – ein Fazit 242
7.2 Das Konzept des DSMS – eine zukunftsweisende Lösung auch für KMU . . 243

Glossar 245

Sachverzeichnis 249

Die Autoren

Prof. Dr. Dirk Loomans ist Professor für Wirtschaftsinformatik im Fachbereich Wirtschaft der Fachhochschule Mainz (Rheinland-Pfalz) und Vorstand der Loomans & Matz AG, einem Beratungshaus für Informationssicherheit, Datenschutz und Business Continuity Management. Als Managementberater unterstützen er und seine Mitarbeiter Unternehmen und Behörden bei der Einführung und dem Betrieb unternehmensweiter Informationssicherheitsprozesse. Die von ihm mitentwickelten „Anforderungen an ein Datenschutzmanagementsystem" waren Grundlage für die Implementierung eines Datenschutzmanagementsystems bei der SAP AG.

RA Manuela Matz ist Geschäftsführerin eines Tochterunternehmens der Loomans & Matz AG für IT-Services. Sie ist ebenfalls Vorstand der Loomans & Matz AG. Als Wirtschaftsjuristin und Rechtsanwältin arbeitet sie aktiv als TÜV-zertifizierte Datenschutzbeauftragte für mittelständische Unternehmen in ganz Deutschland. Sie war gleichfalls an der Entwicklung der o.g. „Anforderungen an ein Datenschutzmanagementsystem" beteiligt.

Michael Wiedemann trat im Anschluss an das Studium der Betriebswirtschaft bei der SAP AG ein und arbeitete in der globalen Support-Abteilung in den Standorten Walldorf und Philadelphia, USA. Er verantwortete über mehrere Jahre die ISO Managementsysteme des SAP-Supports und ist seit 2008 als SQ&S Chief Security Officer für die Umsetzung von Sicherheits- und Datenschutzrichtlinien im Vorstandsbereich Support verantwortlich. In diesem Zusammenhang hat er seit 2010 die Entwicklung und die Erstimplementierung eines Datenschutzmanagementsystems vorangetrieben, welches seither ständig weiterentwickelt wurde und heute in nahezu allen relevanten großen Businessbereichen der SAP eingeführt ist.

Abkürzungsverzeichnis

Abb.	Abbildung
Abschn.	Abschnitt
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
B2B	Business-to-Business
B2C	Business-to-Consumer
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
CRM	Customer-Relationship-Management
DSB	Datenschutzbeauftragter
DSMS	Datenschutzmanagementsystem
EG	Europäische Gemeinschaft
etc.	et cetera
EU	Europäische Union
EU-DSGVO	Kommissionsentwurf zu einer europäischen Datenschutzgrundverordnung vom 25.01.2012; KOM (2012) 11
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen
ff.	fortfolgend/fortfolgende
FISMA	Federal Information and Security Management Act
GDD	Gesellschaft für Datenschutz und Datensicherung e.V.
GmbH	Gesellschaft mit beschränkter Haftung
HR	Human Resources
i.S.d.	im Sinne des/im Sinne der
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization

Kap.	Kapitel
KVP	Kontinuierlicher Verbesserungsprozess
o.Ä.	oder Ähnliche/oder Ähnliches
PDCA	Plan-Do-Check-Act
QMS	Qualitätsmanagementsystem
s.o.	siehe oben
s.u.	siehe unten
Tab.	Tabelle
TMG	Telemediengesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
usw.	und so weiter
vgl.	vergleiche
z.B.	zum Beispiel

Einleitung

1

Zusammenfassung

Die zahlreichen und über die Zeit immer wieder verschärften Datenschutzgesetze verlangen von den Unternehmen und ihren Verantwortlichen die Entwicklung neuer Strategien im Umgang mit den Herausforderungen des Datenschutzes. Seit dem Jahr 2009 betreibt die SAP AG erfolgreich ein zertifiziertes Datenschutzmanagementsystem (DSMS), welches die effiziente Umsetzung der gesetzlichen Anforderungen auch in einem global agierenden Unternehmen wie SAP ermöglicht hat.

Im „Praxisleitfaden für ein Datenschutzmanagementsystem" beschreiben die Autoren einen Ansatz für die Implementierung und den Betrieb eines solchen Datenschutzmanagementsystems. Das Ergebnis ist eine unternehmensneutrale und praxisorientierte Anleitung basierend auf dem langjährigen Erfahrungsschatz der Autoren, die einen neuen, systematischen Ansatz aus der Managementperspektive verfolgt und damit eine Lücke in der Literatur zu diesem Thema schließt.

1.1 Einleitung

Im Jahr 2009 wurde das deutsche Datenschutzrecht durch drei Novellen für die Unternehmen erheblich verschärft. Dies führte zu zahlreichen Änderungen etwa im Bereich des Adresshandels und der Werbung, zur Ausweitung der Bußgeldtatbestände des Bundesdatenschutzgesetzes und – als Reaktion auf die damaligen Datenschutzskandale – zu einer Ergänzung des Beschäftigtendatenschutzes. Die neuen Anforderungen stellten die betroffenen Unternehmen vor neue Herausforderungen in der Ausgestaltung ihrer Datenschutz-Compliance. Insbesondere die neuen umfangreichen Pflichten für die Auftragsdatenverarbeitung führten in der Praxis zu vielen Problemen. Bußgeld-

D. Loomans et al., *Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems*, 1
DOI 10.1007/978-3-658-02806-0_1, © Springer Fachmedien Wiesbaden 2014

und Haftungsrisiken, Rechtsunsicherheit sowie die Gefahr von Imageschäden durch Datenschutzvorfälle mussten angemessen bewältigt werden.

Auch die SAP AG als global agierender Hersteller von Business-Software musste sich diesen Problemen stellen. Dabei entpuppte sich die Umsetzung der Anforderungen des Bundesdatenschutzgesetzes im On Premise-Bereich als die größte Herausforderung: Mehr als 100.000 Kunden aus allen Tätigkeitsfeldern hatten unterschiedlich hohe Anforderungen an den Datenschutz bei der SAP AG und wollten deren Erfüllung nachgewiesen sehen. Gleichzeitig musste SAP diese Anforderungen auch bei den zahlreichen Lieferanten durchsetzen. Dazu kamen die Herausforderungen der Regelungen über den internationalen Datenverkehr sowie die Umsetzung in den einzelnen Konzerngesellschaften, die, soweit sie nichtdeutschem Datenschutzrecht unterliegen, wenig mit den Begrifflichkeiten und der Systematik des deutschen BDSG anfangen konnten, dafür jedoch nationale Datenschutzregeln umzusetzen hatten. Insbesondere im globalen Support-Prozess war und ist der Zugriff auf personenbezogene Daten unvermeidlich und es wurde rasch deutlich, dass man diesen Anforderungen nur mit einem funktionierenden Managementsystem, das internationale Gültigkeit besitzt, erfolgreich Herr werden könne. Hier zeichnete sich Michael Wiedemann verantwortlich für die Einführung eines Datenschutzmanagementsystems im SAP-Support.

Anders als etwa in den Bereichen Qualitätsmanagement oder Informationssicherheit gibt es jedoch keinen internationalen Standard für ein Datenschutzmanagementsystem. Vor diesem Hintergrund entwickelten und definierten Prof. Dr. Dirk Loomans und RA Manuela Matz von der Loomans & Matz AG einen Anforderungskatalog. Basierend auf der international anerkannten Systematik des ISO 9001-Standards fassten sie die aus den Erfahrungen ihrer langjährigen Beratertätigkeit gesammelten Best Practices in einem Konzept zusammen. Dabei folgten sie einem risikobasierten Ansatz, der aufgrund der Orientierung an den ISO-Standards zudem international anwendbar war. Auch Edgar Wagner, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz, begrüßte den Ansatz und sprach eine Empfehlung für die Umsetzung aus.

Auf Basis dieser Anforderungen startete die SAP AG noch im gleichen Jahr mit der Implementierung im globalen Support-Prozess, welche mit der ersten Zertifizierung des Datenschutzmanagementsystems durch die British Standards Institution im Jahr 2010 erfolgreich abgeschlossen wurde. SAP befand sich nun in der komfortablen Situation, seinen Kunden jederzeit die Datenschutzkonformität der Prozesse und Verfahren im Support nachweisen zu können. Weitere Verbesserungen waren die Abstimmung der internen Strukturen auf den Datenschutz und die Optimierung des Systems zur Überprüfung der eigenen Unterauftragnehmer. Die positiven Erfahrungen mit diesem Ansatz haben dazu geführt, dass SAP seither das Datenschutzmanagementsystem in weitere Geschäftsbereiche überträgt und in den bestehenden Prozessen weiterentwickelt. Heute deckt es neben dem Support-Prozess auch die Bereiche Marketing, Human Resources, Entwicklung und Consulting ab und wurde alljährlich erfolgreich rezertifiziert. Dabei unterstützt das Datenschutzmanagementsystem den Nachweis der Datenschutz-Compliance bei der SAP AG gegenüber ihren Kunden und weist erhebliche Effizienzvorteile auf.

Das auf diese Weise entstandene Praxiswissen möchten die Autoren mit den Leserinnen und Lesern dieses Buches teilen und sie bei der Implementierung eines eigenen Datenschutzmanagementsystems begleiten.

1.2 Über diesen Praxisleitfaden

In diesem Praxisleitfaden beschreiben die Autoren den aus ihren langjährigen Erfahrungen abgeleiteten bestmöglichen Weg zur Einführung eines Datenschutzmanagementsystems. Da bisher ein solcher strukturierter Ansatz fehlt, wird mit dem Leitfaden zugleich eine Lücke in der Managementliteratur zum Thema Datenschutz geschlossen. Er zeigt Verantwortlichen anhand einer schrittweisen Anleitung den Weg hin zu einem systematischen, risikobasierten und damit kostenoptimierten Lösungsansatz für den Datenschutz in ihrer Organisation. Der Leser erhält Handlungsempfehlungen und wird somit selbst in die Lage versetzt, ein Datenschutzmanagementsystem einzuführen. Zahlreiche Praxistipps, Beispiele, Tabellen und Grafiken unterstützen dieses Ziel ebenso wie die Hinweise auf weiterführende Informationsmöglichkeiten und Literatur an jedem Kapitelende.

Als erfolgreiches Beispiel aus der Praxis tritt das Datenschutzmanagementsystem der SAP AG auf. Dort konnte bereits auf bestehendem Managementwissen und gereiften Organisationsstrukturen aufgebaut werden. Hieraus sind die zahlreichen Best Practices entstanden, die den Kern des Praxisleitfadens ausmachen. Weiterhin bildet das im Rahmen der Umsetzung und Anwendung erworbene Know-how zum Umgang mit auftretenden Problemen eine wichtige Grundlage für diesen Praxisleitfaden. Basierend auf den Beratungserfahrungen der Autoren werden zusätzlich analoge Lösungsansätze für kleinere und mittlere Unternehmen anhand den beiden eigens hierfür entwickelten Szenarien der Klein GmbH und der Medium AG präsentiert, die die jeweiligen unterschiedlichen organisatorischen Eigenarten und vorhandenen Ressourcen berücksichtigen.

An dieser Stelle ist der Leser auch darauf hinzuweisen, dass nicht pauschal jede Einführung eines Datenschutzmanagementsystems auf Anhieb in allen Punkten erfolgreich sein wird. Einfluss darauf hat eine Vielzahl von Gründen: Unternehmen wie die SAP AG, die bereits andere Managementsysteme eingeführt und entsprechende Prozesse geschaffen haben, profitieren von den dort gemachten Erfahrungen auch in Bezug auf das hier vorgestellte Datenschutzmanagementsystem, das auf viele Grundprinzipien bekannter Managementsystemansätze zurückgreift. Umgekehrt kann ohne solche Kenntnisse der ganzheitliche Ansatz des Managementsystems die Verantwortlichen überfordern. Gerade der hier vorgestellte prozessorientierte Ansatz kann im Widerspruch zu traditionellen Organisationsstrukturen stehen. Auch mag in einigen Fällen zwar die formale Umsetzung des Datenschutzmanagementsystems gelingen, der Datenschutz kommt jedoch nicht in der „lebendigen" Praxis an. Damit wäre das Ziel des Datenschutzmanagementsystems verfehlt. Um dies zu vermeiden, erhält der Leser an den passenden Stellen im Buch wichtige Hinweise, wie diese Hindernisse überwunden werden können. Denn viele Schwierigkeiten

kommen aus Sicht der Autoren in der Praxis wiederholt vor und sind dem Leser möglicherweise ebenfalls vertraut. Der vorliegende Praxisleitfaden ist damit nicht als Garant für ein einhundertprozentig funktionierendes Datenschutzmanagementsystem zu verstehen, vielmehr stellt er solide Grundregeln für ein solches auf. Die tatsächliche Umsetzung muss sich immer an den Gegebenheiten des jeweiligen Unternehmens orientieren. So ist es insbesondere geeignet, einzelne als besonders kritisch erachtete Prozesse im Unternehmen zu regulieren. Eine vollständige Umsetzung in der gesamten Organisation ist nämlich in vielen Fällen aufgrund der vorgegebenen Ressourcen nicht möglich. Umso mehr dagegen baut der Erfolg des DSMS auf dem Willen zur tatsächlichen Umsetzung und dem Engagement seiner Beteiligten auf. Der Leser soll aktiv an der Einführung mitwirken. Dies fördert den Erfolg des DSMS auch in seinem Unternehmen.

1.3 Aufbau des Praxisleitfadens

- Kapitel 2 gibt einen kurzen und prägnanten Überblick über die komplexen *Anforderungen des Datenschutzes*, denen sich jedes Unternehmen stellen muss. Ausgehend von einer Beschreibung des aktuellen Zustands und möglicher Entwicklungen des Datenschutzes werden sowohl die rechtlichen Zielsetzungen, insbesondere die des Bundesdatenschutzgesetzes (BDSG), als auch die daraus folgenden Wechselwirkungen mit der betrieblichen Organisation in kompakter Art und Weise dargestellt. Der Leser erfährt hier auf einen Blick, wie der Datenschutz in die betrieblichen Abläufe eingreift.
- Kapitel 3 stellt das Konzept des *Datenschutzmanagementsystems* (DSMS) dar. Es beschreibt Vorteile und widerlegt gängige Vorurteile. Zudem werden branchenspezifische Standards und Gütesiegel auf ihre Eignung für ein solches DSMS verglichen. Der Leser erhält so einen Überblick über bisherige Entwicklungen im Bereich der Standardisierung von Managementsystemen im Datenschutz sowie Anknüpfungsmöglichkeiten für die eigene Vorgehensweise bei der Implementierung.
- Kapitel 4 beschreibt die *Voraussetzungen für die Einführung* eines DSMS und gibt wichtige Anregungen für Vorüberlegungen, die sich die Verantwortlichen vor der Implementierung machen müssen. Es wird beschrieben, wie das DSMS auf Basis eines Scoping-Prozesses in den bestehenden betrieblichen Rahmen integriert werden kann und wie die relevanten Personen identifiziert und einbezogen werden. Dabei werden, wie in den Folgekapiteln auch, jeweils unterschiedliche Herangehensweisen für kleine, mittlere und große Unternehmen dargestellt.
- In Kap. 5 wird umfassend der Prozess der *Implementierung* des DSMS dargestellt. Dieser Prozess orientiert sich am Modell des PDCA-Regelkreises und seinen vier Phasen: Plan, Do, Check und Act. Anhand einer Prozessabfolge von zwölf Schritten werden die einzelnen Komponenten vorgestellt, erläutert und in ihrer praktischen Anwendung gezeigt. Am Ende entsteht ein funktionierendes DSMS, das anschließend in den Regelbetrieb überführt und kontinuierlich verbessert werden kann.

- Kapitel 6 erklärt, wie auf Basis eines funktionierenden DSMS in einem bestimmten Geschäftsbereich die *Ausweitung* auf andere Geschäftsbereiche erfolgen kann und so schließlich alle datenschutzrelevanten Prozesse und Verfahren abgedeckt werden können.
- In Kap. 7 und damit als abschließendes *Fazit* ziehen die Autoren aus ihrer Position als Verantwortliche bzw. Berater ein Resümee zu den von ihnen gemachten Erfahrungen.
- Im beigefügten *Glossar* als Nachschlagehilfe werden schließlich die wichtigsten im Buch verwendeten DSMS-Begriffe in prägnanter Art und Weise erläutert.

Anforderungen an den Datenschutz

2

Zusammenfassung

Dem Datenschutz kommt im Zuge der Entwicklungen hin zur Informationsgesellschaft eine tragende Rolle zu. Als Ausfluss des Grundrechtes auf informationelle Selbstbestimmung schützt er die Betroffenen vor der unsachgemäßen Verwendung ihrer personenbezogenen Daten und nimmt die Unternehmen in die Pflicht. Zahlreiche gesetzliche Änderungen und die immer höheren Erwartungen der Kunden stellen die Unternehmen dabei vor große Herausforderungen, die sich nicht nur als lediglich zusätzliche Kosten darstellen. So stellt zum einen die Nichtbeachtung des Datenschutzes heute einen immensen Risikofaktor dar, was neben Bußgeldern und Reputationsschäden bis zur Haftung der Leitungsebene führen kann. Zum anderen kann sich ein Unternehmen heute über den Nachweis der eigenen Datenschutzkonformität hervorragend im Wettbewerb positionieren.

In dieser Situation stößt die unkoordinierte Vorgehensweise im Rahmen von Ad-hoc-Maßnahmen an ihre Grenzen und offenbart das Potential für neue, ganzheitliche Lösungen wie die des Datenschutzmanagementsystems.

▶
- Welche Bedeutung kommt dem Datenschutz heute und in Zukunft zu?
- Welche Ziele verfolgt der Datenschutz?
- Auf welchen Grundsätzen basiert der Datenschutz?
- Welche rechtlichen Regelungen sind in welchen Fällen zu beachten?
- Wie wirken sich diese Regelungen auf die betriebliche Praxis aus?
- Welche zusätzlichen Datenschutzanforderungen werden an ein Unternehmen gestellt?
- Warum ist Datenschutz mehr als ein reiner Kostenfaktor?
- Wie löst man den Konflikt zwischen den rechtlichen und betrieblichen Anforderungen?

D. Loomans et al., *Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems*,
DOI 10.1007/978-3-658-02806-0_2,

2.1 Bedeutung des Datenschutzes

Im Zuge der gesellschaftlichen und wirtschaftlichen Veränderungen im 21. Jahrhundert kommt dem Datenschutz zunehmend eine Schlüsselrolle zu. Globalisierung, Internationalisierung und die Entwicklung hin zur Informationsgesellschaft üben großen Einfluss auf die Unternehmen aus. Wachstumstechnologien, wie aktuell Cloud Computing, Funk-Vernetzung und Mobile Devices führen zu exponentiell anwachsenden Datenvolumina. Durch den vorangetriebenen technischen Fortschritt ist der Personenbezug von Daten zudem immer leichter herstellbar: Auf Basis moderner Analysetools und Big-Data-Anwendungen ist der gläserne Konsument heute bereits Alltag geworden. Als Zielsetzung des Datenschutzes rückt der Schutz des Einzelnen vor dem unsachgemäßen Umgang mit seinen persönlichen Daten an dieser Stelle in den Mittelpunkt. Das Recht des Betroffenen auf informationelle Selbstbestimmung bildet ein Grundrecht, das die Bürgergesellschaft immer stärker einfordert.

Die Unternehmen geraten damit in ihrer Rolle als Datenverarbeiter zunehmend in den Fokus der Öffentlichkeit. Zahlreiche Datenschutzskandale in den letzten Jahren und die regelmäßig damit einhergehenden Sanktionen der Aufsichtsbehörden bringen das Thema auf die Agenda der Geschäftsleitung. So zeichnet eine im Jahr 2012 von der Beratungsgesellschaft PricewaterhouseCoopers (PwC) [14] durchgeführte Umfrage bei den Datenschutzbeauftragten aus 250 großen und mittelgroßen deutschen Unternehmen ein deutliches Bild: Die Zahl der befragten Unternehmen, die den Datenschutz als sehr wichtig einstufen, verdoppelte sich allein im Vergleich zum Vorjahr auf mehr als 27 %.

Auch die Betroffenen sehen den Datenschutz als ein starkes Kriterium für eine vertrauensvolle Geschäftsbeziehung an. Einer im Jahr 2013 durchgeführten und veröffentlichten Umfrage der BITKOM [4] nach sehen 75 % der befragten Verbraucher einen nachvollziehbaren Datenschutz als wichtig für das Kundenvertrauen an. Dabei kommt dem Schutz der personenbezogenen Daten nicht nur in Deutschland eine Schlüsselrolle zu. Bereits in Schwellenländern wie Brasilien, kulturell unterschiedlichen Gesellschaften, wie der koreanischen und selbst im kommunistisch ausgerichteten China wächst das Bedürfnis nach Datenschutz enorm. Diesen Trend konnte eine Vergleichsstudie des Münchner Kreises aus dem Jahr 2013 [11] nachdrücklich aufzeigen.

Folglich reagieren Kunden weltweit zunehmend kritischer und erkennen Gesetzeskonformität in diesem Bereich als wichtigen Qualitätsfaktor an, den sie zuverlässig nachgewiesen haben möchten. Ebenfalls treten die Aufsichtsbehörden als Prüfinstanzen auf und verhängen bei Nichtkonformität Sanktionen. Nicht zuletzt hat in Deutschland der Gesetzgeber gehandelt und dabei im Jahr 2009 umfangreiche gesetzliche Verschärfungen für die Privatwirtschaft eingeführt. Zudem steht aktuell eine große Neuordnung des Datenschutzes auf europäischer Ebene in den Startlöchern [8]. Eines kann man somit sicher sagen: Der Datenschutz wird die Unternehmen auch in den kommenden Jahren intensiv beschäftigen und vor große Herausforderungen stellen.

2.2 Datenschutzrecht

2.2.1 Informationelle Selbstbestimmung

Mit dem Volkszählungsurteil aus dem Jahr 1983 [6] wurde vom Bundesverfassungsgericht zum ersten Mal explizit das Grundrecht des Einzelnen auf informationelle Selbstbestimmung formuliert. Ursprünglich als Abwehrrecht gegen zu viel Datenhunger des Staates entwickelt, gewährt es auch als Teil des allgemeinen Persönlichkeitsrechtes dem Betroffenen das Recht, über Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst entscheiden zu können. Bund und Länder sind in ihren Handlungen zur Berücksichtigung der Grundrechte verpflichtet, ebenso wie sie diese gewährten Rechtsgüter vor Beeinträchtigungen Dritter zu schützen haben. Das bedeutet, dass der Staat im Rahmen seiner Schutzpflicht gegenüber den Betroffenen Behörden wie Unternehmen in diesem Bereich einer Regulierung unterziehen muss. Darauf basierend haben der nationale und der europäische Gesetzgeber seither den Datenschutz durch zahlreiche legislative Maßnahmen ausgestaltet. Zudem werden die oben in Abschn. 2.1 geschilderten Entwicklungen in Zukunft weitere Aktivitäten nach sich ziehen. Die Unternehmen stehen in der Verantwortung, diese rechtlichen Anforderungen konsequent zu befolgen.

2.2.2 Datenschutzgrundsätze

Als konsequente Fortführung des Gedankens der informationellen Selbstbestimmung orientiert sich der Gesetzgeber an übergeordneten Datenschutzgrundsätzen. Viele dieser Zielsetzungen fördern gleichzeitig die Umsetzung des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme („IT-Grundrecht“, „Computer-Grundrecht“). Abbildung 2.1 zeigt die verschiedenen Datenschutzgrundsätze, die sich aus dem Recht auf informationelle Selbstbestimmung ableiten.

Nur wenn alle diese Ziele in angemessener Art und Weise verwirklicht werden, kann ein effektiver Schutz des Betroffenen gewährleistet werden. Dies betrifft daher auch die Unternehmen, deren Datenschutzmaßnahmen sich ebenfalls daran orientieren müssen. Hinter den einzelnen Grundsätzen verbirgt sich dabei Folgendes:

- **Verhältnismäßig** ist eine Maßnahme dann, wenn sie zur Förderung eines legitimen Zweckes sowohl erforderlich, geeignet als auch angemessen ist. Als Adressaten des Datenschutzrechts müssen sich auch die Maßnahmen der Unternehmen zur Umsetzung des Datenschutzes an diesem Prinzip orientieren.
- Die Prinzipien der **Datensparsamkeit und -vermeidung** stellen die Anforderung auf, dass Verfahren nach Möglichkeit mit so wenig personenbezogenen Daten wie möglich operieren sollen. Dies kann u. U. dazu führen, dass ganz auf personenbezogene Daten verzichtet werden muss, wenn diese für das entsprechende Verfahren nicht unbedingt erforderlich sind. Auf technischer Ebene kann dies auch über Pseudonymisierung oder Anonymisierung personenbezogener Daten umgesetzt werden.

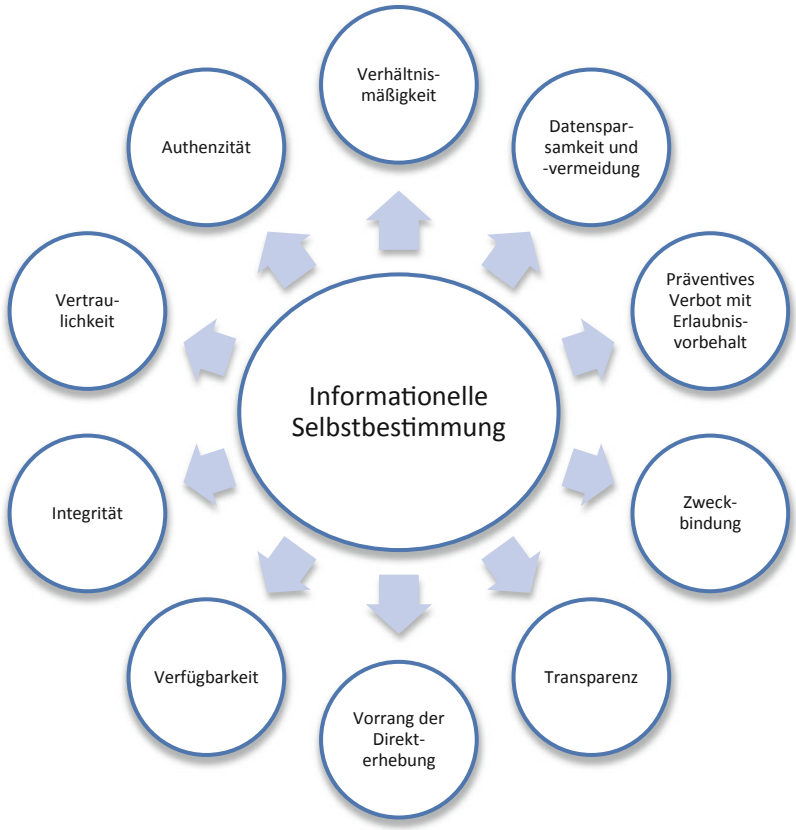

Abb. 2.1 Datenschutzgrundsätze

- Als ordnungspolitischer Hintergrund des deutschen Datenschutzrechtes ist der Umgang mit personenbezogenen Daten durch Dritte grundsätzlich verboten, es sei denn, eine Rechtsnorm erlaubt dies ausdrücklich (**Präventives Verbot mit Erlaubnisvorbehalt**). Eine solche Erlaubnis als Form der informationellen Selbstbestimmung ist auch durch eine qualifizierte Einwilligung des Betroffenen möglich.
- Personenbezogene Daten sind bei ihrer Verarbeitung an den **Zweck gebunden**, zu dem sie erhoben wurden. Eine nachträgliche Zweckänderung ist nur in engen Grenzen möglich.
- Die Verarbeitung von personenbezogenen Daten muss dem Betroffenen gegenüber **transparent** gemacht werden. Denn nur auf diese Weise kann dieser Art und Ausmaß des Eingriffs in sein Recht auf informationelle Selbstbestimmung beurteilen und entsprechend reagieren.
- Daran anschließend müssen personenbezogene Daten grundsätzlich **beim Betroffenen direkt erhoben** werden. Dritterhebungen sind nur in engen Grenzen zulässig.

- Bezogen auf das personenbezogene Datum und damit insbesondere vom technischen Datenschutz zu gewährleisten sind die Prinzipien der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität**:**
  - **Verfügbar** ist ein Datum, wenn es zeitnah zur Verfügung steht und ordnungsgemäß verarbeitet werden kann
  - **Integer** ist ein Datum, wenn es vollständig, unversehrt und aktuell ist
  - **Vertraulich** ist ein Datum, wenn es nur dem befugten Personenkreis zugänglich ist
  - **Authentisch** ist ein Datum, wenn dessen Herkunft zum rechtmäßigen Urheber zurückverfolgt werden kann

2.2.3 Datenschutzgesetze

Die erwähnten Grundsätze bilden den Hintergrund für die erlassenen Datenschutzgesetze. An dieser Stelle wird dem Leser ein kompakter Überblick über die wichtigsten Regelungen präsentiert:

- Die **europäische Datenschutzrichtlinie (95/46/EG)** stellt einen Mindeststandard für den Datenschutz in allen Mitgliedsstaaten der europäischen Union sicher. Unternehmen mit Sitz in der EU müssen daher in jedem Fall diesen Anforderungen entsprechen, wobei die einzelstaatlichen Umsetzungen zum Teil erheblich divergieren. Zwei Aspekte führen aktuell zu der Diskussion um eine neue europäische Regelung des Datenschutzes in Form einer Grundverordnung (EU-DSGVO) [8]: Zum einen gilt die Richtlinie in vielen Punkten als nicht mehr aktuell und praktikabel umsetzbar und berücksichtigt bestimmte technische Entwicklungen nicht ausreichend. Zum anderen hofft man, den durch die unterschiedlichen Umsetzungen entstandenen „Flickenteppich“ europaweit harmonisieren zu können. Denn die EU-DSGVO wäre als Verordnung unmittelbar geltendes Recht in allen EU-Staaten, während eine Richtlinie immer der Umsetzung durch nationales Recht bedarf.
- Die Umsetzung der EG-Richtlinie in der Bundesrepublik Deutschland erfolgte im Wesentlichen durch entsprechende Anpassungen des zentralen **Bundesdatenschutzgesetzes (BDSG)**. Dieses stellt zugleich in einigen Fällen wesentlich strengere Anforderungen auf als von der europäischen Richtlinie gefordert. Weltweit fordert das deutsche Datenschutzrecht daher mit das höchste Schutzrecht für personenbezogene Daten ein. Dabei unterscheidet das BDSG zwischen öffentlichen Stellen (öffentliche Verwaltung) und nicht öffentlichen Stellen (Unternehmen). Adressat ist dabei jeweils die verantwortliche Stelle[1] i. S. d. § 3 VII BDSG. Die in diesem Leitfaden verwendeten Fachbegriffe aus

[1] Im Folgenden soll statt des Ausdrucks „verantwortliche Stelle“ konsequent der Begriff des Unternehmens verwendet werden, da dieser Praxisleitfaden sich weniger mit der rechtlichen als mit der unternehmensinternen Verantwortlichkeit auseinandersetzt. Sollte an einer Stelle in diesem Buch die datenschutzrechtliche Verantwortlichkeit i. S. d. verantwortlichen Stelle nicht auf das beschriebene Unternehmen fallen, wird dies über die entsprechende Verwendung des Fachbegriffs „verantwortliche Stelle“ klargestellt.

dem BDSG, etwa das personenbezogene Datum oder die Auftragsdatenverarbeitung, werden für den interessierten Leser im Glossar am Ende dieses Buches erläutert.
- Die einzelnen **Landesdatenschutzgesetze** stellen lediglich Spezialregelungen für die in den jeweiligen Ländern ansässigen Behörden auf und betreffen die Unternehmen daher nicht direkt.

Zahlreiche **Spezialgesetze** enthalten bereichsspezifische Regelungen zum Datenschutz und gehen den allgemeineren Regelungen wie dem BDSG regelmäßig vor. Übersichten dieser großen Masse an Gesetzen finden sich beispielsweise bei den Aufsichtsbehörden[2]. Auszugsweise sind hierbei von besonderer praktischer Relevanz:

- Das **Telemediengesetz (TMG)** stellt Anforderungen u.a. an den Datenschutz von internetbasierten Diensten wie Websites, Apps etc., die vom Unternehmen als Telemediendienstleister angeboten werden.
- Ist die verantwortliche Stelle Telekommunikationsanbieter, so müssen die einschlägigen Datenschutzregelungen des **Telekommunikationsgesetzes (TKG)** beachtet werden.
- Spezielle **Geheimhaltungspflichten** für Ärzte, Rechtsanwälte etc. erheben hohe Anforderungen an die Vertraulichkeit der personenbezogenen Daten und müssen auch im entsprechenden Angestelltenverhältnis beachtet werden.
- Im Bereich des Handels-, Steuer- und Sozialrechtes sind **Übermittlungspflichten** sowie **Aufbewahrungspflichten** zu beachten.
- Ebenso gibt es im stark zersplitterten **Arbeitsrecht** weitere gesetzliche Regelungen, die im Rahmen des Datenschutzes Beachtung finden müssen. So bedürfen beispielsweise Videoüberwachungen regelmäßig der Zustimmung des Betriebsrates.
- Auch enthalten die einzelnen Gesetze zahlreiche **Straf- und Haftungstatbestände**, die sich bei einer Verletzung des Datenschutzes verwirklichen können.

Abhängig vom Umfang der Geschäftstätigkeit, sind zudem **internationale Normen** zu berücksichtigen. So sind auch in außereuropäischen Ländern wie beispielsweise in Korea [3, 1] Datenschutzgesetze in Kraft, die in einzelnen Teilbereichen durchaus europäisches Niveau erreichen können. Auch in den USA, wo der Privatsphärenschutz eher liberal gehandhabt wird, haben sich einzelne Bundesstaaten wie etwa Massachusetts zur Verabschiedung von Gesetzen entschieden [7]. Zu beachten ist, dass die internationalen Normen im Konflikt untereinander wie auch mit nationalen Normen stehen können. Als bekanntes Beispiel dient hier der Sarbanes-Oxley-Act (SOX) aus den USA zur Einführung eines internen Kontrollsystems in Unternehmen, der basierend auf der angelsächsi-

[2] Wie hier vom Landesbeauftragten für den Datenschutz in Rheinland-Pfalz: http://www.datenschutz.rlp.de/de/rechtsgrundlagen.php.

schen Praxis dem Privatsphärenschutz im Gegensatz zum kontinentaleuropäischen Ansatz grundsätzlich weniger Gewicht zukommen lässt.[3] [2]

Bezogen auf dieses Beispiel müssen nach überwiegender Auffassung etwaige aus Deutschland ausgehende Datenübermittlungen auf Grundlage von SOX hinter den strengen Anforderungen des BDSG zurückstehen und damit im Zweifel unterbleiben.

Weiterhin ist zu beachten, dass die Anforderungen an die Unternehmen durch entsprechende **Kundenforderungen** nochmals steigen können. Relevant wird dies, wenn in B2B-Geschäften der Auftraggeber als Adressat von Spezialgesetzen selbige Anforderungen an seine Auftragnehmer weitergibt. Dies ist beispielsweise der Fall, wenn die an einer Auftragsdatenverarbeitung teilnehmenden Unternehmen in verschiedenen Ländern oder Branchen tätig sind. So sind Unternehmen aus der Finanzbranche regelmäßigen (Datenschutz-)Kontrollen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ausgesetzt (§ 44 KWG i. V. m. § 25a KWG) und müssen entsprechend sicherstellen, dass alle ihre Auftragnehmer kapitalmarktspezifische Datenschutzregelungen umsetzen.

Weiterhin ist zu beachten, dass nicht nur formelle Gesetze Anforderungen aufstellen können. So sind gerade in Staaten, in denen die Gesetzgeber bisher nur zurückhaltend aufgetreten sind, **alternative Normenwerke** in Anwendung bzw. in Entwicklung. Beispielsweise hat das National Institute of Standards and Technology (NIST) des U.S. Department of Commerce im Jahr 2013 Mindestanforderungen an den Privatsphärenschutz für Informationssysteme von US-Behörden veröffentlicht [12]. Konkret diente dies dazu, die Umsetzung des Federal Information Security and Management Act (FISMA) zu befördern. Als Nebenzweck fordert auch die bekannte ISO 27001 für Informationssicherheitsmanagementsysteme die Sicherstellung des Datenschutzes. Hintergrund der beschriebenen Entwicklungen ist die im Zuge der Globalisierung erforderliche Mindestumsetzung von Privatsphärenstandards, auch ohne dass explizite Gesetze in diesem Bereich vorliegen. Denn alleine aus der Tatsache, dass der Gesetzgeber nicht aktiv geworden ist, lässt sich nicht schließen, dass Kunden und Betroffene keine Ansprüche an den Datenschutz stellen. Vielmehr stellt gerade in einem solchen Fall die Sicherstellung des Datenschutzes ein positives Alleinstellungsmerkmal für Unternehmen dar.

Nicht zuletzt kann das Unternehmen auch selbst zusätzlich Anforderungen an den unternehmensinternen Datenschutz schaffen, indem es entsprechende **interne Richtlinien** festlegt. Relevant wird dies beispielsweise im Konzern über die sog. „Binding Corporate Rules", welche eine Möglichkeit zur Sicherstellung eines angemessenen Datenschutzniveaus bei einer Geschäftstätigkeit in mehreren Ländern darstellen. Dabei stehen dann die Gesellschaften in Drittländern vor der Herausforderung der Umsetzung dieser Anforderungen. Ebenfalls in diese Kategorie gehören die Datenschutz-Policy (Abschn. 5.2.1.3) oder die Compliance-Richtlinien.

Auch können sich Unternehmen, die Datenschutzgütesiegel (Abschn. 3.2) für ihre Produkte anstreben, selbst die jeweiligen Anforderungen für das Gütesiegel auferlegen. Zudem

[3] Zu Lösungsansätzen in diesem Bereich vgl. die Stellungnahme 01/2006 der Art. 29-Datenschutzgruppe der Europäischen Kommission.

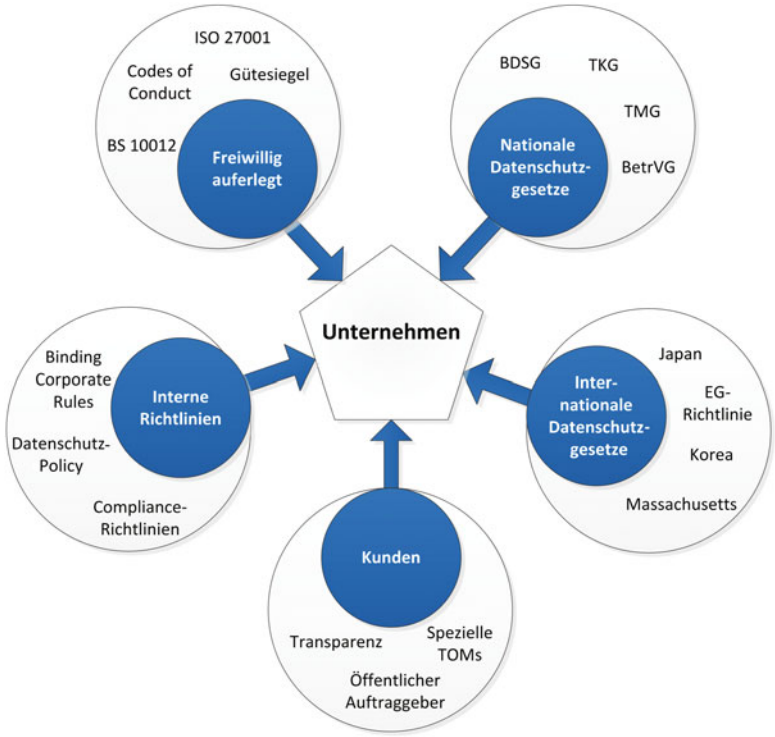

Abb. 2.2 Datenschutzanforderungen an die Unternehmen

können Unternehmen sich **freiwillig selbst verpflichten** und sog. „Codes of Conduct" unterzeichnen. Solche sind bspw. vom Gesamtverband der deutschen Versicherungswirtschaft in Zusammenarbeit mit dem Berliner Landesbeauftragten für den Datenschutz und einem Verbraucherschutzverband erstellt worden. [10]

Die zahlreichen hier beschriebenen Anforderungen aus dem Bereich Datenschutz, die an ein Unternehmen gestellt werden, zeigt Abb. 2.2.

Bereits aus der Masse der vielen möglichen einschlägigen Gesetze und Anforderungskataloge ergibt sich für die Unternehmen das Problem, die genauen Anforderungen zu ermitteln. Hinzu kommt, dass sich die Gesetze regelmäßig ändern, wobei besonders Verschärfungen zu Problemen führen. Daraus folgt, dass die genaue Kenntnis über die einschlägigen Anforderungen an das Unternehmen bei der betrieblichen Umsetzung eine zentrale Voraussetzung darstellt.

▶ Das hier vorgestellte DSMS wurde – als risikobasierter Ansatz – bewusst unabhängig von sich wandelnden Gesetzen konstruiert, um die genannten Probleme zu vermeiden. Stattdessen wurden Methoden integriert, die eine Identifikation der relevanten Anforderungen und deren adäquate Behandlung ermöglichen.