

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?

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.

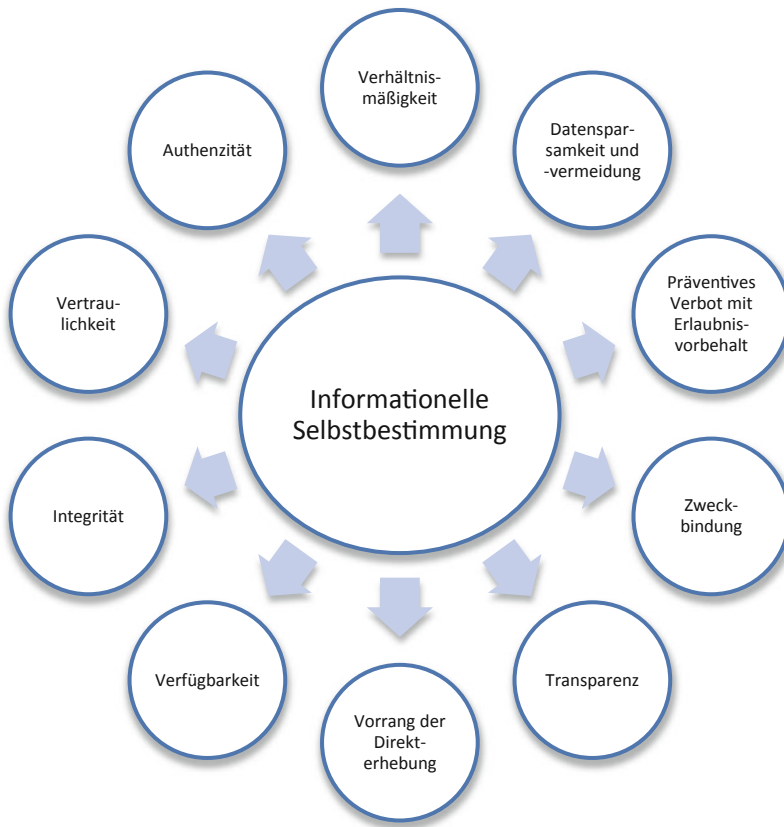


Abb. 2.1 Datenschutzgrundsätze

- 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 Stelle¹ 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 Aufsichtsbehörden². 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 diene 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.

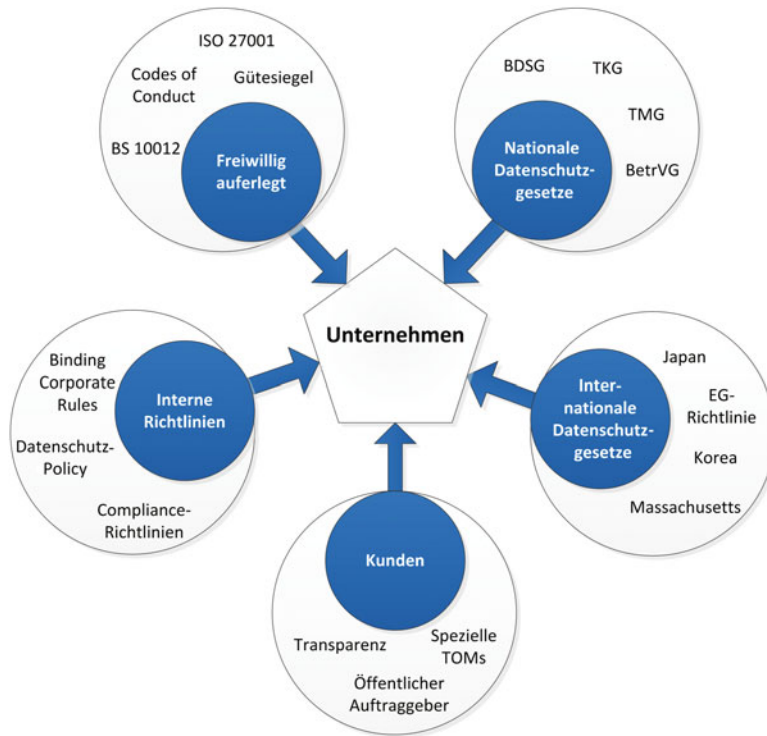


Abb. 2.2 Datenschutzanforderungen an die Unternehmen

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.

Auf diese Weise wird das DSMS der Dynamik im Bereich der Datenschutzanforderungen besser gerecht als über starre Schutzstandards (siehe auch Kap. 3.1).

2.3 Auswirkungen auf die betriebliche Praxis

Als Adressaten der dargestellten Datenschutznormen sowie über die mittelbare Drittwirkung der Grundrechte ist auch die Privatwirtschaft verpflichtet, das Recht des Einzelnen auf informationelle Selbstbestimmung sicherzustellen.

Betrachtet man die zahlreichen gesetzlichen Anforderungen, so wird deutlich, dass sie nahezu alle Unternehmensbereiche durchdringen und die qualifizierte Umsetzung des Datenschutzes daher einen spürbaren **Kostenfaktor** darstellen kann. So können alleine die für ein angemessenes Datenschutzniveau erforderlichen technischen und organisatorischen Maßnahmen (TOMs) eine aufwendige Umgestaltung der bestehenden Infrastruktur im Unternehmen bedeuten. Dies wird sich zukünftig noch verstärken. So sieht auch der Bundesbeauftragte für den Datenschutz in seinem aktuellen Tätigkeitsbericht für die Jahre 2011 und 2012 die Notwendigkeit einer Stärkung auf technischer Ebene [5], um die notwendige Differenzierung bei der Behandlung von personenbezogenen Daten und den damit einhergehenden Konzepten Pseudonymisierung und Anonymisierung umsetzen zu können. Auch das zukunftsweisende Konzept der Industrie 4.0. verlangt mit dem zukünftig immer leichter herzustellenden Personenbezug eine entsprechende Fokussierung auf diesen Aspekt. Außerdem kann die Kontrolle der Auftragnehmer im Rahmen der Auftragsdatenverarbeitung (ADV) sich auf bestehende Geschäftsbeziehungen auswirken. Das bedeutet, dass im konkreten Fall neue Konditionen ausgehandelt oder sogar die Trennung von einzelnen Geschäftspartnern notwendig ist. Und auch die organisatorische Einbindung des betrieblichen Datenschutzbeauftragten sowie die Bereitstellung der für seine Tätigkeit erforderlichen Ressourcen, darunter Schulungsmaßnahmen für die Mitarbeiter, dürfen die Verantwortlichen nicht unterschätzen. Eine rein kostenfokussierte Betrachtung vernachlässigt wesentliche Konsequenzen für die Unternehmen und ihre Geschäftsleitungen.

Datenschutzvorfälle sind heute ein immenser **Risikofaktor**. Dabei beschränkt sich dieser nicht nur auf die direkten Folgen eines Verstoßes gegen die oben genannten Gesetze wie im Folgenden dargelegt wird.

- Zunächst führen Bußgelder, Schadenersatz- und Schmerzensgeldforderungen der Betroffenen, verwirkte Vertragsstrafen etc. zu erheblichen **finanziellen Belastungen**. Dabei muss auch beachtet werden, dass über die geplante Neuregelung des Datenschutzes in Europa zukünftig sogenannte „Privacy Havens“ – Staaten mit geringem Schutzniveau – durch die nach derzeitigem Stand absehbare Einführung des Marktortprinzips nur eingeschränkt weiter als Geschäftsmodell zur Umgehung des europäischen

Datenschutzes funktionieren werden [9]. In solchen Fällen würden demnach in Zukunft Sanktionierungen durch die in den europäischen Staaten ansässigen Aufsichtsbehörden ermöglicht, obwohl das betroffene Unternehmen keinen Sitz in der Europäischen Union hat. Nicht zu unterschätzen sind ebenfalls die **internen Aufwände**, die zur Beseitigung des Datenschutzverstoßes anfallen. Zwar lässt sich eine generelle Quantifizierung schwerlich vornehmen, dennoch ermittelt eine im Mai 2013 veröffentlichte Studie des Ponemon Instituts im Auftrag von Symantec die durchschnittlichen Kosten *eines* verlorenen Datensatzes in Deutschland auf ca. € 151 – der höchste Wert aller untersuchten Länder! [13]

- Auch im Geschäftsverkehr zwischen Unternehmen ist die Beachtung des Datenschutzes von Bedeutung. Die zunehmende Sensibilität für dieses Thema bedingt, dass **Geschäftspartner sich distanzieren**, wenn die Umsetzung des Datenschutzes nicht zweifelsfrei nachgewiesen werden kann. Dies gilt vor allem dann, wenn besonders hohe Anforderungen an den Datenschutz gestellt werden, was regelmäßig bei Geschäftspartnern aus stark regulierten Bereichen wie dem Finanz- oder Gesundheitssektor der Fall ist.
- Insbesondere über die Medien verbreitete Datenschutzvorfälle führen regelmäßig zu schweren **Reputationsschäden**, die sich nur sehr schwer über die Zeit kompensieren lassen. Unternehmen dürfen dabei nicht die Auswirkungen auf die Unternehmenskultur und das Vertrauensverhältnis zu den Beschäftigten und deren Arbeitsmotivation aus dem Blick verlieren. In diesen Fällen kann der Vertrauensverlust einen zwar impliziten aber dafür umso gravierenderen negativen Einfluss auf die Produktivität innerhalb des Unternehmens mit sich bringen.
- Damit einhergehend wird deutlich, dass ein nicht funktionierendes Datenschutzkontrollsystem eine **persönliche Haftung** der Verantwortlichen im Unternehmen begründen kann, sowohl zivilrechtlicher als auch strafrechtlicher Natur. Vorstände und Geschäftsführer begehen durch eine nicht ausreichende Sicherstellung des Datenschutzes eine schwere Pflichtverletzung. Es besteht zudem die reale Gefahr, dass in einem solchen Fall der entsprechende Versicherungsschutz entfällt. Im Strafrecht ist zudem bei Verstößen durch Mitarbeiter unter den entsprechenden Voraussetzungen die Gefahr der Organhaftung für die Geschäftsleitung gegeben. Folglich muss den Verantwortlichen im Unternehmen bewusst sein: Datenschutz ist heute mehr denn je eine Führungsaufgabe.

Der Umgang mit den genannten Risiken verlangt ein geeignetes Risikomanagement von den Unternehmen. Dieser Praxisleitfaden stellt dafür im weiteren Verlauf einen risikobasierten Ansatz vor, mit dem Risiken identifiziert, bewertet und angemessen behandelt werden können.

Weiterhin stellt der Datenschutz einen wichtigen **Qualitätsfaktor** dar. Als konsequente Anwendung des Risikogedankens fordern Unternehmen immer häufiger eine nachgewiesene Datenschutz-Compliance ihrer Geschäftspartner ein. Nur die Unternehmen, die diese Kundenanforderungen umsetzen und nachweisen können, werden für die Auftragsvergabe berücksichtigt. Unternehmen mit direkten datenschutzrelevanten Tätigkeiten gegenüber

natürlichen Personen sind zudem unmittelbar den Anforderungen der Betroffenen ausgesetzt. Als Gegenstück zur negativen Medienaufmerksamkeit sind jedoch positive Beispiele einer Beachtung des Datenschutzes eine Seltenheit geblieben: In der Diskussion etwa um die Zugriffsbefugnisse der Geheimdienste auf den globalen Internetverkehr konnten sich jedoch Anbieter mit darauf angepassten technischen Schutzmaßnahmen insbesondere in Kontinentaleuropa profilieren [1]. Nicht zu unterschätzen ist auch das Bedürfnis der Mitarbeiter, dass die im Rahmen des Beschäftigungsverhältnisses erhobenen personenbezogenen Daten datenschutzkonform verarbeitet werden. Dies wird beispielsweise in der Diskussion um die (Video-)Überwachung am Arbeitsplatz deutlich, gerade wenn das mitbestimmungsrechtliche Korrektiv eines Betriebsrates fehlt.

Es zeigt sich: Der Datenschutz ist heutzutage ein gewichtiger **Wettbewerbsfaktor**. Die Unternehmen, die in diesem Bereich positiv hervortreten, setzen dies gewinnbringend am Markt durch. Auch in der öffentlichen Auftragsvergabe wird der Nachweis der Datenschutzkonformität für den Auftragnehmer erforderlich und von den je nach Vertragstyp einschlägigen „Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT)“ eingefordert. Die weiter zunehmende Bedeutung des Datenschutzes im Rahmen des technischen Fortschrittes verstärkt diesen Trend weiter.

2.4 Notwendigkeit eines Datenschutzmanagementsystems

- Gesetzliche Anforderungen
- Unternehmensgefährdende Risiken
- Kundenanforderungen
- Begrenzte Ressourcen

Schlagworte, die kurz und knapp die Situation beschreiben, in der sich viele Unternehmen derzeit befinden. An diesem Punkt stellt sich zurecht die Frage: Wie wird man all diesen Anforderungen gerecht?

Die klassische **Ad-hoc**-Vorgehensweise, d.h. die von den Datenschutzgesetzen geforderten Tätigkeiten nacheinander bis zu einem bestimmten Stichtag abzuarbeiten, mag für kleinere Unternehmen sinnvoll sein, die kaum datenschutzrelevante Verfahren betreiben. In einem solchen Fall kann es möglich sein, beispielsweise das externe Verfahrensverzeichnis erst auf Kundenwunsch oder Anfrage der Aufsichtsbehörde zu aktualisieren. Je mehr jedoch solche Verfahren im Unternehmen betrieben werden, je mehr Mitarbeiter daran beteiligt sind und je komplexer die Datenströme sind, umso eher stößt die Ad-hoc-Methode an ihre Grenzen. Besonders deutlich wird dies, wenn Ressourcen knapp sind und die Tätigkeiten priorisiert werden müssen. Dann werden die Nachteile dieses Ansatzes deutlich:

- Die stichtagsbezogene Umsetzung lässt regelmäßig eine **Qualitätskontrolle** und daraus resultierende Verbesserungsmaßnahmen außer Acht. So sind etwa während der

Durchführung oder nach dem Stichtag verabschiedete Gesetzesänderungen nur durch ein erneutes Ad-hoc-Projekt umsetzbar.

- Damit einhergehend lässt sich die qualifizierte Umsetzung der Datenschutzerfordernungen nicht zuverlässig bestimmen. Es besteht weiter die **Unsicherheit** von Datenschutzvorfällen im laufenden Betrieb. So kommt die oben erwähnte Pricewaterhouse Coopers-Umfrage aus dem Jahr 2012 [14] zu dem Ergebnis, dass Unachtsamkeit und Unwissenheit der eigenen Mitarbeiter wie bereits in den Jahren zuvor die häufigste Ursache für Datenschutzverstöße sind. Der Datenschutz kann somit nicht einfach von oben herab mit einer Arbeitsanweisung verordnet werden, sondern muss durch Schaffung einer Datenschutz-Awareness bei den Mitarbeitern in die betrieblichen Arbeitsabläufe integriert werden.
- Der scheinbar einmalige Charakter der Tätigkeiten bei der Ad-hoc-Vorgehensweise führt zu **fehlenden Verantwortlichkeiten** im späteren laufenden Geschäftsbetrieb. Auch aktuelle legislatorische Entwicklungen verstärken dieses Problem: So ist bereits absehbar, dass die oben erwähnte EU-Datenschutzgrundverordnung [8] die Pflicht zur Bestellung des betrieblichen Datenschutzbeauftragten einschränken wird. Dieser teilweise Verzicht auf die obligatorische Selbstkontrolle durch den betrieblichen Datenschutzbeauftragten entlässt die Unternehmen jedoch nicht aus der Pflicht, den gesetzlichen Anforderungen nachzukommen. Vielmehr stellt sich gerade in diesen Fällen die Frage, wie der Datenschutz auch ohne die zentrale Instanz des betrieblichen Datenschutzbeauftragten umgesetzt werden kann. Alternative Kontrollinstrumente werden daher in Zukunft an Bedeutung gewinnen und damit einhergehend auch die Notwendigkeit klarer Verantwortlichkeiten.
- Die unzureichende zentrale Koordinierung der Aktivitäten führt zur **uneinheitlichen Umsetzung** in den einzelnen Geschäftsbereichen und ist aufgrund von Doppelarbeiten **ineffizient**. Ebenso sind unerwartete Verzögerungen keine Seltenheit. Denn oftmals wird aufgrund der Vernachlässigung der Planungsphase das Ausmaß der erforderlichen Maßnahmen erst im späteren Verlauf ersichtlich.

An dieser Stelle wird das Erfordernis einer systematischen Herangehensweise an den Datenschutz ersichtlich. Die aufgezeigten Probleme des Ad-hoc-Ansatzes können über ein funktionierendes **Datenschutzmanagementsystem** (DSMS) vermieden werden. Ein solches wurde von SAP erfolgreich eingeführt. Indem klare Verantwortlichkeiten innerhalb des Systems festgelegt und Strukturen etabliert werden sowie ein kontinuierlicher Verbesserungsprozess in Gang gesetzt wird, bereitet das DSMS den Weg hin zu einer effektiven Umsetzung der Datenschutzerfordernungen im SAP-Konzern. Durch die Einbeziehung der Mitarbeiter legt es die Basis für eine notwendige Datenschutz-Awareness der Belegschaft. Über einen risikobasierten Ansatz werden die erwähnten Datenschutzrisiken und Veränderungen der gesetzlichen Rahmenbedingungen angemessen berücksichtigt und eine höhere Effizienz in der Umsetzung der Maßnahmen erreicht. Diese Vorzüge erkennt SAP und nutzt sie. Folglich setzt SAP auch in Zukunft weiter auf dieses Konzept, um den Datenschutz im Konzern sicherzustellen. Dieser Praxisleitfaden gibt dem Leser Hand-

lungsempfehlungen zur Errichtung eines solchen DSMS. Im folgenden Kapitel werden die Funktionsweise und Vorteile – auch für kleine und mittlere Unternehmen – genauer dargestellt.

Fazit

- Die Bedeutung des Datenschutzes in der Informationsgesellschaft wird weiter zunehmen.
- Das Grundrecht des Einzelnen auf informationelle Selbstbestimmung muss auch von den Unternehmen sichergestellt werden.
- Zahlreiche, sich stetig ändernde Datenschutzgesetze sowie besondere Kundenbedürfnisse stellen hohe Anforderungen an die Unternehmen.
- Die Kosten für die Sicherstellung eines angemessenen Datenschutzniveaus sind nicht zu unterschätzen.
- Datenschutzvorfälle sind heute ein immenser Risikofaktor, dem durch ein geeignetes Risikomanagement begegnet werden muss.
- Durch die nachweisliche Konformität mit den Datenschutzerfordernissen können sich Unternehmen hervorragend im Wettbewerb positionieren.
- Eine Ad-hoc-Herangehensweise liefert in vielen Fällen nur unbefriedigende Ergebnisse und eignet sich nicht für mittlere und große Unternehmen.
- Als Verbindung der rechtlichen und betrieblichen Anforderungen unter einem systematischen, managementorientierten Ansatz empfiehlt sich ein Datenschutzmanagementsystem (DSMS). Dieses hat sich in der Praxis bewährt.

Literatur

1. AFP (25. August 2013) Deutsche E-Mail-Anbieter profitieren von NSA-Affäre. <http://www.handelsblatt.com/unternehmen/it-medien/medienbericht-deutsche-e-mail-anbieter-profitieren-von-nsa-affaere/8690072.html>. Zugriffen: 28. Okt. 2013
2. Art. 29-Datenschutzgruppe der Europäischen Kommission (Hrsg) (2006) Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität. 00195/06/DE
3. Bier C (2013) Das koreanische Datenschutzrecht. DuD Datenschutz Datensicherheit 37(7):457–460
4. BITKOM (Hrsg) (2013) Vertrauen und Sicherheit im Netz. http://www.bitkom.org/files/documents/Vertrauen_und_Sicherheit_im_Netz.pdf. Zugriffen: 28. Okt. 2013
5. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) (2013) Tätigkeitsbericht zum Datenschutz für die Jahre 2011–2012. S 24–25
6. BVerfG.: Urteil v. 15. Dezember 1983. Az. 1 BvR 209, 269, 362, 420, 440, 484/83
7. The Commonwealth of Massachusetts (Hrsg) (2007) 201 CMR 17.00: Standards for the protection of personal information of residents of the commonwealth. <http://www.mass.gov/>

- ago/doing-business-in-massachusetts/privacy-and-data-security/standards-for-the-protection-of-personal.html. Zugriffen: 28. Okt. 2013
8. Europäische Kommission (Hrsg) (2012) Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). KOM (2012) 11
 9. FAZ.Net, Reuters (Hrsg) (20. Juni 2013) Europa attackiert Google & Co. <http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/nach-prism-europa-attackiert-google-co-12238587.html>. Zugriffen: 28. Okt. 2013
 10. Gesamtverband der Deutschen Versicherungswirtschaft GDV (Hrsg) (27. März 2013) Versicherungswirtschaft und Datenschützer schaffen neue Maßstäbe für Datenschutz. <http://www.gdv.de/2013/03/versicherungswirtschaft-und-datenschuetzer-schaffen-neue-massstaebe-fuer-datenschutz/>. Zugriffen: 28. Okt. 2013
 11. Münchner Kreis (Hrsg) (2013) Bedürfniswelten. http://www.zukunft-ikt.de/wp-content/uploads/2013_Innovationsfelder_der_digitalen_Welt.pdf. Zugriffen: 28. Okt. 2013
 12. National Institute of Standards and Technology (Hrsg) (2013) Security and privacy controls for federal information systems and organizations. 800-53 Revision 4
 13. Ponemon Institute, Symantec (Hrsg) (2013) Cost of data breach study 2013. http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013-en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach. Zugriffen: 28. Okt. 2013
 14. PricewaterhouseCoopers (Hrsg) (2012) Daten schützen. http://www.pwc.de/de_DE/de/compliance/assets/PwC_Studie_Datenschutz_2012.pdf. Zugriffen: 28. Okt. 2013

Praxisleitfaden zur Implementierung eines
Datenschutzmanagementsystems

Ein risikobasierter Ansatz für alle Unternehmensgrößen

Loomans, D.; Matz, M.; Wiedemann, M.

2014, XVI, 251 S. 48 Abb., 15 Abb. in Farbe., Softcover

ISBN: 978-3-658-02805-3