manuela und georg **REISS**

Praxisbuch IT DOKUMENTATION

BETRIEBSHANDBUCH, SYSTEMDOKUMENTATION UND NOTFALLHANDBUCH IM GRIFF

HANSER

Reiss/Reiss

Praxisbuch IT-Dokumentation

Manuela Reiss
Georg Reiss

Praxisbuch IT-Dokumentation

Betriebshandbuch, Systemdokumentation und Notfallhandbuch im Griff

HANSER

Die Autoren:
Manuela und Georg Reiss, Limeshain

Bibliografische Information der Deutschen Nationalbibliothek:

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

Lektorat: Brigitte Bauer-Schiewek
Copy editing: Petra Kienle, Fürstenfeldbruck
Herstellung: Irene Weilhart
Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München
Umschlagrealisation: Stephan Rönigk
Gesamtherstellung: Kösel, Krugzell
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702
Printed in Germany

Print-ISBN: 978-3-446-43780-7
E-Book-ISBN: 978-3-446-43833-0

Inhalt

Vorwort

Seit der Veröffentlichung der ersten Auflage 2008 unseres Praxishandbuchs IT-Dokumentation haben wir viel positives Feedback erhalten. In der letzten Zeit sind aber auch kritische Stimmen dazugekommen, die bemerken, dass das Buch die aktuellen Entwicklungen nicht berücksichtigt. Für derartige konstruktive Kritik sind wir sehr dankbar. Zum einen zeigt sie uns, dass sich unsere Leser mit den von uns beschriebenen Themen ernsthaft auseinandersetzen. Zum anderen aber haben uns diese Kritiken darin bestärkt, die ohnehin geplante umfassende Überarbeitung unseres Praxishandbuchs endlich in Angriff zu nehmen.

In der Welt der IT hat sich in den vergangenen Jahren viel geändert. Das betrifft nicht nur technische Weiterentwicklungen (beispielsweise im Bereich der Virtualisierung) und neue Themen wie zum Beispiel Collaboration und Cloud Computing. Vielmehr müssen sich IT-Organisationen heute anders aufstellen. In der Vergangenheit hat sich die IT vielfach darauf konzentriert, die Informations- und Kommunikationstechnologien zu beherrschen mit Mitarbeitern[1], die sich in starkem Maß auf konkrete Technologien oder Anwendungen (Netze, Server, Storage usw.) spezialisiert haben. IT-Organisationen mit einseitigem Technologiefokus bekommen jedoch zunehmend Probleme, denn die Anforderungen, die heute an sie gestellt werden, lauten: Serviceorientierung, Prozessorientierung und Kundenorientierung. Die Triebfeder für diese Anforderungen ist die zunehmende Überzeugung, dass die IT einen Mehrwert für das Business erbringen muss. IT-Abteilungen sind daher in der Pflicht, sich auch als interne Service-Provider aufzustellen, die ihren internen Kunden vertraglich geregelte Dienstleistungen mit definierten SLAs anbieten. Zusammen mit einer wachsenden Abhängigkeit der Geschäftsprozesse von der IT ergeben sich daraus auch zunehmende Anforderungen an die IT-Dokumentation.

Damit war für uns klar, dass der dem Buch zugrunde liegende Ansatz zumindest deutlich erweitert werden muss, zum einen in Richtung einer IT-Dokumentation, die auch serviceorientiert agierenden IT-Organisationen gerecht wird, und zum anderen in Richtung einer unternehmensspezifischen Ausprägung der Dokumentation. Wir sind daher dankbar, dass unser Praxisbuch nach den Veränderungen bei Pearson beim Hanser Verlag nicht nur eine neue Heimat gefunden hat, sondern dass wir auch bei der Veröffentlichung einer deutlich erweiterten Auflage mit viel Engagement unterstützt wurden.

Was erwartet Sie in der neuen Auflage?

---

[1] Wenn bei personellen Bezeichnungen die männliche Form gewählt wurde (z. B. Mitarbeiter, Administrator), so ist damit in gleicher Weise die weibliche Form (Mitarbeiterin, Administratorin) gemeint.

Um das Buch durchgängig noch praxistauglicher zu gestalten, führen wir Sie Schritt für Schritt durch Ihr Dokumentationsprojekt zum Aufbau bzw. zur Optimierung Ihrer IT-Dokumentation. Als Leitschnur dienen hierbei die folgenden Fragestellungen:

- Warum muss dokumentiert werden?
- Welche Dokumentationsfelder gibt es? Wie kann eine IT-Dokumentation strukturiert werden?
- Was gehört zur Dokumentation für den IT-Betrieb?
- Was sind notwendige Dokumente der Notfalldokumentation?
- Worauf ist bei der IT-Projektdokumentation zu achten?
- Wie können Dokumentationsanforderungen in der Praxis umgesetzt werden?
- Mit welchen Tools kann dokumentiert werden?

Zu einer höheren Praxistauglichkeit trägt auch der in dieser Auflage neu entwickelte Strukturierungsansatz bei, der die Dokumentationserfordernisse der meisten IT-Organisationen trotz ihrer unterschiedlichen Ausprägungen hinsichtlich Prozess- und Serviceorientierung abbildet. Wie uns nämlich die Erfahrungen aus den vorangegangenen Ausgaben des Praxishandbuchs IT-Dokumentation zeigen, ist es schwierig, aus einem komplexen generischen Modell die für das eigene Unternehmen relevanten Dokumente zu identifizieren. Um diesem Problem zu begegnen, haben wir in dieser Auflage den Dokumentationsleitfaden für die IT-Betriebsdokumentation in fünf Bereiche unterteilt, von denen jeder Teil die komplette IT-Betriebsdokumentation für eine Stufe abbildet.

Was erwartet Sie in den einzelnen Kapiteln?

Unabhängig davon, ob Sie den Aufbau Ihrer IT-Dokumentation oder eine Re-Organisation planen: Zu Beginn müssen Sie Ihre Ziele und Anforderungen ermitteln. Diese leiten sich aus gesetzlichen Verpflichtungen, Normen und Standards, aber auch aus wirtschaftlichen und anderen unternehmensstrategischen Entscheidungen ab. Leider wird in der Praxis die Analyse der Ziele und Anforderungen häufig vernachlässigt. Stattdessen wird oft ein Tool angeschafft, ohne aber zu wissen, wohin die Reise eigentlich gehen soll. In **Kapitel 1, »Anforderungen an die IT-Dokumentation«** möchten wir Sie bei der Beantwortung dieser Fragen unterstützen. Hierbei betrachten wir, welche Dokumentationsanforderungen sich aus gesetzlichen Regelungen und anderen Compliance-Anforderungen ableiten lassen und welche Standards und Zertifizierungen Relevanz für die IT-Dokumentation haben. Außerdem beleuchten wir, welche Anforderungen Prüfer auf Basis der international und national gültigen Prüfungsstandards stellen, da »Revisionssicherheit« und »Compliance« nicht nur Schlagwörter sind, sondern eine immer höhere Bedeutung erlangen.

Im nächsten Schritt möchten wir mit Ihnen das Grundgerüst einer ganzheitlichen Dokumentation »zimmern«. Dazu zeigen wir Ihnen in **Kapitel 2, »Strukturierung einer ganzheitlichen IT-Dokumentation«**, welche Bereiche im Rahmen der IT-Dokumentation zu berücksichtigen sind, und wir werden dabei die IT-Dokumentation auch im Kontext einer unternehmensweiten Dokumentation betrachten.

Nachdem gewissermaßen der »Schrank« für die IT-Dokumentation steht, werden wir mit Ihnen gemeinsam in den daran anschließenden Kapiteln »die Schubladen dieses Schranks füllen«. Hierzu erläutern wir, welche Dokumente im Rahmen der **»Betriebsdokumentation« (Kapitel 3)**, der **»Notfalldokumentation« (Kapitel 4)** und der **»Projektdokumentation« (Kapitel 5)** zu erstellen sind.

Einen Schwerpunkt bildet dabei die **Betriebsdokumentation**. Auf Basis eines Strukturierungsmodells möchten wir Sie dabei unterstützen, eine für Ihre IT-Organisation passende Struktur zu entwickeln und die erforderlichen Dokumente zu ermitteln. Seit der ersten Auflage war es unser Anspruch, einen Ansatz für den Aufbau einer IT-Dokumentation zu bieten, der generisch ist und für jede Unternehmensgröße[2] passt. Die zuvor beschriebenen Erweiterungen in Richtung eines service- und prozessorientierten Ansatzes erfordern aber eine komplexere Struktur. Und diese kann nicht für alle Unternehmen passen, da sich natürlich jede IT-Organisation in einer anderen Situation befindet. Aus diesem Grund haben wir ein Stufenmodell entwickelt, mit dem Sie einfach ermitteln können, wie eine für Ihr Unternehmen passende IT-Dokumentation aussehen kann und was zu dokumentieren ist.

Bis zu diesem Schritt wissen Sie, »Warum« und »Was« es zu dokumentieren gilt. Im anschließenden **Kapitel 6 »Umsetzung in der Praxis«** steht das »Wie« im Mittelpunkt, beispielsweise mit der Frage: Wie schaffe ich es, die Dokumentation aktuell zu halten?

An dieser Stelle werden wir häufig nach Vorlagen für die verschiedenen Dokumente gefragt. Achtung: Dieses Buch versteht sich nicht als eine Sammlung von Vorlagen, mit denen schematisch Dokumente erstellt werden können. Denn unsere jahrelangen Erfahrungen zeigen, dass diese nur eines erzeugen: Dokumente, die nach der Fertigstellung (und der Vorlegung beim Auditor) irgendwo in den Weiten des Dateisystems verschwinden.

Entscheidend ist vielmehr, individuelle und auf die Bedürfnisse des eigenen Unternehmens ausgerichtete Dokumente zu erstellen, diese aktuell zu halten und weiterzuentwickeln. Hierzu bedarf es der Einrichtung eines Dokumentationsmanagements. Ohne ein solches ist es kaum möglich, eine nachhaltige Dokumentation bzw. IT-Dokumentation aufzubauen. Ohne festgelegte Verantwortlichkeiten, Richtlinien und definierte Abläufe wird es nicht gelingen, aus einer unzusammenhängenden Sammlung von Dokumenten eine ganzheitliche Dokumentation aufzubauen. Einen Schwerpunkt des Kapitels zur Umsetzung in der Praxis bilden deshalb die Dokumentationsrichtlinie sowie die erforderlichen Dokumentationsverfahren. Wie wir Ihnen zeigen werden, ist eine solche Richtlinie ein gutes Instrument zur Umsetzung der Dokumentationsziele und Anforderungen.

Aber natürlich ist es hilfreich, bei der Erstellung von Dokumenten auf die eine oder andere Vorlage zurückgreifen zu können. Soweit möglich und sinnvoll liefern wir Ihnen Beispiele und mögliche Inhalte für zu erstellende Dokumente und verweisen auf hilfreiche Quellen.

Bleibt als letzte Frage offen: Womit, d. h. mit welchen Tools kann dokumentiert werden? Diese werden in **Kapitel 7 »Eine Toolbox für die IT-Dokumentation«** behandelt. Je umfangreicher die Anzahl an Dokumenten und je größer die Komplexität der Abhängigkeiten ist, desto stärker ist das Erfordernis nach einer zentralen IT-gestützten Datenhaltung und Tool-Unterstützung bei der Dokumentation. Auch in dieser Auflage stellen wir Ihnen daher eine Reihe von Tools vor, die Sie bei der Bewältigung der unterschiedlichen Dokumentationsaufgaben unterstützen können. Dabei ist uns klar, dass wir uns hiermit dem Vorwurf einer willkürlichen und nicht objektiven Auswahl aussetzen.

Wir haben jedoch in keiner Weise den Anspruch, Ihnen den Sieger eines fundierten Vergleichstests zu präsentieren, und wir behaupten auch nicht, das beste oder einzig mögliche Tool vorzustellen. Wir möchten Ihnen lediglich exemplarisch anhand von durch uns als

[2] Wenn in diesem Buch von Unternehmen die Rede ist, sind damit in gleicher Weise auch andere Organisationen wie Behörden, Körperschaften usw. gemeint.

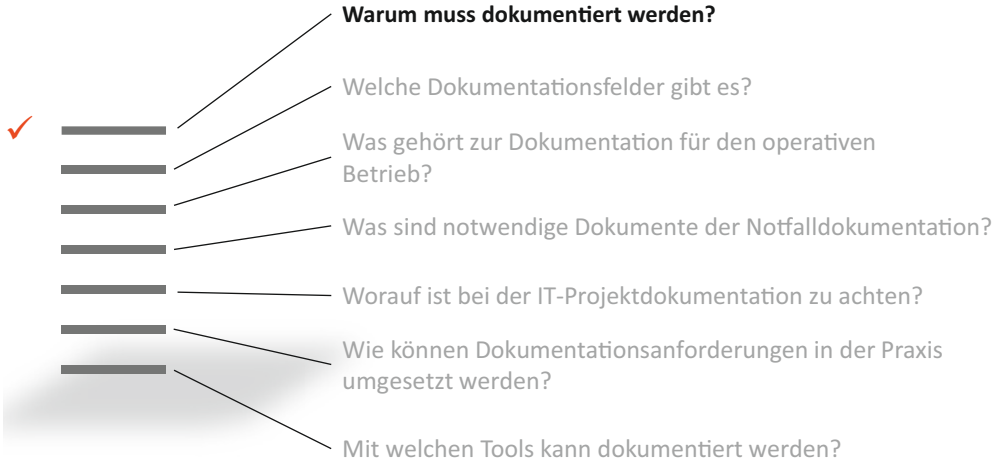
nützlich eingestuften Tools zeigen, wie Anwendungen Sie bei der Bewältigung der verschiedenen Dokumentationsaufgaben unterstützen können, und wir möchten Ihnen insbesondere Anregung für die zwingend notwendige Evaluierung bieten. Nicht mehr und nicht weniger.

Wir freuen uns auf Ihr Feedback und auf einen regen Gedankenaustausch!

Ihre Autoren Manuela und Georg Reiss

info@dokuit.de

1 Anforderungen an die IT-Dokumentation



Richtigerweise startet ein Projekt zur Erstellung bzw. Optimierung der IT-Dokumentation mit der Frage: »Was muss ich in meiner IT-Organisation eigentlich dokumentieren?« Denn es ist entscheidend, dass man neben individuellen Anforderungen und Zielen im ersten Schritt analysiert, welche verbindlichen Dokumentationsverpflichtungen oder mit anderen Worten, welche Compliance-Anforderungen es für das eigene Unternehmen gibt. Hierbei möchte dieses Kapitel Sie unterstützen. Es beleuchtet, welche Anforderungen sich aus gesetzlichen Anforderungen und Verordnungen für die IT-Dokumentation ableiten lassen.

Unternehmen müssen aber nicht nur sicherstellen, dass Compliance-Anforderungen eingehalten werden, sondern dies auch regelmäßig kontrollieren und im Rahmen der Jahresabschlussprüfung gegebenenfalls auch nachweisen. Welche Anforderungen Prüfer und Revisoren an die IT-Dokumentation stellen, wird daher ebenfalls vorgestellt.

In diesem Kapitel finden Sie die folgenden Themenschwerpunkte:

- Was heißt Compliance?
- Branchenübergreifende Anforderungen an die IT-Dokumentation
- Anforderungen aus branchenspezifischen Vorschriften
- Was prüfen Abschlussprüfer und Revisoren?
- Dokumentationsanforderungen in Österreich und in der Schweiz
- Relevante Normen und Standards

1.1 Was heißt Compliance?

Die Bezeichnung *Compliance* stammt ursprünglich aus dem Englischen und bedeutet so viel wie »Einhaltung« oder »Befolgung«. Leider sucht man eine allgemeingültige Definition für den Begriff vergebens. Bezogen auf gesetzliche Anforderungen verbirgt sich hinter dem Begriff Compliance die Bedeutung eines gesetzestreuen Verhaltens. Weiter gefasst bedeutet Compliance die Erfüllung aller rechtlichen Vorgaben und aller branchenspezifischen Vorgaben sowie der innerbetrieblichen Richtlinien.

Bei *IT-Compliance* als Teilbereich von Compliance bezieht sich die oben genannte Einhaltung internationaler, nationaler und innerbetrieblicher Gesetze, Richtlinien und Bestimmungen auf den Umgang mit der im Unternehmen vorhandenen Informationstechnik. Dabei adressiert IT-Compliance vor allem die Bereiche Sicherheit, Verfügbarkeit, Integrität und Datenschutz. Für diese Bereiche müssen Maßnahmen, Prozesse und Kontrollen implementiert und nachvollziehbar dokumentiert werden.

Compliance-Anforderungen mit Relevanz für die IT

Für eine Umsetzung der Compliance-Anforderungen ist es aber selbstverständlich erst einmal notwendig, diese zu kennen. Leider gibt es keinen allgemeingültigen Standard, was in eine IT-Dokumentation aufzunehmen ist, oder gar ein gesondertes Dokumentationsgesetz.

Es existieren jedoch eine ganze Reihe von Verpflichtungen für die Erstellung und Vorhaltung einer Dokumentation, die deren Inhalt und Aufbau prägen. Branchenübergreifend sind insbesondere Vorschriften aus dem Bereich der Buchführung und Rechnungslegung sowie Datenschutz und steuerliche Thematiken für verschiedenartige Unternehmen relevant. Die Vorschriften des Handelsgesetzbuchs, die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), das Bundesdatenschutzgesetz (BDSG) sowie die entsprechenden Regelungen der Abgabenordnung (AO) gilt es hier zu beachten. Und mit dem amerikanischen Sarbanes-Oxley Act (SOX) und dem europäischen Pendant 8. EU-Richtlinie (auch als »Euro-SOX« bezeichnet) bzw. deren Umsetzung in nationales Recht in Form des Bilanzrechtsmodernisierungsgesetzes (BilMoG) wurden in den letzten Jahren Regelungen mit Gesetzeskraft verabschiedet, die einen erheblichen Einfluss auf die vorzuhaltende IT-Dokumentation haben. Wenn auch die meisten gesetzlichen Regelungen von kaufmännischen Grundsätzen wie dem Gläubigerschutz getrieben sind, so haben sie dennoch für die IT eine direkte Bedeutung, da die kaufmännischen Kernprozesse wie Buchhaltung und Einkauf in aller Regel IT-gestützt ablaufen (z. B. die ERP-Anwendung SAP). Neben den branchenübergreifenden Vorgaben unterliegen Unternehmen einzelner Branchen z. T. zusätzlichen, sehr spezifischen Anforderungen.

Den Gesetzen und Verordnungen ist allerdings gemein, dass die beschriebenen Anforderungen mehr oder weniger allgemein gehalten sind und die konkrete Umsetzung offen bleibt. Mit der Frage, wie der Aufbau einer gesetzeskonformen IT-Dokumentation sichergestellt werden kann, werden die Verantwortlichen allein gelassen. An dieser Stelle lohnt sich ein Blick auf einige relevante Standards und Normen.

Während Gesetze und daraus abgeleitete Rechtsnormen verbindlichen Charakter haben, entfalten Standards ihre Wirkung durch nationale oder internationale Anerkennung wie beispielsweise bei den ISO-Normen oder den DIN-Standards. Normen und Standards helfen

dabei, gesetzliche Anforderungen einzuhalten, und dienen bei deren Umsetzung als Nachweis der Einhaltung. So weist ein Unternehmen, das eine Zertifizierung nach dem Sicherheitsstandard ISO 27001 erlangt hat, damit nach, dass es einen Sicherheitsprozess und die nach aktuellem Erkenntnisstand möglichen Sicherheitsmaßnahmen implementiert hat. Eine Organisation, die nicht über diese Zertifizierung verfügt, muss hierfür Einzelnachweise erbringen.

1.2 Branchenübergreifende Anforderungen an die IT-Dokumentation

Ein Gesetz ist eine Sammlung von allgemein verbindlichen Rechtsnormen, die in einem förmlichen Verfahren vom Gesetzgeber erlassen worden ist. Und entgegen der landläufigen Meinung gerade auch vieler erfahrener IT-Administratoren gibt es eine Reihe von allgemeinen Unternehmensgesetzen, aus denen sich aufgrund der immer stärkeren Abhängigkeiten der Geschäftsprozesse von der IT direkt oder indirekt Anforderungen an die IT-Dokumentation ergeben.

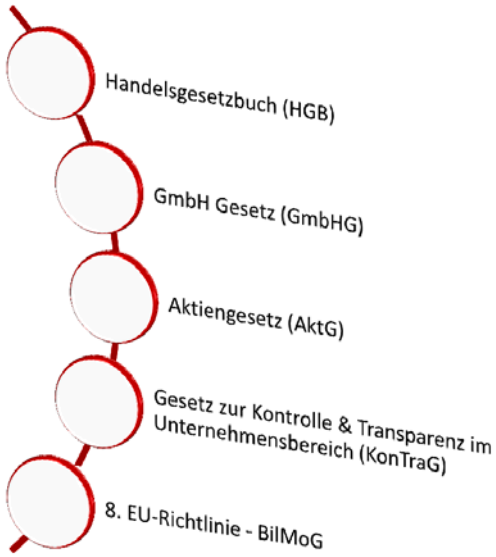


Bild 1.1
Für die IT-Dokumentation relevante allgemeine Unternehmensgesetze

Zusätzlich zu den allgemeinen Unternehmensgesetzen gibt es eine Reihe weiterer Gesetze, Richtlinien und Verordnungen, die ebenfalls Relevanz für die IT-Dokumentation haben. Bei den Richtlinien und Verordnungen handelt es sich um Handlungsvorschriften mit bindendem Charakter, die im Gegensatz zu Gesetzen nicht vom Staat, sondern von einer Organisation ausgegeben werden.

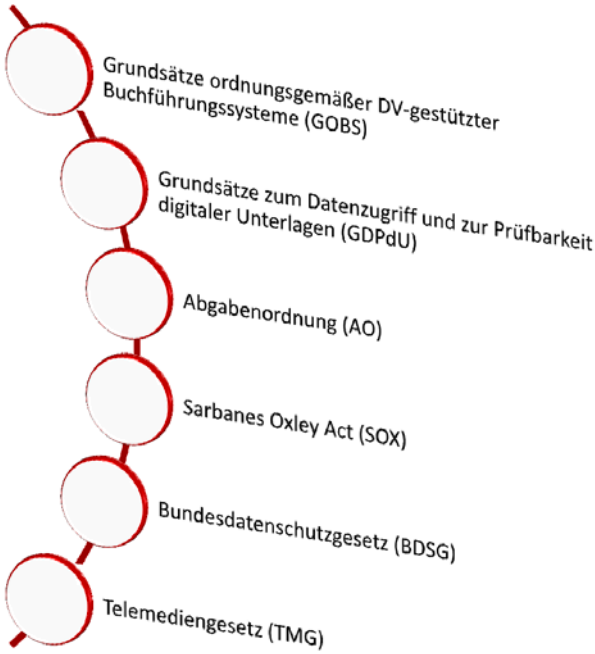


Bild 1.2 Weitere Gesetze und Verordnungen mit Relevanz für die IT-Dokumentation

In den folgenden Abschnitten werden die vorstehend aufgeführten Gesetze und Verordnungen im Überblick vorgestellt und die daraus ableitbaren Anforderungen an die IT-Dokumentation erläutert. Weitere Informationen zu den konkreten Dokumentationsanforderungen finden Sie auch in *Abschnitt 1.4*. In diesem wird beschrieben, welche Anforderungen Wirtschaftsprüfer und Revisoren an die Dokumentation stellen.

1.2.1 Handelsgesetzbuch (HGB)

Das Handelsgesetzbuch (HGB) ist die zentrale Vorschrift für das Handelsrecht in Deutschland. Es enthält sowohl Regelungen für Gesellschaftsformen als auch für Handelsgeschäfte und die Führung der relevanten Handelsbücher.

Im dritten Buch des HGB sind die Vorschriften für das Führen der Handelsbücher enthalten. So ist in § 238 Abs. 1 geregelt, *»dass die Buchführung so beschaffen sein muss, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann«* (HGB). Die Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung verfolgen lassen. Gemäß § 239 Abs. 2 müssen die Eintragungen in Büchern und die sonst erforderlichen Aufzeichnungen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden. Und in Abs. 4 ist festgelegt, dass *»die Handelsbücher und die sonst erforderlichen Aufzeichnungen auch in der geordneten Ablage von Belegen bestehen oder auf Datenträgern geführt werden können, soweit diese Formen der Buchführung einschließlich des dabei angewandten Verfahrens den Grundsätzen ordnungsmäßiger Buchführung entsprechen. Bei der Führung der Handelsbücher und der*

sonst erforderlichen Aufzeichnungen auf Datenträgern muss insbesondere sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb einer angemessenen Frist lesbar gemacht werden können« (HGB).

Ableitbare Anforderungen an die IT-Dokumentation

Die zuvor genannten Absätze sind der Kern der Grundsätze ordnungsgemäßer Buchführung (GoB), die wiederum die Basis für die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) darstellen. Informationen zur GoBS finden Sie in *Abschnitt 1.1.5*. Wichtig ist in diesem Zusammenhang, dass die Zulässigkeit der Speicherung auf Datenträger davon abhängig gemacht wird, dass auch das dabei angewandte Verfahren den Grundsätzen ordnungsmäßiger Buchführung entsprechen muss. Hier ist bereits ein sehr direkter Bezug zur IT und damit zur IT-Dokumentation gegeben.

Auch im Zusammenhang mit den Festlegungen zur Aufbewahrung von Unterlagen in § 257 wird ein Bezug zur IT hergestellt. So ist nach Abs. 1 jeder Kaufmann verpflichtet, Unterlagen wie zum Beispiel Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen geordnet aufzubewahren, und zwar für zehn Jahre (Abs. 4). Hieraus kann abgeleitet werden, dass damit auch die Verfahrensdokumentation gemeint ist.

Die Art der Aufbewahrung regelt § 257 Abs. 3 des HGB derart, dass mit Ausnahme der Eröffnungsbilanzen, Jahresabschlüsse und Konzernabschlüsse die in Abs. 1 aufgeführten Unterlagen

> *»auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden können, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten*
>
> 1. *mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden,*
> 2. *während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.«* (HGB)

Bemerkenswert hierbei ist, und dies hat Relevanz für die gesamte IT-Dokumentation, dass das HGB Anforderungen definiert, die sich auf drei Teilbereiche eingrenzen lassen: *Verfügbarkeit*, *Integrität* und *Ordnungsmäßigkeit*.

- **Verfügbarkeit:** Die Verfügbarkeit der geführten Handelsbücher und der geschäftlichen Unterlagen muss sichergestellt sein. Ein Großteil der geschäftlichen Unterlagen wird mittlerweile elektronisch in Dokumentenmanagementsystemen und anderen IT-Systemen geführt sowie elektronisch archiviert. Wirtschaftsprüfer und Finanzbehörden verlangen daher bei einer Prüfung Nachweise darüber, dass die Daten in angemessener Zeit wiederherzustellen sind.
- **Integrität:** So wie man in den »alten« Buchhaltungskladden keine Veränderung der Buchungen vornehmen durfte, die nicht nachvollziehbar war, so gilt dies auch für die heutigen Buchhaltungssysteme und Daten. Integrität ist zum Beispiel wegen der gesetzlichen Aufbewahrungsfristen eine kritische Anforderung an die E-Mail-Archivierung. Entscheidend sind hierbei die hardwaremäßigen, softwaremäßigen und organisatorischen Sicherheitsfunktionen, die auch nachzuweisen sind.

- **Ordnungsmäßigkeit:** Gemäß HGB müssen die Eintragungen in Büchern und die sonst erforderlichen Aufzeichnungen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden, wobei es heute wohl kaum noch Unternehmen gibt, die für die Buchführung keine IT-gestützten Buchhaltungssysteme im Einsatz haben. Entsprechend gilt dies für die verwendeten Buchhaltungssysteme und muss für diese überprüfbar sein. In enger Verbindung damit steht die Authentizität, für die die Überprüfung der Benutzerrechte wichtig ist.

1.2.2 Aktiengesetz (AktG) und GmbH-Gesetz (GmbHG)

Das Aktiengesetz ist anwendbar auf alle Aktiengesellschaften sowie OHGs und KGs, auf GmbHs bei entsprechender Größe, Branche, Struktur usw. sowie auf Versicherungen und Banken. Es beschreibt die gesetzlichen Anforderungen an eine Aktiengesellschaft und regelt unter anderem die Aufgaben der Organe der Aktiengesellschaft. Im Aktiengesetz wird festgelegt, dass ein Vorstand persönlich haftet, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG). (AktG)

Geschäftsführern einer GmbH wird im GmbH-Gesetz *»die Sorgfalt eines ordentlichen Geschäftsmannes«* (GmbHG) auferlegt (§ 43 Abs. 1 GmbHG), welches ähnliche Folgerungen für das Risikomanagement beinhaltet wie für Vorstände nach dem Aktiengesetz.

Ableitbare Anforderungen an die IT-Dokumentation

Die oben genannten Formulierungen klingen recht allgemein und unverbindlich. Hieraus lassen sich jedoch konkrete Verpflichtungen an die Gewährleistung angemessener IT-Sicherheitsmaßnahmen ableiten, die natürlich auch zu dokumentieren sind. IT-Sicherheitsvorfälle können massive wirtschaftliche Schäden verursachen und gegebenenfalls den Bestand eines Unternehmens gefährden. Erleidet das Unternehmen aufgrund der Verletzung von Organisations- und Aufsichtspflichten einen Schaden, haftet die Geschäftsleitung u. U. persönlich auf Schadensersatz (Organisationsverschulden).

Für bestimmte Berufsgruppen wie Ärzte, Rechtsanwälte oder Angehörige sozialer Berufe gibt es darüber hinaus Sonderregelungen im Strafgesetzbuch, die Freiheitsstrafen vorsehen, wenn vertrauliche Angaben von Patienten, Mandanten bzw. Klienten ohne deren ausdrückliche Einwilligung öffentlich gemacht werden (§ 203 StGB). Ein fahrlässiger Umgang mit Informationstechnik kann diesen Tatbestand unter Umständen bereits erfüllen.

Zusätzlich beinhalten beide Gesetze die klare Aufforderung an die Unternehmensleitung, ein geeignetes Risikomanagementsystem einzurichten und nachzuweisen. Diese zweite Forderung ist erst 1998 in das Gesetz mit aufgenommen worden und bildet die Basis für das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).

1.2.3 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Ausgehend von den zunehmenden Korruptions- und Bilanzskandalen der 1980er- und 1990er-Jahre des letzten Jahrhunderts wurde 1998 das Gesetz KonTraG verabschiedet. Seine Anwendung erstreckt sich über die Aktiengesellschaft hinaus auch auf GmbH-Gesellschaften. Ziel dieses Gesetzes ist die Stärkung und Verbesserung der Unternehmensführung und Unternehmenskontrolle. Das KonTraG präzisiert dabei die entsprechenden Festlegungen im Aktiengesetz und im Handelsgesetzbuch. (KonTraG)

Das KonTraG ist ein Artikelgesetz und damit eine Änderung und Ergänzung mehrerer vorhandener Gesetze. Es hat bei seiner Verabschiedung auf andere Gesetze Einfluss genommen, beispielsweise durch Änderungen und Ergänzungen des Handelsgesetzbuchs (HGB) und des Aktiengesetzes (AktG), durch die die Corporate Governance in deutschen Unternehmen erhöht werden soll. Demzufolge ist u. a. ein unternehmensweites Risikofrüherkennungs- und Überwachungssystem zu implementieren. Ebenfalls müssen

- Aussagen zu potenziellen Risiken und
- Aussagen zur Risikostruktur des Unternehmens

dokumentiert im Lagebericht des Jahresabschlusses präsentiert werden.

Zu diesem Zweck ist in das Aktiengesetz in § 91 der Absatz 2 neu aufgenommen worden, wonach der Vorstand verpflichtet wird, geeignete Maßnahmen zu treffen. Insbesondere ist *»ein Überwachungssystem einzurichten, damit Entwicklungen, die den Fortbestand der Gesellschaft gefährden, frühzeitig erkannt werden.«* (AktG) Hervorgehoben wird die Betonung der internen Überwachung durch die Aufnahme eines weiteren Absatzes (Nr. 4) in § 317 des HGB, wonach im Rahmen der Jahresabschlussprüfung zu beurteilen ist, *»ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.«* (AktG)

Mit dem § 91 Abs. 2 AktG ist also nicht nur die Vorhaltung einer Revision gefordert, sondern auch, ob diese ihre Aufgaben erfüllen kann. Der Jahresabschlussprüfer hat also zu beurteilen, ob eine im Verhältnis zu den Unternehmensrisiken angemessene Revision existiert. In diesem Zusammenhang wird ebenfalls regelmäßig kontrolliert, wie viel und welche IT-Prüfungen im Berichtsjahr durchgeführt wurden.

Ableitbare Anforderungen an die IT-Dokumentation

Häufig werden für die Organisation und die Berichtserstellung des Risikofrüherkennungs- und -Überwachungssystems Anwendungen als Unterstützung implementiert. Hier ist insbesondere auf die Integrität der Anwendungen und die Eignung sowie auf das Rechte- und Rollenkonzept zu achten.

1.2.4 8. EU-Richtlinie/BilMoG

Nicht nur in Amerika haben Bundesgesetze eine immer stärkere Bedeutung für die IT. Auch in der EU sind mit der Richtlinie über die Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen aus dem Jahr 2006 Regelungen geschaffen worden, die eine

Auswirkung auf die IT-Dokumentation entfalten. In journalistischer Vereinfachung wird diese sogenannte 8. EU-Richtlinie als »Euro-SOX« bezeichnet, da sie eine ähnliche Auswirkung auf die Überwachungs- und Nachweispflichten der Unternehmen hat. (Union)

Tatsächlich stellt diese Richtlinie aber eine Harmonisierung und Konkretisierung bereits bestehender EU-Richtlinien aus den Jahren 1978 bis 1984 dar und ist nicht wie SOX direkt an die Unternehmen, sondern an die Mitgliedsstaaten der EU gerichtet. Erfasst werden auch nur Unternehmen von öffentlichem Interesse, wobei jeder Mitgliedsstaat eine eingeschränkte Entscheidungsfreiheit hat.

Ableitbare Anforderungen an die IT-Dokumentation

Für die IT ist insbesondere der Artikel 41 der Richtlinie entscheidend, wonach jedes von der Richtlinie erfasste Unternehmen einen Prüfungsausschuss zu bilden hat, unabhängig von den sonstigen Überwachungsorganen, wie zum Beispiel einer internen Revision. Im Rahmen des BilMoG hat der Prüfungsausschuss die Wirksamkeit des internen Kontrollsystems (IKS) und des Risikomanagements zu überwachen. Dies beinhaltet die Verpflichtung des Abschlussprüfers, entsprechende IKS-Dokumentationen zu prüfen und über wesentliche Schwächen bei der internen Kontrolle des Rechnungslegungsprozesses zu berichten.

Auch wenn sich aus Artikel 41 nicht ableiten lässt, welche Anforderungen an die Prozesse und an das interne Kontrollsystem gestellt werden, so verbirgt sich hinter den Begriffen »Überwachung« und »Wirksamkeit« die Grundforderung nach einer aussagefähigen Dokumentation zum IT-Risiko- und Sicherheitsmanagement.

1.2.5 Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)

Die GoBS sind eine Verwaltungsvorschrift und beschreiben in Präzisierung des HGB und der Abgabenordnung die organisatorischen und technischen Anforderungen an die IT-gestützte Buchführung.

Generell stellen die GoBS die gleichen Prinzipien an die DV-gestützte Buchführung, wie sie für eine manuell erstellte Buchführung gelten. Aus Sicht der IT sind insbesondere die *Kapitel 4, Internes Kontrollsystem (IKS),* und *Kapitel 6, Dokumentation und Prüfbarkeit,* von Bedeutung. (GoBS)

Nach Kapitel 6.1 der GoBS ist eine Verfahrensdokumentation erforderlich, aus der Inhalt, Aufbau und Ablauf des Abrechnungsverfahrens vollständig ersichtlich sind. Die Verfahrensdokumentation für das Abrechnungssystem muss insbesondere folgende Bereiche beinhalten:

- eine Beschreibung der sachlogischen Lösung,
- die Beschreibung der programmtechnischen Lösung,
- eine Beschreibung, wie die Programmidentität gewahrt wird,
- eine Beschreibung, wie die Integrität von Daten gewahrt wird,
- Arbeitsanweisungen für den Anwender.

Allein hinter der Anforderung zur Beschreibung der sachlogischen Lösung verbergen sich gemäß Kapitel 6.2.1 der GoBS die folgenden Dokumentationsanforderungen:

- *»Generelle Aufgabenstellung*
- *Beschreibung der Anwenderoberflächen für die Ein- und Ausgabe einschließlich der manuellen Arbeiten*
- *Beschreibung der Datenbestände*
- *Beschreibung von Verarbeitungsregeln*
- *Beschreibung des Datenaustausches (Datenträgeraustausch/Datentransfer)*
- *Beschreibung der maschinellen und manuellen Kontrollen*
- *Beschreibung der Fehlermeldungen und der sich aus den Fehlern ergebenden Maßnahmen*
- *Schlüsselverzeichnisse*
- *Schnittstellen zu anderen Systemen«* (GoBS)

In Kapitel 4 der GoBS werden die Anforderungen an das interne Kontrollsystem definiert, wobei das IKS als *»die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen«* verstanden wird. Das IKS hat nach Kapitel 4.1 die folgenden Aufgaben zu erfüllen:

- *Sicherung und Schutz des vorhandenen Vermögens und vorhandener Informationen vor Verlusten aller Art;*
- *Bereitstellung vollständiger, genauer und aussagefähiger sowie zeitnaher Aufzeichnungen;*
- *Förderung der betrieblichen Effizienz durch Auswertung und Kontrolle der Aufzeichnungen;*
- *Unterstützung der Befolgung der vorgeschriebenen Geschäftspolitik.* (GoBS)

Aus GoBS wird GoBIT

Die GoBS sind in Zusammenarbeit mit der *Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV)* entwickelt worden. Aufgrund der Weiterentwicklung der technischen, rechtlichen und organisatorischen Rahmenbedingungen werden die GoBS seit dem Jahr 2005 durch eine Projektgruppe bei der AWV überarbeitet. Die neue Fassung trägt den Namen *GoBIT: Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz*.

Seit dem 13. 10. 2013 liegt ein öffentlicher Entwurf der GoBIT vor. Sie können diesen in der jeweils aktuellen Fassung (bis zur Veröffentlichung der verabschiedeten Version) von der Website des AWV herunterladen [*http://www.awv-net.de/cms/index-b-267-848.html*] (AWV).

Ableitbare Anforderungen an die IT-Dokumentation

Insgesamt beschreiben die GoBS einen umfangreichen Forderungskatalog an die IT-Dokumentation, der noch um weitere Kapitel wie die Datensicherheit und die Wiedergabe der auf Datenträgern geführten Unterlagen ergänzt wird. Bei Nichtbeachtung der Dokumentationsanforderungen der GoBS und insbesondere beim Fehlen einer Verfahrensdokumentation kann die Ordnungsmäßigkeit der Buchführung formell infrage gestellt werden. Außerdem

werden Buchführungsmängel von den Prüfern im Prüfungsbericht vermerkt, was gegebenenfalls negative Auswirkungen auf das Rating haben kann.

Aus dem HGB leiten sich vor allem Anforderungen an die Archivierung von kaufmännischen Unterlagen ab:

- Ordnungsmäßigkeit,
- Vollständigkeit,
- Sicherheit des Gesamtverfahrens,
- Schutz vor Veränderung und Verfälschung,
- Sicherung vor Verlust,
- Nutzung nur durch Berechtigte,
- Einhaltung der Aufbewahrungsfristen,
- Dokumentation des Verfahrens,
- Nachvollziehbarkeit,
- Prüfbarkeit.

Das eigentliche Dokument mit den Vorgaben zum Thema Verfahrensdokumentation aber ist die GoBS. Demzufolge muss die Verfahrensdokumentation den gesamten organisatorischen und technischen Prozess für Dokumente beschreiben, die nach Handelsrecht und steuerrechtlichen Vorgaben aufbewahrt werden müssen. Dies umfasst:

- die Entstehung (Erfassung),
- die Indizierung,
- die Speicherung,
- das eindeutige Wiederfinden,
- die Absicherung gegen Verlust und Verfälschung und
- die Reproduktion der archivierten Informationen.

Was ist ein Verfahren?

Die Verfahrensdokumentation nach GoBS dient dazu, nachweisen zu können, dass die Anforderungen des Handelsgesetzbuchs (HGB), der Abgabenordnung und der GoBS für die Aufbewahrung von Daten und Belegen erfüllt sind. Auch für bestimmte Branchen gibt es, unabhängig von den HGB-Anforderungen, Vorgaben zur Erstellung von Verfahrensdokumentationen, so zum Beispiel für die Pharmaindustrie.

Im IT-Umfeld wird der Begriff Verfahren jedoch eher im Kontext von Prozessen verwendet. Während die *Prozessbeschreibung* den Prozessablauf strukturiert darstellt und die Abläufe beschreibt, in denen Verfahren abgewickelt werden, stellt eine *Verfahrensanleitung* dar, wie ein Prozess operativ auszuführen ist bzw. wie ein Ergebnis erzielt wird. Auch viele Standards und Normen unterscheiden in diesem Sinne zwischen Prozessen und Verfahren.

Sie sollten daher immer darauf achten, in welchem Kontext der Begriff Verfahren verwendet wird. Dies gilt vor allem bei zahlreichen Artikeln, die im Internet zu diesem Thema zu finden sind.

1.2.6 Abgabenordnung (AO)

Die Abgabenordnung (AO) ist das elementare Gesetz des deutschen Steuerrechts. In ihr sind die grundlegenden Regelungen enthalten, wie die Steuern zu erheben sind. Zusätzlich sind in Anlehnung an das HGB auch Anforderungen an das Führen der Bücher sowie weiterer steuerlich relevanter Unterlagen beschrieben.

Im vierten Teil der AO, in dem es um die Durchführung der Besteuerung geht, konkretisieren die Paragrafen 145 bis 147 die Anforderungen an die Buchführung und an die Aufzeichnungen. Danach muss gemäß § 145 Abs. 1 *»die Buchführung so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann«.* (AO) Dies ist einer der Kernsätze der GoB sowie auch die Basis jeder Ordnungsmäßigkeitsprüfung einer Revision.

Ableitbare Anforderungen an die IT-Dokumentation

Insgesamt lässt sich festhalten, dass bereits die grundlegenden Gesetze für die Wirtschaftsunternehmen eine Grundhaltung normiert haben, die in Richtung einer nachvollziehbaren Dokumentation der Geschäftsvorfälle und Geschäftsabläufe abzielt.

Die weiteren Anforderungen entsprechen weitgehend denen aus dem HGB. Es gibt jedoch in der AO eine kleine Ergänzung zum HGB, die für die IT von erheblicher Relevanz ist. In § 147 Abs. 1 sind zunächst gleichlautend zum § 257 Abs. 1 die aufzuhebenden Unterlagen genannt. Zusätzlich werden in der AO aber noch Unterlagen dazugezählt, wenn diese für die Besteuerung von Bedeutung sind. Im Rahmen wirtschaftlicher Aktivitäten sind aber fast alle Geschäftsvorfälle von steuerlicher Relevanz. Somit können die Anforderungen auf weite Bereiche des IT-Betriebs Anwendung finden.

1.2.7 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

Im Zusammenhang mit den GoBS sind auch die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), die seit 2002 Anwendung finden, für die IT-Dokumentation wichtig. (GDPdU)

Die GDPdU enthalten Regeln zur Aufbewahrung digitaler Unterlagen und zur Mitwirkungspflicht der Steuerpflichtigen bei Betriebsprüfungen. Es handelt sich dabei um eine Verwaltungsanweisung des Bundesfinanzministeriums, in der dieses bestimmte Rechtsnormen aus der Abgabenordnung und dem Umsatzsteuergesetz zur digitalen Aufbewahrung von Buchhaltungen, Buchungsbelegen und Rechnungen konkretisiert.

In Kapitel I GDPdU wird auf den § 147 Abs. 6 AO Bezug genommen, *»wonach der Finanzbehörde das Recht eingeräumt ist, die mithilfe eines Datenverarbeitungssystems erstellte Buchführung des Steuerpflichtigen per Datenzugriff zu prüfen. Diese neue Prüfungsmethode tritt neben die Möglichkeit der herkömmlichen Prüfung. Das Recht auf Datenzugriff steht der Finanzbehörde nur im Rahmen steuerlicher Außenprüfungen zu.«* (GDPdU)

Weiter wird in Kapitel I.1 GDPdU ausgeführt, dass sich der digitale Zugriff nur auf steuerlich relevante Daten, also im Wesentlichen auf Daten der Finanz- und Anlagenbuchhaltung bezieht. Im weiteren Verlauf wird jedoch ergänzt, dass, soweit sich auch in anderen Bereichen des Datenverarbeitungssystems steuerlich relevante Daten befinden, diese durch den Steuerpflichtigen nach Maßgabe seiner steuerlichen Aufzeichnungs- und Aufbewahrungspflichten zu qualifizieren und für den Datenzugriff in geeigneter Weise vorzuhalten sind. Diese Ausweitung kann dazu führen, dass ein großer Teil der Geschäftsvorfälle steuerlich relevant sein kann.

Ableitbare Anforderungen an die IT-Dokumentation

Die Verankerung der GoBS in der GDPdU macht deutlich, dass der Umfang der Dokumentationspflichten zunimmt. Sofern Dokumente elektronisch unter Zuhilfenahme einer elektronischen Signatur zu Abrechnungszwecken verarbeitet und dabei gegebenenfalls verschlüsselt werden, muss nach Kapitel II.1 der GDPdU der Originalzustand der übermittelten Dokumente jederzeit überprüfbar sein. Dies setzt neben einer Reihe anderer Tatbestände voraus, dass die Übertragungs-, Archivierungs- und Konvertierungssysteme den Anforderungen der GoBS, insbesondere an die Dokumentation, an das interne Kontrollsystem, an das Sicherungskonzept sowie an die Aufbewahrung, entsprechen.

1.2.8 Sarbanes-Oxley Act (SOX)

Neben nationalen Gesetzen bekommen auch internationale Gesetze eine zunehmende Bedeutung für die IT-Abteilungen und damit auch für die IT-Dokumentation. Wesentliche Gesetze in diesem Zusammenhang stellen der amerikanische Sarbanes-Oxley Act (SOX) sowie die 8. EU-Richtlinie dar, die ihre nationale Umsetzung im Bilanzrechtsmodernisierungsgesetz (BilMoG) findet.

Unter dem Eindruck der Aufsehen erregenden Bilanzskandale in Amerika wurde mit dem Sarbanes-Oxley Act (SOX) 2002 ein US-amerikanisches Bundesgesetz verabschiedet, das die Wiederherstellung des Vertrauens der Öffentlichkeit in die Finanzberichte der Unternehmen durch Anforderungen an die Offenlegung und Genauigkeit von veröffentlichten finanzwirtschaftlichen Informationen zum Ziel hat. Das Gesetz ist auf der Website der U.S. Securities and Exchange Commission erhältlich: [*http://www.sec.gov/about/laws/soa2002.pdf*] (SOX).

Die Gültigkeit dieses Gesetzes erstreckt sich auch auf deutsche Unternehmen, sofern sie an einer amerikanischen Börse gelistet sind oder sich im überwiegenden Besitz einer amerikanischen Muttergesellschaft befinden.

SOX besteht aus elf Hauptsektionen, wobei für die IT die *Section 404* von besonderer Bedeutung ist. In der Section 404, *Management Assessment of Internal Controls*, wird die Notwendigkeit zur Einrichtung eines *Internen Kontrollsystems (IKS)* beschrieben.

Ableitbare Anforderungen an die IT-Dokumentation

Die Brisanz der Section 404 liegt darin, dass die Einhaltung der Sicherheitsregelungen und die Effizienz des internen Kontrollsystems im Einzelnen nachgewiesen werden müssen – und dies jährlich. Im Fokus stehen hier insbesondere die Integrität der Anwendungen und

das Rechte- und Rollenkonzept. In der Prüfungspraxis haben sich unter anderem die folgenden Anforderungen herauskristallisiert:

- Die Systemdokumentation muss aktuell sein und dem tatsächlichen Verfahren entsprechen.
- Die manuellen Prozesse und insbesondere die manuellen Kontrollen müssen dokumentiert werden.
- Die im Unternehmen selbst entwickelten Anwendungen müssen gegen den Zugriff Unbefugter geschützt werden und einer geregelten Datensicherung unterliegen. Die Regelungen sind zu dokumentieren.
- Die Benutzerkonten ausgeschiedener Mitarbeiter oder nicht aktiver Berater müssen gesperrt werden (im Berechtigungskonzept zu dokumentieren).
- Benutzer dürfen nur diejenigen Berechtigungen erhalten, die sie wirklich brauchen. Besonders kritisch sind in diesem Zusammenhang die »Super-User«-Berechtigungen (im Berechtigungskonzept zu dokumentieren).
- Es ist sicherzustellen, dass Mitarbeiter im Entwicklungsbereich über keine Berechtigungen im Produktivbereich verfügen dürfen (im Berechtigungskonzept zu dokumentieren).
- Die Betriebssysteme und Datenbanken, auf denen Anwendungen wie beispielsweise SAP aufsetzen, sind genauso zu schützen wie die Anwendungssysteme selbst (Sicherheitskonzept erforderlich).

1.2.9 Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz (BDSG) ist ausgerichtet auf den Schutz der Privatsphäre und regelt sowohl für öffentliche (unter anderem Kommunen, Ämter und staatliche Unternehmen) als auch für nichtöffentliche Stellen (unter anderem natürliche und juristische Personen und Gesellschaften) den Umgang mit personenbezogenen Daten. Es ist eine Reaktion des Gesetzgebers auf das Volkszählungsurteil von 1983, wonach die bisher vorhandenen Datenschutzgesetze nicht den verfassungsrechtlichen Anforderungen genügten. Nachdem daraufhin bereits einige Bundesländer eigene Landesdatenschutzgesetze verabschiedet hatten, trat das Bundesdatenschutzgesetz 1990 in Kraft. Es liegt nach der Novellierung in 2009 in der Fassung vom 14. 08. 2009 vor.

»Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.« (BDSG)

Das BDSG ist ein Verbotsgesetz, das die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich untersagt. Sie sind nur dann zulässig, wenn dieses oder andere Gesetze es erlaubt oder der Betroffene eingewilligt hat. Die Einwilligung hat in der Regel schriftlich zu erfolgen und hat zur Voraussetzung, dass sie aus freier Entscheidung und in Kenntnis des Zwecks und der Folgen der Verarbeitung gefallen ist. Es ist in sechs Abschnitte unterteilt, wobei im Abschnitt 1 die allgemeinen Bestimmungen enthalten sind. Für den IT-Betrieb wichtig ist auch der Abschnitt 3, in dem die Verarbeitung personenbezogener Daten geregelt ist.

Nach § 3, Abs. 1 sind personenbezogene Daten *»Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.«* (BDSG) Von besonderem Inte-

resse dabei sind Einzelangaben, aus deren Kombination oder Auswertung sich eine Person ableiten, also bestimmen lässt, so wie beispielsweise aus der Telefonnummer in Kombination mit der Adresse. Besonders schutzwürdig sind Daten zur rassischen und ethnischen Herkunft, politische Meinungen sowie religiöse und philosophische Überzeugungen und Angaben zur Gewerkschaftszugehörigkeit, zur Gesundheit und zum Sexualleben.

Nach § 4f Abs. 1 hat jede nichtöffentliche Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt, einen *Datenschutzbeauftragten* zu bestellen, sofern mehr als vier Personen damit beschäftigt sind. Kleinstbetriebe sind also von dieser Vorschrift ausgenommen. Sofern der Betrieb jedoch geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung erhebt, gilt diese Einschränkung nicht mehr. Dem Datenschutzbeauftragten ist nach § 4g Abs. 2 eine Übersicht über die in § 4e beschriebenen Verfahren zur Verfügung zu stellen. Nach Abs. 1 des Paragrafen ist er rechtzeitig, also vor der Einführung, zu unterrichten. Weiter hat er die ordnungsgemäße Verwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen.

Weitergehende Datenschutzregelungen in zusätzlichen Gesetzen

Das wohl bekannteste deutsche Regelwerk zum Datenschutz ist das Bundesdatenschutzgesetz. Es gilt für Bundesbehörden und für die Privatwirtschaft. Daneben haben die deutschen Bundesländer eigene Landesdatenschutzgesetze, die für die jeweiligen Landesbehörden und die Kommunen gelten. Sowohl das Bundesdatenschutzgesetz als auch die Landesdatenschutzgesetze finden nur Anwendung, soweit für den konkreten Sachverhalt kein spezielleres Datenschutzgesetz existiert.

Für Postdienstleister gilt beispielsweise die *Postdienste-Datenschutzverordnung*. Erhebliche Bedeutung haben auch die in den Sozialgesetzen verankerten Vorschriften zum Schutz des Sozialgeheimnisses. Und Internet-Provider müssen bei der Verarbeitung personenbezogener Daten ihrer Kunden die besonderen Datenschutzvorschriften des Telemediengesetzes beachten.

Ableitbare Anforderungen an die IT-Dokumentation

Eine wesentliche Bestimmung des BDSG ist die der Meldepflicht nach § 4d, wonach Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde bzw. dem betrieblichen Datenschutzbeauftragten zu melden sind. Eine Produktivsetzung einer Verarbeitung personenbezogener Daten, etwa eines Kundenmanagementsystems, ist danach nicht zulässig und kann gerichtlich untersagt werden.

Aus dem § 4g Abs. 2 Satz 1 leitet sich das Erfordernis zur Aufstellung eines Verfahrensverzeichnisses ab, in dem alle meldepflichtigen Verfahren zu dokumentieren sind. Dieses Verzeichnis hat die verantwortliche Stelle zu führen und dem Datenschutzbeauftragten zur Verfügung zu stellen. Nähere Erläuterungen zu Verfahrensbeschreibungen finden Sie in *Kapitel 3 in Abschnitt 3.8.9.*

Diese Bestimmungen führen zu hohen Anforderungen an die Dokumentation von IT-Verfahren. Es muss also vor der Implementierung eines Verfahrens, in dem personenbezogene Daten verarbeitet werden sollen, exakt festgelegt und damit dokumentiert sein, welche

Daten von wem und für wen zu welchem Zweck erhoben, verarbeitet und genutzt werden sollen. Vor allem aber genügt es nicht, nur das Verfahren mitzuteilen. Das Unternehmen hat nach *§ 9 des BDSG* technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes – insbesondere die in der Anlage des Gesetzes genannten Anforderungen – zu gewährleisten. Danach sind bei der Verarbeitung von personenbezogenen Daten folgende Kontrollen umzusetzen:

- **Zutritts- und Zugangskontrollen:** Datenschutzrelevante IT-Systeme dürfen nur befugten Personen zugänglich sein und nur von ihnen genutzt werden können. Es ist sicherzustellen, dass nur befugte Personen Zutritt zu Gebäuden, Räumen und IT-Systemen mit personenbezogenen Daten erhalten (Beschreibung des Zutrittskontrollsystems, zum Beispiel Ausweisleser, kontrollierte Schlüsselvergabe etc.)
- **Zugriffskontrollen:** Dies umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsslungsverfahren entsprechend dem Stand der Technik). Dies schließt auch die Überwachung des Lebenszyklus von Datenträgern ein, d. h., ob die Anforderungen an die Speicherung von personenbezogenen Daten bei der Initialisierung, der Aufbewahrung, der Verwendung und der Entsorgung der Datenträger erfüllt werden.
- **Weitergabekontrollen:** Es muss nachvollziehbar sein, an welche Stellen welche Daten weitergegeben wurden bzw. falls noch keine Daten weitergegeben wurden, an welche Stellen eine Weitergabe vorgesehen ist. Übermittelte bzw. transportierte personenbezogene Daten dürfen während der Übermittlung oder des Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsslungsverfahren entsprechend dem Stand der Technik). Bei Online-Zugriffen ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.
- **Eingabekontrollen:** Es muss eindeutig nachvollziehbar sein, von wem welche personenbezogenen Daten eingegeben, geändert oder gelöscht wurden. Werden personenbezogene Daten im Auftrag einer anderen Stelle verarbeitet, so muss gewährleistet sein, dass die Benutzer die Daten nicht anders als beauftragt verarbeiten können (sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens drei Jahre lang durch den Auftragnehmer aufbewahrt).
- **Verfügbarkeitskontrollen:** Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Backup-Konzept, Medium, Aufbewahrungszeit und Aufbewahrungsort für Backup-Kopien.).
- **Trennungskontrollen:** Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. (BDSG)

Für die entsprechende IT-Dokumentation zur Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten hat dies zur Folge, dass sie bereits vor der Implementierung eines neuen Verfahrens vorliegen muss und dem Datenschutzbeauftragten zur Prüfung zu übergeben ist. Dieser beurteilt damit auch die Ordnungsmäßigkeit der IT-Dokumentation im Sinne des Gesetzes.