Kapitel 8

Rechtliche Aspekte der Archivierung

Eine ganze Reihe von Gesetzen, Verordnungen und Vorschriften fordert direkt oder indirekt die Aufbewahrung von Dokumenten zum Nachweis erbrachter Leistungen, erhaltener Aufträge oder Bescheide, von geleisteten Ausgaben, Abgaben und vielem mehr. Dieses Kapitel versucht, in einer auch für Nicht-Juristen verständlichen Sprache, einige dieser gesetzlichen Anforderungen zu erläutern und einen ersten Überblick über die wichtigsten Aspekte zu geben.

Die Autoren haben sich mit dem Thema intensiv auseinander gesetzt, sind aber weder Juristen noch Steuerfachleute. Sie können deshalb **keine Gewährleistung** für die Korrektheit, Vollständigkeit und Aktualität der Aussagen übernehmen!

⇨ *Beachten Sie bitte, dass sich Gesetze und Verordnungen ändern können.*
Zusätzlich können neue Auslegungen und Urteile die Interpretation verschieben.

Buchungs- und andere betriebswirtschaftliche Belege unterliegen bestimmten steuer- und handelsrechtlichen Nachweis- und Aufbewahrungsfristen. Teilweise sind sogar bestimmte Aufbewahrungsformen gefordert. Besondere Aspekte gelten für Urkunden oder urkundenähnliche Dokumente. Die Archivierung wird u. a. durch folgende Gesetze geregelt:

AO = *Abgabenordnung*
HGB = *Handelsgesetzbuch*
ZPO = *Zivilprozessordnung*
StPO = *Strafprozessordnung*
BGB = *Bürgerliches Gesetzbuch*
StGB = *Strafgesetzbuch*
BetrVG = *Betriebsverfassungsgesetz*
IuKDG = *Informations- und Kommunikationsgesetz*

- ❏ **Handels- und Steuerrecht** (HGB, AO)
- ❏ **Zivil- und Strafrecht** (ZPO, BGB, StGB, StPO)
- ❏ **Signaturgesetz**
- ❏ **Datenschutz** (BDSG d. h. Bundesdatenschutzgesetz)
- ❏ **Urheberrecht** (UrhG d. h. Urheberrechtsgesetz)
- ❏ **Betriebsverfassungsgesetz** (bei der Arbeitsplatzgestaltung)

Weitere Nachweis- und Aufbewahrungspflichten können sich implizit aus dem Produkthaftungsgesetz ergeben. Auch branchenspezifische Gesetze und Verordnungen sind zu beachten, so z. B. Vorschriften aus dem Bank- und Versicherungsrecht oder aus dem öffentlichen Haushalts- und Kassenrecht. Basierend auf dem Europarecht kommen Arbeitsschutzgesetze hinzu, in Deutschland etwa in Form der *Bildschirmarbeits-Verordnung* oder Anforderungen aus dem *Betriebsverfassungsgesetz*.

Diese Rechtsgrundlagen sind bisher noch landes- bzw. staatenspezifisch geregelt, auch wenn auf europäischer Ebene eine Harmonisierung angestrebt wird. Die rechtliche Situation in Deutschland weicht in wesentlichen Punkten beispielsweise von jener der Schweiz, Großbritanniens oder der USA ab. Daneben kommen Gesetze und Vorschriften hinzu, welche spezifisch für ein Bundesland sind oder nur für Behörden intern gelten. So kennt Baden-Württemberg z. B. für den öffentlichen Dienst eine verschärfte Arbeitsplatzverordnung, und das Bundesdatenschutzgesetz formuliert für öffentliche Stellen verschärfte Kontrollen und Auflagen.

Die nachfolgende Betrachtung bezieht sich auf die in Deutschland geltenden Verordnungen –, es gibt noch keine international verbindlichen Regelungen – und beschränkt sich weitgehend auf solche Belege, die aus Gründen des Steuerrechts und des Wirtschaftsrechts aufzubewahren sind. Es wird versucht, die rechtlichen Grundlagen möglichst verständlich darzulegen. Hierbei wird weitgehend auf die im Anhang B aufgeführte Literatur zurückgegriffen.*

* *Siehe Seite 698 ff.*

Prinzipiell ist bei allen Arten von Belegen festzuhalten, dass die für sie geltenden Aufbewahrungspflichten nicht durch die Art der Archivierung bestimmt werden. Ist die Schriftform nicht explizit vorgeschrieben, so gelten für die elektronische Archivierung die gleichen Voraussetzungen wie für die in Papierform.

8.1 Handels- und Steuerrecht

Die Aufbewahrungsfrist und -art von Dokumenten und Belegen ist in folgenden Paragraphen des Handelsgesetzbuchs geregelt:

§ 238 HGB (Buchführungspflicht)
§ 239 HGB (Führung der Handelsbücher)
§ 257 HGB (Aufbewahrungsfristen und -anforderungen)
§ 261 HGB (Unterlagen auf Bild-/Datenträgern)

Im Steuerrecht sind u. a. folgende Paragraphen relevant:

§ 140 AO (Buchführungspflicht)
§ 146 AO (Buchführung und Aufzeichnungen)
§ 147 AO (Aufbewahrung von Unterlagen)

§ 14 IV UStG (Prüfbarkeit digitaler Unterlagen, z. B. Rechnungen)
GDPdU (Datenzugriff und Prüfbarkeit digitaler Unterlagen)

UStG = *Umsatzsteuergesetz*

Die Vorschriften im Handels- und Steuerrecht sagen für den überwiegenden Teil der Dokumente wenig aus über das konkrete Speicherungsverfahren oder den dabei zu verwendenden Datenträger. Sie schreiben weder ein bestimmtes Buchführungssystem vor, noch legen sie das Aufzeichnungsverfahren fest. Ausnahmen gelten für *Eröffnungsbilanzen*, *Jahresabschlüsse* und *Konzernabschlüsse*, die zumindest auch als Originale in Papierform aufzubewahren sind.

Eröffnungsbilanzen, Jahresabschlüsse und Konzernabschlüsse müssen immer (auch) in Papierform aufbewahrt werden.

Handels- und Steuerrecht stellen lediglich eine Reihe von Anforderungen an das Verfahren, z. B. die Abrufbarkeit, Reproduzierbarkeit und Wiedergabetreue gespeicherter Informationen und Belege. Es wird eine *ordnungsgemäße, qualifizierte Ablage und Aufbewahrung der Nachweise* verlangt.

Die wesentlichen Anforderungen von HGB und GoB sind

GoB = *Grundsätze ordnungsgemäßer Buchführung*

- ❏ eine richtige und vollständige Erfassung buchführungspflichtiger Geschäftsvorfälle,
- ❏ eine zeitgerechte Erfassung,
- ❏ eine geordnete Darstellung,
- ❏ die Sicherheit der Aufbewahrung über den gesamten vorgeschriebenen Zeitraum.

Hierbei betreffen die ersten beiden Punkte stärker den Bereich der Organisation und des Buchführungssystems und weniger die elektronische Archivierung.

Seit einer Neufassung dieser Vorschriften im Jahre 1977 wird explizit die Speicherung der Belege auf *Datenträgern* für zulässig erklärt* und die Führung von Handelsbüchern auf solchen gestattet

** § 257 Abs. 3 HGB, 147 Abs. 2 AO*

(§ 239 Abs. 4 HGB und § 146 Abs. 2 AO). Die AWV *(**A**rbeits-**g**emeinschaft für **w**irtschaftliche **V**erwaltung e. V.)* erarbeitete inzwischen die GoBS – die ***G**rundsätze **o**rdnungsgemäßer DV-gestützter **B**uchführungs**s**ysteme*. Diese Definition wird in einer Reihe von Vorschriften wieder aufgegriffen.

In den gesetzlichen Vorschriften ist der Begriff *Datenträger* weitgehend unbestimmt gelassen. 1991 äußerte sich das Bundesfinanzministerium dahingehend, dass eine spezielle Genehmigung für eine Speicherung auf Mikrofilm oder optischen Platten **nicht** notwendig ist. Diese Aussage ist mit den entsprechenden Ministerien der Länder abgestimmt.

Eine DMS-Anbieter-Zertifizierung, wie vom VOI vorgeschlagen, ist nicht notwendig und entlastet den Steuerpflichtigen nicht von der Verantwortung für das von ihm (oder für ihn) betriebene System. Eine (Einzel-) Zertifizierung für das konkret aufgesetzte und betriebene Archiv (z.B. durch einen Wirtschaftsprüfer) hingegen kann nützlich sein.

Es obliegt damit dem Steuerprüfer – oder im Fall des Handelsrechts dem Wirtschaftsprüfer –, im Einzelfall zu beurteilen, ob eine *ordnungsgemäße* Ablage mit Hilfe des Archivierungssystems erfolgt.

Eine solche Ablage bzw. das System setzt voraus, dass die notwendigen Unterlagen vorgeführt werden können und zwar:

- ❏ *problemlos* (d.h. mit angemessenem Aufwand)
- ❏ *zeitnah* (d.h. in angemessener Zeit)
- ❏ *in der erforderlichen Reihenfolge* und
- ❏ *jederzeit* über den gesamten Zeitraum der Nachweispflicht

Vergleicht man hier die Möglichkeiten eines DM-Systems mit der konventionellen Papierablage, so wird offensichtlich, dass eine elektronische Ablage zumindest die ersten drei Forderungen besser erfüllt, als dies Papier- oder Mikrofilmablagen zulassen.

Die Forderung nach der jederzeit möglichen Reproduktion im Aufbewahrungszeitraum impliziert, dass bei einem Systemwechsel entweder das alte System betriebsbereit gehalten werden muss – was in der Regel wirtschaftlich unsinnig ist –, oder die Daten für das neue System konvertiert werden und dort wieder zugänglich sein müssen.

Bei der Speicherung auf maschinenlesbaren Datenträgern wird zusätzlich die Möglichkeit gefordert, die Dokumente problemlos ohne technische Hilfsmittel für den Prüfer lesbar zu machen – z. B. durch Ausdrucken (für den Prüfer kostenlos).

Das Verfahren muss zusätzlich eine *bildliche Übereinstimmung* von produzierter Abbildung und ursprünglicher Vorlage bei Buchungsbelegen und empfangenen Handels- oder Geschäftsbriefen sicherstellen (nach § 147 Abs. 2 Nr. 1 der AO). Bei allen anderen Unterlagen (z.B. auch bei ausgehenden Handelsbriefen) reicht eine *inhaltliche Wiedergabe* – wozu aber auch die Reproduktion der eventuell vorgedruckten Geschäftsbedingungen gehört.

Dort, wo eine bildliche Übereinstimmung zwischen Original und Reproduktion verlangt wird, ist die Übereinstimmung* nicht für

** entsprechend § 257 Abs. 3 Nr. 1 HGB, § 147 Abs. 2 Nr. 1 AO*

die Speicherung, sondern erst für die Reproduktion notwendig. Es ist daher z. B. möglich, in Formularen mit Blindfarben zu arbeiten, die beim Scannen ignoriert werden, wenn eindeutig ist, um welche Art von Formular es sich handelt. Zur Reproduktion muss das korrekte Formular dann wieder eingeblendet werden können.

8.1.1 Explizite Forderung nach Originalen

Neben den bereits aufgeführten *Eröffnungsbilanzen, Jahresabschlüssen* und *Konzernabschlüssen*, welche zumindest auch im Papieroriginal aufzubewahren sind, müssen nach dem aktuellen deutschen Umsatzsteuergesetz (§ 14 Abs. 4 UStG) auch vorsteuerrelevante Rechnungen (typisch: Kreditorbelege, bei denen ein Vorsteuerabzug erfolgt) als Original vorgelegt werden. Das elektronische Original muss eine *qualifizierte* Signatur mit Anbieter-Akkreditierung besitzen.*

* *Siehe hierzu Abschnitt 8.1.5.*

Eine Befreiung vom Original ist bei eingescannten Rechnungsbelegen möglich (ohne gesetzliche Verankerung), muss aber im (Kunden-) Einzelfall mit der zuständigen Finanzbehörde abgeklärt werden.** Wir haben von mehreren Archiv-Kunden erfahren, welche dies beantragten und die Genehmigung erhielten.

** *Siehe BMF vom 24.9.1998.*

Nach den GDPdU sind (ab 1. 1. 2002) zusätzlich die *elektronischen Originale* (Original-Dateien) von elektronisch eingehenden steuerrelevanten Belegen aufzubewahren – also insbesondere elektronische Rechnungen. Sind aus technischen Gründen Konvertierungen (z. B. in andere Formate) notwendig, so sind neben den so erzeugten (konvertierten) Dokumenten auch die Originale weiterhin aufzubewahren.

Zur GDPdU siehe Abschnitt 8.1.4.

Zusätzlich aufzubewahrende Dokumente

Die ***G**rundsätze **o**rdnungsgemäßer DV-gestützter **B**uchführungssysteme* (kurz: **GoBS**) fordern auch eine **Verfahrensdokumentation**. Sie sollte im deutschsprachigen Raum vorzugsweise auch in Deutsch vorliegen. Für sie gilt der erweiterte Aufbewahrungszeitraum von 10 Jahren. Sie darf sowohl als Papier als auch in elektronischer (jederzeit reproduzierbarer) Form aufbewahrt werden. Hiermit gewinnt auch die Aufbewahrung von Handbüchern eine eigenständige Bedeutung.

Zum Thema ›Verfahrensdokumentation‹ siehe Kapitel 9.8. Eine Art Checkliste zur Verfahrensdokumentation ist in [Zöller-1] zu finden.

Ist ein Umkopieren von Dokumenten auf neue Datenträger erforderlich – und dies ist bei längeren Aufbewahrungszeiten elektronisch gespeicherter Dokumente und größeren Systemwechseln

kaum zu vermeiden –, so ist darüber in geeigneter Form ein **Protokoll zu führen und dieses aufzubewahren**. Dies setzt eine strukturierte Arbeitsplanung und festgelegte, dokumentierte Arbeitsabläufe voraus.

Ebenso ist die Bedienungsanleitung der bei der Buchführung und der Archivierung eingesetzten Programme über diese Zeit – zusammen mit den Programmdatenträgern – aufzubewahren. Wie weit und wozu dies sinnvoll ist, sei dahingestellt.

8.1.2 Aufbewahrungsfristen

Die Aufbewahrungsfristen sind in § 257 HGB und § 147 AO geregelt. Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen müssen 10 Jahre lang aufbewahrt werden. Dies gilt auch für die System- und Verfahrensdokumentation der für die Buchung und Archivierung eingesetzten Systeme! Die Frist von 10 Jahren* gilt ebenso für empfangene und abgesandte Handelsbriefe sowie für Buchungsbelege (vollständiger: Belege für Buchungen in den nach § 238 Abs. 1 HBG zu führenden Büchern). Für steuerliche Zwecke gelten grundsätzlich die gleichen Fristen, wobei einzelne Steuergesetze eine kürzere Frist vorsehen.**

** Bis Dezember 1998 galt hier eine Frist von 6 Jahren.*

*** Für die kürzeren Fristen ist jedoch die ›Allgemeine Festsetzungsfrist‹ aus Anlage 231 AO, § 169/2 AO zu beachten.*

Von den oben genannten Unterlagen müssen Eröffnungsbilanzen sowie Jahres- und Konzernabschlüsse (zumindest auch) in Originalform auf Papier aufbewahrt werden – für sie ist also die Aufbewahrungsart explizit vorgegeben. Eine Archivierung kann (zusätzlich) trotzdem sinnvoll sein, um schnell und ortsunabhängig darauf zugreifen zu können.

Die Aufbewahrungsfrist beginnt mit dem Ende des Kalenderjahres, in dem die **letzte** Eintragung in das Handelsbuch vorgenommen, das Inventar aufgestellt, die Eröffnungsbilanz oder der Jahresabschluss festgestellt, der Konzernabschluss aufgestellt, der Handelsbrief empfangen oder abgesandt wurde oder der Buchungsbeleg entstanden ist. Damit ergeben sich oft Aufbewahrungsfristen von 7 bzw. 11 Jahren, gemessen ab dem Eingangsdatum.

Eine übersichtliche Darstellung der Aufbewahrungsfristen und -anforderungen gibt [AWV-1] (s. S. 700).

Für eine vereinfachte Handhabung in den Archiv-Systemen bedeutet dies, dass der Beleg, gerechnet vom Erstellungs- oder Archivierungsdatum an, ein oder sogar zwei Jahre über die oben genannten Fristen hinaus zu archivieren ist. Das deutsche Steuerrecht verlängert die Aufbewahrungspflicht automatisch (für die davon betroffenen Belege), sobald eine Prüfung angemeldet oder

ein Verfahren gegen den Steuerpflichtigen eingeleitet ist. Gleiches gilt für noch offene Verfahren.

Die Speicherung darf natürlich auch *offline* (ausgelagert) erfolgen, sofern die Daten für eine Prüfung wieder verfügbar gemacht werden können.

8.1.3 Aufbewahrungsort

Nach § 146 AO müssen Bücher und Aufzeichnungen im G*eltungsbereich des Gesetzes* geführt und aufbewahrt werden. Handelt es sich also um zu archivierende Belege für ein Unternehmen in Deutschland, das dem deutschen Steuerrecht unterliegt, so muss der Ablageort auch Deutschland sein – nicht jedoch notwendigerweise der Ort des Unternehmens.*

§ 148 AO gestattet jedoch – auf Antrag an die zuständige Finanzbehörde – Erleichterungen für die Aufbewahrung. Die Finanzbehörde ist gehalten, die Genehmigung zur Archivierung auch außerhalb von Deutschland zu erteilen (d.h. sie **muss**, wenn keine triftigen Gründe dagegen sprechen), sofern sichergestellt ist, dass ein Finanzprüfer (oder Wirtschaftsprüfer) jederzeit von Deutschland aus auf die Belege zugreifen und sie lokal ausdrucken kann und soweit bei der Speicherung im Ausland die in Deutschland geltenden GoB- bzw. GoBS-Richtlinien eingehalten werden.

Es ist davon auszugehen, dass im Zuge des EU-Rechts eine Aufbewahrung in einem anderen EU-Land auch ohne vorherige Genehmigung zulässig sein wird.

** Eine zentrale Archivierung für mehrere deutsche Töchter oder Standorte ist also ohne Genehmigung zulässig.*

8.1.4 GDPdU – Prüfbarkeit und Datenzugriff

Das Bundesfinanzministerium (der BRD) detaillierte 2001 in den GDPdU* (*Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen*) seine Vorstellungen bzw. Forderungen hinsichtlich der Prüfbarkeit von und insbesondere für den Datenzugriff auf digitale Unterlagen – dies gilt für Außenprüfungen (also eine Prüfung vor Ort beim Steuerpflichtigen oder dessen Steuerberater). Während sich am sachlichen Umfang der (Außen-) Prüfung damit nichts ändert, ist darin explizit die Möglichkeit für den Prüfer vorgesehen, auf die digital (elektronisch) gespeicherten Daten (Belege) zuzugreifen und eine (elektronische) Kopie der Daten zu erhalten – z.B. für eine eigene elektronische Weiterverarbeitung wie Summierung, Saldenbildung usw.

** Schreiben vom 16.07.2001 (Az. IV D 2-S 0316-0136/0) (siehe [[GDPdU]], auf S. 701).*

Damit besteht die (auch für andere Zwecke) sinnvolle Forderung, steuerrelevante Daten aus einem Archiv, DMS oder elektronischen Buchhaltungssystem (Finanz-, Anlagen- und Lohnbuchhaltung) wieder in elektronischer Form exportieren und elektronisch auswerten zu können. Der Prüfer hat dabei die Wahl zwischen drei Zugriffsverfahren:

A) Einen ›Nur-Lesen‹-Zugriff des Prüfers direkt im Datenverarbeitungssystem *(unmittelbarer Zugriff)*: Hierzu muss ihn der Geprüfte soweit notwendig einweisen.
Um eine eventuelle versehentliche Veränderung der Daten durch den Prüfer auszuschließen, muss das System einen Nur-Lesen-Modus unterstützen.*

* *oder man macht zuvor eine vollständige Sicherung*

B) Der Steuerpflichtige (oder ein beauftragter Dritter) erstellt die Auswertung nach den Vorgaben des Prüfers im ›Nur-Lesen‹-Zugriff *(mittelbarer Zugriff)*. Für die Auswertung müssen dem Prüfer dabei die im Buchhaltungssystem vorhandenen Auswertungsmöglichkeiten genügen.

C) Der Prüfer kann verlangen, dass ihm die Daten auf einem maschinenlesbaren Datenträger zur Verfügung gestellt werden *(Datenträgerüberlassung)*. In diesem Fall sind die Daten vom Finanzamt nach dem ergangenen Bescheid zurückzugeben oder zu löschen.

Bei den hier aufgeführten Rechten und Maßnahmen gilt nach der GDPdU explizit der ›Grundsatz der Verhältnismäßigkeit‹.

Die Programme zur Weiterverarbeitung hingegen sind Angelegenheit des Prüfers und nicht des Geprüften. Ebenso ist dies kein Freibrief des Prüfers für einen Datenzugriff auf alle möglichen in den Systemen gespeicherten Daten, sondern beschränkt sich auf *›steuerrelevante Daten‹*, wobei der Begriff natürlich Interpretationsspielräume zulässt.

Daten, welche vor dem 1. 1. 2002 auf nicht maschinell auswertbaren Datenträgern (oder ungeeigneten Formaten) erfasst wurden, sind von dieser Regelung ausgenommen.

8.1.5 Elektronische Abrechnung nach § 14 Abs. 4 UStG

Im Zuge der Steueränderungsgesetze vom Jahr 2001 und in Umsetzung der EU-Richtlinie (77/388/EWG) wurde § 14 Abs. 4 Satz 2 des UStG von 1999 so geändert, dass elektronische (und elektronisch verschickte) Rechnungen eine *qualifizierte elektronische Signatur* mit Anbieter-Akkreditierung (nach SigG 2001)* benötigen.

* *Siehe hierzu Abschnitt 8.4.2.*

Diese Forderung geht dabei für den 2002 (und wohl auch noch 2003) geltenden (wirtschaftlich machbaren) Stand der Technik

(bzw. der dafür verfügbaren Produkte) **unrealistisch** weit, indem dort gefordert wird, dass

A) vor einer weiteren Verarbeitung der elektronischen Abrechnung die qualifizierte elektronische Signatur im Hinblick auf die Integrität der Daten und die Signaturberechtigung geprüft wird und das Ergebnis dokumentiert wird;

B) die Speicherung der elektronischen Abrechnung auf einem Datenträger erfolgt, der Änderungen nicht mehr zulässt. Bei einer temporären Speicherung auf einem änderbaren Datenträger muss das DV-System sicherstellen, dass Änderungen nicht möglich sind;*

C) bei Umwandlung (Konvertierung) der elektronischen Abrechnung in ein unternehmenseigenes Format (sog. Inhouse-Format) beide Versionen archiviert und nach den GoBS mit demselben Index verwaltet werden sowie die konvertierte Version als solche gekennzeichnet wird;

*D) der Signaturprüfschlüssel aufbewahrt wird;***

E) bei Einsatz von Kryptographietechniken die verschlüsselte und die entschlüsselte Abrechnung sowie der Schlüssel zur Entschlüsselung der elektronischen Abrechnung aufbewahrt wird;

F) der Eingang der elektronischen Abrechnung, ihre Archivierung und ggf. Konvertierung sowie die weitere Verarbeitung protokolliert werden;

G) 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;

* *Eigentlich sollte die Signatur den Nachweis der Authentizität erlauben.*

** *Diese Aufgabe übernimmt nach SigG für qualifizierte Zertifikate mit Anbieter-Akkreditierung der Zertifizierungsdiensteanbieter. Er muss deshalb nicht beim Unternehmen erfolgen.*

Während die Punkte B, C, F und G sicher sinnvoll und erfüllbar sind, ist Punkt D erfüllbar oder überflüssig.** Bei Punkt E kann argumentiert werden, dass erst das dechiffrierte Objekt als verarbeitbarer Eingang angesehen werden kann und eine (zusätzliche) Archivierung des Dokuments (der Nachricht, des Datenobjektes), welches nur zur Transportsicherung verschlüsselt wurde, überflüssig ist. Bei Punkt B sollte bereits die zuvor geforderte Signatur den Nachweis der Authentizität erlauben, so dass die Speicherung auf einem ›*Datenträger, der Änderungen nicht zulässt*‹ eigentlich nicht unbedingt notwendig ist.

Zur maschinellen Erstellung von ›qualifizierten Signaturen‹, siehe Seite 393 unten.

Dieser Teil des Schreibens ist mithin in mancherlei Hinsicht unausgegoren und dürfte im Laufe der Jahre 2002/03 korrigiert und detailliert werden.

8.1.6 Archivierung digitaler Unterlagen

Die bereits aufgeführten GDPdU verlangen (seit dem 1. 1. 2002):

1. *Originär digitale Unterlagen nach § 146 Abs. 5 AO sind auf maschinell verwertbaren Datenträgern zu archivieren. Originär digitale Unterlagen sind die in das Datenverarbeitungssystem in elektronischer Form eingehenden und die im Datenverarbeitungssystem erzeugten Daten; ein maschinell verwertbarer Datenträger ist ein maschinell lesbarer und auswertbarer Datenträger. Die originär digitalen Unterlagen dürfen nicht ausschließlich in ausgedruckter Form oder auf Mikrofilm aufbewahrt werden. Somit reicht die Aufzeichnung im COM-Verfahren (Computer-Output-Microfilm) nicht mehr aus. Diese Einschränkung gilt nicht, wenn die vor der Übertragung auf Mikrofilm vorhandenen Daten vorgehalten werden, die eine maschinelle Auswertbarkeit durch das Datenverarbeitungssystem gewährleisten. Nicht ausreichend ist auch die ausschließliche Archivierung in maschinell nicht auswertbaren Formaten (z.B. pdf-Datei).*
   Eine Pflicht zur Archivierung einer Unterlage i. S. des § 147 Abs. 1 AO in maschinell auswertbarer Form (§ 147 Abs. 2 Nr. 2 AO) besteht nicht, wenn diese Unterlage zwar DV-gestützt erstellt wurde, sie aber nicht zur Weiterverarbeitung in einem DV-gestützten Buchführungssystem geeignet ist (z.B. Textdokumente).
2. *Originär in Papierform angefallene Unterlagen, z.B. Eingangsrechnungen, können weiterhin mikroverfilmt werden.*[*]
3. *Kann im Falle eines abweichenden Wirtschaftsjahrs die Archivierung ab 1. Januar 2002 nachweisbar aus technischen Gründen nicht auf einem maschinell auswertbaren Datenträger (§ 147 Abs. 2 Nr. 2 AO) erfolgen, wird dies nicht beanstandet, wenn der Steuerpflichtige bis spätestens zu Beginn des anschließenden abweichenden Wirtschaftsjahrs den Archivierungspflichten gemäß § 147 Abs. 2 Nr. 2 AO nachkommt.*

Man beachte hier die Forderung nach ›maschinell auswertbaren Formaten‹. Diese Forderung kann (logisch und wirtschaftlich begründbar) nur für die Kernbuchhaltungsdaten (z.B. Kontendaten) und nicht für alle Belege gelten (z.B. nicht für die Belege ausgedruckt verschickter Rechnungen und Bestätigungen).

** Anmerkung des Autors: Dies müsste sinngemäß für eine Archivierung als eingescanntes Image auf optischen Platten gelten.*

8.1.7 Nachweis der Datensicherheit (nach Gob/GoBS)

Beim Einsatz solcher Systeme ist nachzuweisen, dass alles mögliche (besser: *sinnvolle und wirtschaftlich vertretbare*) getan wurde, um die Vollständigkeit und Korrektheit zu gewährleisten und die Daten vor unzulässigen Veränderungen zu schützen. Dies fordert unter anderem der so genannte *Radierparagraph* (§ 239 Abs. 3 HGB). Der Manipu-

lationsschutz impliziert auch, dass zur Archivierung aufbewahrungspflichtiger Dokumente WORM- oder CD-/DVD-Technologie (d.h. *nur einmalbeschreibbare Medien*) eingesetzt wird, da sie eine (wirtschaftlich vertretbare) höhere Sicherheit vor Löschungen und Verfälschungen bietet. Bei Einsatz von elektronischen Signaturen und Verwendung zuverlässiger Zeitstempel ist faktisch der Nachweis auch auf anderen (elektronischen) Datenträgern möglich und sollte als ausreichend anerkannt werden.

Um der obigen Forderung nachzukommen, darf das Archivierungsverfahren keine Möglichkeit bieten, erfasste Belege zu manipulieren – beispielsweise mittels eines Image-Editors. In Unternehmen, in denen z.B. zur Archivierung technischer Dokumente solche Werkzeuge benötigt werden, müssen deshalb die Belegerfassungs- und Buchungsarbeitsplätze (bzw. die dazu verwendeten Softwaresysteme) getrennt von jenen betrieben werden, die eine Dokumentenveränderung erlauben. Es empfiehlt sich auch eine Speicherung auf getrennten Datenträgern!

Da eine absolute technische Sicherheit gegen Manipulationen mit akzeptablem wirtschaftlichen Aufwand nicht gewährleistet werden kann, ist das Restrisiko durch explizite Anweisungen an das Bedienungspersonal zu minimieren. Hierzu dient die **Verfahrensdokumentation*** sowie **schriftliche und mündliche Arbeitsanweisungen**. Diese sind eventuell durch entsprechende **Organisationsanweisungen** zu ergänzen.

Die Aspekte der Langzeitarchivierung elektronisch signierter Dokumente diskutieren Roßnagel et al. in [Roßnagel-3] (s. S. 701) ausführlich und verständlich, eine vollständige Lösung liefern aber auch sie nicht

** Siehe hierzu Kapitel 9.8.*

8.1.8 Weitere Sicherheitsmaßnahmen

Darüber hinaus muss (mit wirtschaftlich zu vertretendem Aufwand) sichergestellt sein, dass kein Unbefugter Zugang zum System bzw. zu dessen Daten hat. Dies ist in der Regel eher eine organisatorische Frage als eine Frage der verwendeten Hard- und Softwaresysteme – hier müssen zumindest die inzwischen auch auf PC-Systemen üblichen Zugangskontrollen über Login-Name und Passwort einsetzt werden. Bei SAP-R/2- oder R/3-Systemen wird dies z.B. zusätzlich durch die Anwendungssoftware erzwungen. Die meisten DM-Systeme (als eigenständige Anwendungen) erfordern ebenso eine explizite Benutzeranmeldung.

Ein Duplizieren der archivierten Daten ist für Belege aus der normalen Buchführung gesetzlich nicht erforderlich und bei einem Papierarchiv auch nicht üblich. **Trotzdem sollte dies erfolgen**, weil das Unternehmen die Belegdaten als gesetzlich geforderten Nachweis und zur Klärung interner und externer Rückfragen benötigt.

Der Ausfall der Rechnertechnik bzw. einzelner Datenträger ist auch deutlich wahrscheinlicher als ein Brand im Papierarchiv! Wird dupliziert, so sollte die Kopie sicher und nicht im gleichen Gebäude lagern. Bis dies geschehen ist, sollte das Papieroriginal aufbewahrt werden. Bei einigen anderen Dokumenten/Daten wird eine zusätzliche Datensicherung – oder, wie es in dem Entwurf des Registerverfahren-Beschleunigungsgesetzes von 1993 lautet: *Vorkehrungen gegen einen Datenverlust* – explizit gefordert. Dies gilt z.B. für öffentliche Register, Grundbücher, Handelsregister oder Vereinsregister. Für diese Daten gelten somit erhöhte Sicherungsanforderungen.

8.2 Unterrichtung und Mitsprache des Betriebsrats

Die Einführung von DM-Systemen ändert in aller Regel Arbeitsabläufe und Arbeitsbedingungen. Daher hat nach dem deutschen Arbeitsrecht* der Arbeitgeber den Betriebsrat über die Einführung zu informieren – und zwar rechtzeitig und umfassend. Der Betriebsrat sollte hier bereits in die Planungsphase mit einbezogen und über alle voraussichtlichen Auswirkungen auf die Arbeitnehmer informiert werden.

* *nach § 90 Abs. 1 Nr. 2 bis Nr. 4 Betriebsverfassungsgesetz*

Nach Geis gilt hier:**

> *»Die Beratungen zwischen Arbeitgeber und Betriebsrat müssen so rechtzeitig erfolgen, dass berechtigte Vorstellungen des Betriebsrats bei der Planung berücksichtigt werden können. Aus dem Beratungscharakter dieser Gespräche ergibt sich, dass Vorschläge des Betriebsrats mit dem ernsten Willen zur Verständigung zu erörtern sind.«*

** *Siehe [Geis-2], Seite 701.*

Bei der Planung ist zu berücksichtigen, dass sich durch die Einführung solcher Systeme Änderungen in den Arbeits-, Leistungs- und Qualitätsanforderungen ergeben können, die eine veränderte betriebliche Lohn- und Gehaltsstruktur erfordern. Auch hierbei hat der Betriebsrat ein Mitspracherecht.

Bei der prinzipiellen Entscheidung über die Einführung eines DM-Systems besteht kein Mitbestimmungsrecht des Betriebsrats, da die menschengerechte Gestaltung der Arbeit damit nicht in Frage gestellt wird.

Bei allen Bildschirmarbeitsplätzen ist die seit 1996 gültige Bildschirmarbeits-Verordnung zu beachten. Sie wird im Abschnitt 8.7 genauer beschrieben.

8.3 Zivilprozessrecht

Wesentlich problematischer als nach dem Steuer- und Handelsrecht war bis 2001 die elektronische Archivierung von Dokumenten für einen Rechtsstreit nach der *Zivilprozessordnung* (ZPO). Hier galt bisher **nur** die Original-Urkunde als stichhaltiges Beweismittel. Alle anderen Verfahren – seien es Abschriften, Kopien, Mikrofilme und Images auf WORMs – hatten einen deutlich geringeren Beweiswert und unterlagen der *freien richterlichen Beweiswürdigung*, da sie als *Augenscheinobjekte* gemäß § 371 Zivilprozessordnung betrachtet werden. D.h. es blieb dem jeweiligen Richter in jedem einzelnen Fall überlassen, die Glaubwürdigkeit dieser Kopie zu bewerten. In diesem Sinne waren (nach deutschem Recht bis 2001) weder Mikrofilm noch WORM dazu geeignet, wichtige Verträge und andere Urkunden als (einzigen) Nachweis in zivilrechtlichem Sinne zu speichern. Trotzdem konnte eine solche Speicherung sinnvoll sein, wenn die Vorteile der elektronischen Ablage bei der Bearbeitung (Suche, Darstellung, Interpretation, Vergleich usw.) genutzt werden konnten – solange zusätzlich die Originale aufbewahrt, diese zu keiner gerichtlichen Auseinandersetzung mehr benötigt oder das Prozessrisiko als gering angesehen werden konnte.

Eine Urkunde nach §§ 415 – 444 der ZPO ist ›eine vom Aussteller unterzeichnete Gedankenäußerung, die schriftlich verkörpert ist‹ – also ein Gegenstand mit einer Originalunterschrift.

Zusätzlich kann zwischen Vertragspartnern die Gültigkeit elektronischer Dokumente durch spezielle Vereinbarungen festgelegt werden. Der Einsatz von EDI-Nachrichten im Geschäftsverkehr ist ein Beispiel dafür. Diese Vereinbarungen gelten aber nur zwischen den Parteien.

SigG 2001 liefert neue Bewertung

Mit dem Signaturgesetz (SigG 2001), ergänzt durch das Formanpassungsgesetz von 2001, ergab sich hier für elektronisch signierte Dokumente eine wesentliche Änderung. Nun kann das elektronisch signierte Dokument (entsprechend dem damit eingeführten § 126a des BGB) ebenfalls wie ein händisch signiertes Dokument die Schriftform bei Vorliegen bestimmter Voraussetzungen erfüllen (wo nicht explizit ausgeschlossen). Dies setzt voraus, dass eine angemessene Sicherheitsstufe nach dem SigG für die elektronische Signatur verwendet wird. Hier ist die *qualifizierte* (oder sogar *qualifizierte akkreditierte*) *Signatur* nach SigG 2001 einzusetzen, da alle niedrigeren Stufen für einen Nachweis im Rechtsstreit schwächer oder sogar vollständig ungeeignet sind. Dies gilt deshalb, weil der Gesetzgeber bei Vorlage einer mindestens qualifizierten Signatur eine Beweiserleichterung in § 292a ZPO formuliert hat. Liegen die Voraussetzun-

Das Prinzip der elektronischen Signatur ist im Kapitel 7.13 erläutert, das deutsche Signaturgesetz im Abschnitt 8.4.

gen einer solchen Signatur vor, so gilt der Anschein, dass das Dokument auch echt, d.h. vom Signaturersteller erstellt und auch nicht verändert worden ist. Dort wo die *gesetzliche Schriftform* gefordert wird, kann **nur** die *qualifizierte Signatur* eingesetzt werden.*

* und natürlich die mit Anbieter-Akkreditierung (siehe hierzu Punkt 3 und 4 auf Seite 392).

Eine solche *elektronische Signatur* kann sicherstellen, dass das Dokument wirklich vom angegebenen Urheber (bzw. Signierenden) stammt und seither nicht verändert wurde. Das Verfahren berechnet vom elektronischen Dokument eine komplexe Quersumme (Hashwert) und legt diese chiffriert im bzw. zum Dokument ab. Der mit dem privaten Schlüssel des Signierenden chiffrierte Hashwert bildet zusammen mit Angaben zum Verfahren die elektronische Signatur. Jede Manipulation am Dokument lässt sich hierbei durch einen Vergleich mit dem Hashwert erkennen.

Zur Technik von elektronischen Signaturen siehe Kapitel 7.13.

Enthält die Unterschrift auch einen Zeitstempel, so lässt sich damit zudem nachweisen, wann das Dokument erstellt bzw. *eingepackt* wurde. Wesentlich bei einem solchen Verfahren ist, dass der elektronische Unterschriftsschlüssel bei einer *vertrauenswürdigen Stelle* (CA = ***C**ertification **A**uthorities*) hinterlegt wird, so dass er für eine spätere Überprüfung abgerufen werden kann. Solche CAs und die benötigte PKI existieren seit 1999.

Der früher häufig verwendete Begriff ›digitale Signatur‹ ist inzwischen (so auch im Signaturgesetz) durch ›elektronische Signatur‹ abgelöst.

Bei einem Vertrag im klassischen Sinn müssen dabei beide Parteien ein gleichlautendes Dokument unter Hinzufügung ihres Namens elektronisch unterzeichnen.

Der rechtlich zulässige Einsatzbereich elektronisch signierter Dokumente wächst seit dem Jahr 1997 langsam und seit 2001 deutlich. Ein starker Impuls geht von den verschiedenen nationalen Programmen zum Thema *eGovernment* aus. Hierfür muss jedoch eine nennenswerte Ausstattung des Marktes (der Einwohner) mit digitalen Zertifikaten und anderen PKI-Komponenten ausreichender Qualität erreicht werden. Da der Staat dies aus organisatorischen und Kostengründen kaum erbringen wird, müssen hier voraussichtlich andere Institutionen einspringen. Die großen deutschen Banken und Kreditkartengesellschaften planen dies für 2002/03. Sie haben dabei gewisse eigene Vorteile – man denke hier an sicheres Internet-Banking und eine sichere Bezahlung über Internet.

Seit 2001 bieten einige DM-Systeme – der hohen Kosten wegen zumeist optional – PKI-Komponenten für Signaturen und Zeitstempel. Sollen diese den hohen Anforderungen des deutschen Signaturgesetzes (in den Klassen ›*qualifizierte Signatur*‹ oder ›*akkreditierte, qualifizierte Signatur*‹) entsprechen – wie es z.B. die GDPdU für signierte elektronische Rechnungen fordert –, so werden in aller Regel zusätzliche zertifizierte Komponenten von speziellen Anbietern benötigt.

8.4 SigG – das Signaturgesetz

Bis 1998 hatten auf Mikrofilm oder optischen Datenträgern gespeicherte Dokumente im Fall eines Rechtsstreits einen wesentlich geringeren Beweiswert als handschriftlich unterzeichnete Papierdokumente.

Wir gehen hier sehr ausführlich auf das deutsche Signaturgesetz ein, da es große Bedeutung für elektronische Dokumente hat und in allen EU-Ländern sehr ähnliche Gesetze in Kraft sind.

Das deutsche Recht kannte zwei Arten von Schriftform: Die *gesetzliche Schriftform* und die *gewillkürte Schriftform*. Die *gesetzliche Schriftform* wird dort eingesetzt, wo der Gesetzgeber eine (Papier-) *Urkunde* als Dokumentation eines Vorgangs vorschreibt. Eine Urkunde ist nach der Rechtsvorstellung eine gegenständliche Darstellung, welche mit einer *eigenhändigen Namensunterschrift* (oder einem notariell beglaubigten Handzeichen) versehen ist. Dabei wird angenommen, dass der Unterschreibende den Inhalt des Dokuments zuvor sorgfältig und vollständig gelesen hat und sich über die rechtlichen und wirtschaftlichen Konsequenzen der Unterschrift im klaren ist. Das deutsche Recht forderte bis 2001 an etwa 3 200 Stellen explizit die *gesetzliche Schriftform* (§ 126 BGB). Für Bereiche, bei denen die gesetzliche Schriftform gefordert ist, dürfen nun dort elektronisch signierte Dokumente (mit *qualifizierter Signatur*) eingesetzt werden, wo dies nicht explizit ausgeschlossen wird.

Die *gewillkürte Schriftform* (§ 127 BGB) liegt dann vor, wenn die Schriftform von den Vertragsparteien vereinbart wurde und nicht gesetzlich vorgeschrieben ist. Dies gilt z. B. für den überwiegenden Teil der geschäftlichen Kommunikation wie etwa Bestellung, Auftragsbestätigung, Reklamation, Rechnungsstellung und Ähnliches. Hier bleibt es den beteiligten Parteien überlassen, die akzeptierte Kommunikationsform festzulegen. Jedoch auch hier war bis zur Wirksamkeit des (2001) novellierten Signaturgesetzes das elektronische Dokument gegenüber dem unterschriebenen Papierdokument als Beweis vor Gericht benachteiligt.

Diese Rechtslage erwies sich zunehmend als Hemmnis im Geschäfts- und Rechtsverkehr und schränkte die Funktion elektronischer Dokumente in Situationen ein, wo diese als Nachweis von Vorgängen wirtschaftlich eingesetzt werden könnten. Erst das novelliert deutsche Signaturgesetz und das Formanpassungsgesetz, beide von 2001 brachten Besserung – stimuliert durch eine EU-Richtlinie (1999/93/EG).

Mit dem *Formanpassungsgesetz* von 2001* wurde die Beschränkung der gesetzlichen Schriftform auf die Papierform für die meisten der bis dahin geltenden 3 200 Stellen aufgehoben** und § 126 b BGB neu eingeführt. Zusätzlich wird nun der Begriff der *elektronischen Form* mit aufgenommen – einerseits um sie als eine

* *Siehe [[Forman]], S. 702.*

** *sofern hierfür eine qualifizierte elektronische Signatur eingesetzt wird (siehe Punkt 3 auf S. 392).*

Variante der *Schriftform* zuzulassen (für *gesetzliche Schriftform* ist eine *qualifizierte elektronische Signatur* zu verwenden) und um sie andererseits für bestimmte Anwendungen explizit auszuschließen. Zu den Ausschlüssen zählen z. B. Kündigungen von Arbeitsverträgen, Zeugnisse, Bürgschaftserklärungen, Schuldversprechend und Schuldanerkennungen.

Das Signaturgesetz als Teil des IuKDG

Die erste Version des so genannten *Signaturgesetzes* (kurz **SigG**)* war Teil (d. h. Artikel 3) des IuKDG – des *›Gesetz des Bundes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste‹.*[*] Das Gesetz trat zwar bereits im August 1997 in Kraft, Auswirkungen konnte es jedoch erst mit der Schaffung der darin geforderten *Public-Key-Infrastruktur* (PKI) und dem konkreten Angebot der dafür notwendigen Komponenten und Dienstleistungen haben. Da die erste Version des Gesetzes jedoch in sehr wenigen Bereichen anwendbar war, brachte erste die Novellierung von 2001 eine brauchbare Ausgangsbasis. Die nachfolgende Betrachtung bezieht sich deshalb auf das neue (selbstständige) Signaturgesetz (SigG 2001).

* *Siehe [[SigG]], S. 702.*

Das IuKDG ist auch als ›Multimediagesetz‹ bekannt (siehe [Kampff-3], S. 701).

Das SigG und die ergänzende Signaturverordnung (SigV) definieren den Anwendungsbereich, die technischen und organisatorischen Anforderungen an die elektronische Signatur sowie die für sie notwendige PK-Infrastruktur (PKI). Die *Certification Authority* (CA), – im SigG als *Zertifizierungsdiensteanbieter* bezeichnet – ist in dieser PKI eine wesentliche Komponente. Sie gibt die für die elektronischen Signaturen erforderlichen Signaturzertifikate aus. Dabei wird die Realisierung der CA-Funktion im privatwirtschaftlichen Bereich gesehen. Die Funktion staatlicher Stellen beschränkt sich auf die Lizenzierung und Kontrolle solcher CAs (nach § 66 des Telekommunikationsgesetzes (TKG)** durch die *Regulierungsbehörde der Telekommunikation und Post,* kurz RegTP) sowie auf die Schaffung gesetzlicher und wirtschaftlicher Rahmenbedingungen.

** *Siehe [[TKG]] (s. S. 702).*

Die RegTP ist die Anfang 1998 geschaffene Nachfolgerin des Bundespostministeriums.

Der Anwendungsbereich des neuen Signaturgesetzes

Das Signaturgesetz hat das Ziel, technisch-organisatorische Rahmenbedingungen für elektronische Signaturen zu schaffen. Regelungsadressat sind in erster Linie die *Zertifizierungsdiensteanbieter* (Trust-Center). Erfüllt ein Zertifizierungsdiensteanbieter die im Gesetz genannten Anforderungen, so kann er *qualifizierte Signaturen* anbieten. Lässt er die Erfüllung dieser Anforderungen prüfen und werden sie bestätigt, so erhält er ein Prüfsiegel und gilt als *akkreditierter*

Zertifizierungsdiensteanbieter. Dies ist deshalb interessant, da er somit *qualifizierte* bzw. *akkreditierte Signaturen* herausgeben kann und der Inhaber einer solchen Signatur, wie oben schon beschrieben, nicht nur mit dieser Signatur die Schriftform – soweit nicht ausgeschlossen – erfüllen, sondern auch bei der Verwendung dieser Signatur die Beweiserleichterung des Anscheinsbeweises nach § 292a ZPO geltend machen kann.

8.4.1 Wesentliche Punkte des SigG

Der Anwendungsbereich des SigG sowie die Anforderungen an eine SigG-konforme Signatur sowie die dazu notwendige PKI beruhen auf

- dem Signaturgesetz (siehe [[SigG]]) in der Fassung vom 16. Mai 2001 (BGBl. 2001, Teil I Nr. 22 Seite 876 ff),
- der Signaturverordnung (kurz **SigV**, siehe [[SigG]]) in der Fassung vom 16. November 2001.*

BGBl = Bundesgesetzblatt

** Siehe [[SigG]] (s. S. 702).*

Das Signaturgesetz regelt ausschließlich die elektronische (digitale) Signatur von elektronischen Dokumenten und schränkt seinen Anwendungsbereich auf *Zertifikate für natürliche Personen* ein.** Die *elektronische Signatur* wird dabei als Ersatz der eigenhändigen Unterschrift auf Papierdokumenten (in Anwendung auf elektronischen Dokumenten) gewertet. Dabei muss die Signaturkomponente des Anwenders einige wesentliche Funktionen der eigenhändigen Unterschrift nachempfinden. So muss sie z. B. eine Warnfunktion vor die Signatur setzen und darf nicht automatisch signieren (zumindest nicht in einer offenen Umgebung, wie sie z. B. an einem Arbeitsplatz-PC gegeben ist). Sie muss einen expliziten Hinweis auf die Signatur geben und die explizite Anzeige des zu signierenden Inhalts vor der Signatur gewährleisten (bei automatisierten Signaturen, welche in einem ausreichend gesicherten System erfolgen, kann dies entfallen).

*** Die sichere Identifikation eines Teilnehmers bei einer elektronischen Kommunikation wird außerhalb des signierten Dokuments ebensowenig behandelt wie der Austausch verschlüsselter Informationen.*

Statt des realen Namens des Zertifikatinhabers darf im Zertifikat (und in der Signatur) auch ein Pseudonym verwendet werden. Der wirkliche Name muss der ausstellenden CA jedoch bekannt sein und muss auch Ermittlungsbehörden offengelegt werden – nicht jedoch einem eventuell durch Missbrauch geschädigten Teilnehmer einer elektronischen Kommunikation. Entsprechend sollte man prüfen, in welchen Fällen man digital signierte Dokumente akzeptiert, bei denen statt des Namens des Unterzeichners nur ein Pseudonym vorhanden ist.

Automatisierte Signaturen (z. B. bei ausgehenden Rechnungen) sind prinzipiell möglich. Hier muss jedoch durch technische und

organisatorische Maßnahmen sichergestellt werden, dass dem Signaturprozess keine Dokumente unberechtigt untergeschoben werden können.

8.4.2 Signaturstufen

Im § 2 des SigG sind vier Signaturstufen bzw. -qualifikationen definiert, die sich hinsichtlich der dafür notwendigen organisatorischen und technischen Prozesse und Komponenten unterscheiden:

Die ›einfache elektronische Signatur‹ bietet technisch (als Signatur) praktisch keinen Beweiswert und ist deshalb kaum einsetzbar.

1. **Einfache elektronische Signatur**
   Diese unterste Stufe verzichtet vollständig auf eine Public-Key-Infrastruktur und damit auf einen nachprüfbaren öffentlichen Schlüssel des Unterzeichners. Diese Stufe hat nichts mit elektronischen Signaturen im kryptografischen Sinn zu tun, sondern dient nur zur sprachlichen Trennung von den folgenden Kategorien. Das Einbinden einer eingescannten manuellen Unterschrift als Bild, wie bei Fax vielfach üblich, stellt z. B. schon eine *einfache elektronische Signatur* dar.

Die ›fortgeschrittene elektronische Signatur‹ ist die unterste Stufe mit einem Beweiswert. Auch hier sollten Zertifikate mit entsprechender Inhaberprüfung einer Public-CA eingesetzt werden!

2. **Fortgeschrittene elektronische Signatur**
   Diese Variante ermöglicht die Identifizierung des Inhabers eines öffentlichen Schlüssels und erfordert daher ein Trust-Center (eine CA) zur Ausgabe und Überprüfung eingesetzten Zertifikate. Die Schlüssel dürfen hier z. B. per Software direkt im Rechner generiert werden; auch die Signatur darf hier im Rechner (statt in einer SmartCard) berechnet werden. Diese Stufe lässt sich durch Programme wie z. B. PGP oder die mit Windows 2000 oder XP (Server) mitgelieferten PKI-Werkzeugen erreichen.

Die ›qualifizierte elektronische Signatur‹ ist die richtige Wahl für Verträge, für B2B- und B2C-Transaktionen und für einen hohen Beweiswert.

3. **Qualifizierte elektronische Signatur**
   Diese Stufe baut auf der fortgeschrittenen Signatur auf, erfordert aber zusätzlich eine sichere Signaturerstellungseinheit. Nach dem heutigen Stand der Technik bedeutet dies, dass der private Schlüssel auf einer Smartcard (Chipkarte) erstellt und gespeichert und der Zugriff darauf durch eine PIN oder biometrische Merkmale geschützt sein muss. Der Signaturvorgang muss ebenfalls auf der SmartCard erfolgen und nicht durch die wesentlich anfälligere Software auf dem PC. Die SmartCard und der zugehörige Kartenleser benötigen eine spezielle Zulassung (Zertifizierung). Diese Eigenschaften müssen von den technischen Komponenten auch gewährleistet werden, das heißt, der Schlüssel darf die Karte nie verlassen. Die CA muss

vor der Ausgabe eines Zertifikats die Identität des Antragstellers etwa anhand des Personalausweises überprüfen und ausgestellte Zertifikate öffentlich anbieten, damit jedermann die damit erstellten Signaturen überprüfen kann. Qualifizierte elektronische Signaturen erfordern also den Einsatz einer vollständigen Public-Key-Infrastruktur (PKI).
Diensteanbieter, die eine CA für diese Stufe betreiben wollen, müssen diese bei der RegTP anmelden, unterliegen jedoch keiner weitergehenden obligatorischen Prüfung durch staatliche Stellen. Insofern handelt es sich hier sozusagen um ›*behauptete Sicherheit*‹, die allerdings durch die Haftung des Anbieters bei Mängeln im Zertifizierungsablauf gestärkt wird. Fälscht jemand zum Beispiel eine elektronische Signatur, indem er sich ein Zertifikat unter falschem Namen erschwindelt, so kann der Geschädigte die CA haftbar machen, falls diese das Zertifikat ohne Überprüfung der Identität ausgestellt hat. Der Betreiber der CA muss daher laut Gesetz Deckungsvorsorge treffen.

4. **Qualifizierte elektronische Signatur mit Anbieter-Akkreditierung**
   Die höchste Stufe der Signatur behält das hohe Sicherheitsniveau des alten SigG von 1997 bei, ohne jedoch wie dieses mit einer Genehmigungspflicht für die CA zu arbeiten. Diese Stufe basiert auf der qualifizierten Signatur, enthält aber zusätzlich eine freiwillige Akkreditierung des Diensteanbieters. Der Betreiber der CA muss für die Akkreditierung in einer aufwändigen Prüfung nachweisen, dass er die nötigen Sicherheitsstandards in technischer und organisatorischer Hinsicht einhält. Bei den *qualifizierten Signaturen mit Akkreditierung* handelt es sich also gewissermaßen um nachgewiesene Sicherheit (Sicherheit mit Prüfsiegel). Für die Akkreditierung ist die RegTP zuständig, deren Prüfung als Qualitätsmerkmal fungiert.

In gesicherten Umgebungen – z. B. einem Rechenzentrum mit Zugangskontrolle – können auch *qualifizierte* elektronische Signaturen automatisiert erstellt werden,* wie es z. B. für die Signatur von ausgehenden Rechnungen und anderen Belegen bei einer automatisierten IT-Verarbeitung notwendig ist. Es ist dann aber technisch und organisatorisch sicherzustellen, dass kein Unbefugter Zugang und Zugriff zu dem System erhält und somit keine falschen Dokumente signiert werden. Dies ist **nicht** im SigG oder in der SigV verankert, aber nach der Meinung mehrerer Experten zulässig und für eine automatisierte Verarbeitung unabdingbar.

Eine detaillierte rechtliche Würdigung der Signaturstufen ist in [Roßnagel-2] (s. S. 701) zu finden, eine ausführlich und verständliche Ausführung zur Langzeitarchivierung von elektronischen Signaturen erfolgt in [Roßnagel-3] (s. S. 701).

Die ›qualifizierte, Signatur mit Anbieter Akkreditierung‹ wird für wichtige Verträge empfohlen und in der GDPdU auch für elektronische Rechnungen verlangt.

Auf der Web-Seite der RegTP finden Sie neben weiteren Informationen auch Listen mit bereits akkreditierten Anbietern: www.regtp.de.

** D. h., ohne dass eine Person jeder einzelnen Signatur explizit zustimmt und ohne vorherige Anzeige.*

Die Kosten für eine solche Einheit dürfte (inkl. Projekt) bei etwa 150.000 Euro liegen.

Das Angebot von Systemen (Komponenten) für die automatisierte Erstellung von qualifizierten Signaturen ist bisher ausgesprochen gering (Stand: Anfang 2002) und die Komponenten sind teuer. Hinzu kommt in der Regel ein deutlicher Projekt- und eventuell zusätzlich ein Zertifizierungsaufwand.

8.4.3 Technik-Komponenten des SigG

Signaturverfahren

Als Basistechnik für elektronische Signaturen ist der Einsatz eines asymmetrischen Schlüsselpaars (bestehend aus einem *privaten* und einem *öffentlichen* Schlüssel) für Public-Key-Verfahren vorgesehen. Das Gesetz selbst macht keine Aussagen über die dabei einzusetzenden mathematischen Algorithmen. Erst die Signaturverordnung konkretisiert dies und überlässt die endgültige Festlegung der zulässigen Verfahren und deren Parameter der Detaillierung des BSI, welche im Maßnahmenkatalog erfolgt (für die *qualifizierte* und *qualifizierte, akkreditierte Signatur*). Dies ermöglicht, der fortschreitenden Entwicklung Rechnung zu tragen, ohne das Gesetz ändern zu müssen. Die Signaturverordnung ist schneller änderbar. Es ist deshalb davon auszugehen, dass ein Spektrum von Verfahren möglich sein wird und sich auch weiterentwickelt.

Es ist davon auszugehen, dass der Markt selbst für eine gewisse Bereinigung der Verfahrensvielfalt sorgen wird.

Der Inhalt eines Zertifikats

Das Signaturgesetz sieht mindestens folgende Angaben in einem Zertifikat vor (nach § 7 SigG):

- Den Namen des Inhabers des Signaturschlüssels.
  Dieser muss im Namensraum der CA eindeutig sein.* Statt des Namens darf auch ein Pseudonym verwendet werden.**
- Den zugeordneten öffentlichen Signaturschlüssel
- Die Angabe des für die Erstellung des Zertifikats eingesetzten Signaturverfahrens (Bezeichnung des Signaturalgorithmus) und des verwendeten Hash-Verfahrens
- Die laufende (CA-spezifische) Nummer des Zertifikats
- Beginn und Ende der Gültigkeit des Zertifikats
- Den Namen der ausstellenden CA
- Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist

* *D. h. er darf nur einmal vorkommen*

** *Daneben kann ein Stellvertreter des Inhabers angegeben werden. Dieser ist (sofern bei der Antragstellung benannt) berechtigt, an Stelle des Inhabers das Zertifikat sperren zu lassen.*

- ❏ Angaben, ob es sich um ein qualifiziertes Zertifikat handelt
- ❏ (optional) Attribute des Signaturschlüsselinhabers (diese können auch in einem separaten Attribut-Zertifikat aufgenommen werden)

Weitere Angaben sind zulässig, setzen aber das Einverständnis des Inhabers voraus.

Einige der aufgeführten Angaben sind nicht im Signaturgesetz selbst zu finden, sondern ergeben sich aus der Signaturverordnung.

Die Zertifizierungsstelle (CA)

Eine SigG-konforme Signatur der Stufe *qualifiziert* und höher setzt eine Public-Key-Infrastruktur voraus. Für deren Aufbau und Betrieb ist ein *Zertifizierungsdiensteanbieter* verantwortlich. Er wird hier als CA oder PCA (***Public (öffentliche)* CA**) bezeichnet, um Verwechselungen mit den Stellen zu vermeiden, die ihrerseits diese Instanzen auf Einhalten der gesetzlichen Vorgaben überprüfen und von der RegTP dazu ermächtigt sind. Nach dem SigG sind die PCA-Aufgaben:

Das SigG benutzt statt ›CA‹ oder ›PCA‹ bzw. ›Certification Authority‹ den Begriff ›Zertifizierungsdiensteanbieter‹.

- ❏ **Personen, die ein Signaturzertifikat beantragen, zuverlässig zu identifizieren**
  Der Antragsteller muss zur Erstbeantragung persönlich erscheinen und sich mit einem Ausweisdokument (Personalausweis oder Reisepass) ausweisen. Verlängerungen und nachfolgende Anträge können elektronisch erfolgen – unter Verwendung einer gültigen elektronischen Signatur.
  In vielen Fällen wird die CA diesen Registrierungsvorgang nicht selbst durchführen, sondern einer *Registration Authority* (RA) übertragen. Die Übergabe der PSE* muss an den Inhaber persönlich erfolgen. Er bestätigt dies durch seine Unterschrift.

Die CA ermöglicht mit über den Einzugsbereich verteilten RAs, solche Registrierungen vorzunehmen, ohne dass der Antragsteller dazu zur PCA reist.

- ❏ **Sie muss den Antragsteller eines Zertifikats über die notwendigen Maßnahmen zur fälschungssicheren Erstellung einer Signatur informieren,** (§ 6 SigG)
  ebenso über seine Pflichten und Rechte beim Einsatz der digitalen ID und des Zertifikats. Zu den Pflichten des Inhabers gehört z. B. die sofortige Sperrung des Zertifikats, sobald er von der Kompromittierung des Zertifikats Kenntnis erhält oder die ernsthafte Gefahr dafür besteht.

** PSE = ›Personal Security Environment‹, d.h. die SmartCard mit dem Schlüsselpaar*

- ❏ **Sie hat dafür zu sorgen, dass der Sicherheitstoken der digitalen ID den privaten Schlüssel sicher speichert.**
  Dies impliziert in der Praxis, dass für die Speicherung Krypto-SmartCards eingesetzt werden, bei denen der private Schlüssel die SmartCard nie verlässt und die Signatur des Hashwertes des

Dokuments auf der SmartCard durchgeführt wird. Die Karte muss zusätzlich (nach der SigV) durch eine PIN (oder ein biometrisches Merkmal) gesichert sein.

- **Publikation des Zertifikats (soweit vom Inhaber gewünscht)**[*]

* *so dass dieses für die Überprüfung elektronischer Signaturen abrufbar ist. Dieser Service ist optional.*

- **Sie hat ein Zertifikat auf Antrag des Inhabers oder seines Stellvertreters zu sperren,** indem sie es in eine Sperrliste (die *Certificate Revocation List*) aufnimmt. Stellt sich heraus, dass Angaben im Zertifikat falsch sind, so ist es ebenso zu sperren. Sperrungen dürfen nicht rückwirkend ausgeführt werden und sind nicht mehr umkehrbar.
- **Ausgabe von Zeitstempeln**[**]
  Diese gestatten den fälschungssicheren Nachweis, dass ein elektronisches Dokument zu dem im Zeitstempel angegebenen Zeitpunkt vorgelegen hat.

** *Auch hier gibt es ›qualifizierte Zeitstempel‹, die mit einer speziell zertifizierten Einheit erstellt werden können.*

Eine PCA, welche *qualifizierte Zertifikate* nach dem SigG ausgeben möchte, muss eine Reihe von Anforderungen hinsichtlich fachlicher Kompetenz, Sicherheitsmaßnahmen und Haftungsdeckungen erfüllen und bei der zuständigen Behörde (die *Regulierungsbehörde der Telekommunikation und Post*) registriert und akkreditiert sein. Erst mit einer zusätzlichen – aufwändigen Zertifizierung durch einen von der RegTP zugelassenen Zertifizierer erhält sie zusätzlich eine (freiwillige) *Akkreditierung* und kann erst damit *qualifizierte, akkreditierte Zertifikate* ausgeben.

Zweck der Zertifizierung ist die Prüfung folgender Punkte:

- Sicherheitskonzept der PCA
- Prüfung der Vertrauenswürdigkeit der Geschäftsleitung und des eingesetztes Personals sowie dessen Know-how
- Prüfung der Finanzkraft der PCA, um eine Betriebsgarantie zu gewährleisten
- Überprüfung, dass dort, wo vom SigG oder der SigV gefordert, zertifizierte oder anderweitig zugelassene Komponenten eingesetzt werden
- Sicherheitsanforderungen an die Betriebsräume und deren Zugangskontrollen

Die PCA muss darüber hinaus bestimmte Zugriffszeiten auf die Zertifikate sowie eine ausreichend hohe Verfügbarkeit sicherstellen. Sie kann auch qualifizierte Zeitstempel ausstellen. Die Zertifikatsverzeichnisse müssen gegen Manipulationen gesichert sein. Die

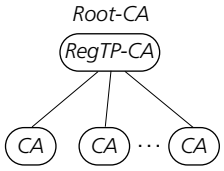
PCA muss über ausreichende finanzielle Ressourcen verfügen, um auch bei Aufgabe des Geschäftsbereichs die weitere Pflege (Publikation und Archivierung) der ausgestellten Zertifikate durch eine andere PCA sicherstellen zu können. Die PCA muss alle wesentlichen Transaktionen protokollieren. Die ausgestellten Zertifikate müssen 35 Jahre* über ihre Gültigkeit hinaus archiviert werden und abrufbar sein.

* *Dies gilt nur für akkreditierte CAs.*

Die CA-Hierarchie

Die akkreditierte (P)CA erhält ihre eigenen Signaturschlüssel (die sie für die Ausstellung der Zertifikate und Zeitstempel einsetzt) von der kontrollierenden Behörde – die RegTP. Diese Behörde stellt damit die *Wurzelinstanz* (*Root-CA*) dar. Das SigG sieht dabei in der gesamten PKI nur eine zweistufige Hierarchie vor: die Wurzelinstanz und die PCA. Unter der PCA dürfen nach dem SigG keine weiteren CAs (PCAs) angeordnet sein.

Das SigG erlaubt für qualifizierte Signaturen nur eine 2-stufige CA-Hierarchie:



Geltungsdauer von Signaturen

Eine elektronische Signatur gilt zunächst nur solange wie das für die Erstellung verwendete Zertifikat.** Die SigV sieht eine maximale Zertifikatsgültigkeit von 5 Jahren vor. Die meisten PCAs stellen jedoch nur Zertifikate mit einer kürzeren Laufzeit aus (1–2 Jahre). Die vom SigV zugelassene maximale Lebensdauer hängt auch von der eingesetzten Technik ab. So definierte der Maßnahmenkatalog (von 1998) beispielsweise, dass beim Einsatz von 768 Bit langen RSA-Schlüsseln das Zertifikat maximal eine Lebensdauer von 3 Jahren haben darf, während bei 1 024 Bit langen Schlüsseln 5 Jahre Lebenszeit möglich sind. Diese Parameter-basierte Beschränkung soll sicherstellen, dass die Signatur nicht innerhalb ihrer Gültigkeitsdauer gefälscht werden kann. Die Lebensdauerbeschränkungen sind deshalb sehr konservativ.

** *Korrekter: Sie ist solange gültig, wie das dabei eingesetzte Verfahren (in Kombination mit den Schlüssellängen) gültig bzw. sicher ist. Angaben hierzu sind auf der Home-Page der RegTP (www.regtp.de) zu finden.*

Die Gültigkeit bzw. Beweiskraft eines digital signierten Dokuments kann verlängert werden, indem innerhalb der Gültigkeit der Signatur das Dokument erneut mit einer länger gültigen Signatur signiert wird – wobei die Originalsignatur nun Teil des Dokuments wird und mitsigniert wird. Diese *Verlängerungssignatur* muss dabei nicht vom Aussteller der Originalsignatur erfolgen, sondern darf auch von einer anderen Person durchgeführt werden. Hierfür ist zusätzlich ein Zeitstempel erforderlich. Die nachsignierende Person bescheinigt mit ihrer Signatur lediglich, dass das Dokument bei der Nachsignatur noch gültig (im Sinne der Erstsignatur) war. Technisch verlängert sie den Zeitraum, in dem eine unbemerkte Dokumentenfälschung praktisch unmöglich ist. Dieser Vorgang ist wiederholbar.

Signaturkomponenten

Das Signaturgesetz definiert in § 17 die Anforderungen an die technischen Komponenten für elektronische qualifizierte Signaturen. Diese Forderungen sind jedoch bewusst allgemein gehalten, um keine einzelne technische Realisierung zu bevorzugen, sondern Entwicklungsspielraum zu geben. So wird z. B. in § 17 Abs. 1 SigG 2001 gefordert:

(1) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend.

Absatz 2 fordert, dass der signierte Inhalt vollständig und eindeutig angezeigt werden muss:

(2) Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht.
Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

1. *auf welche Daten sich die Signatur bezieht,*
2. *ob die signierten Daten unverändert sind,*
3. *welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,*
4. *welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und*
5. *zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.*

Betrachtet man z. B. MS-Word-Dokumente, so können diese ausgeblendete Textstücke enthalten. Hier wäre unklar, was signiert wird. Um diese Problematik zu vermeiden, wandelt die Signatursoftware der Firma Utimaco das Word-Dokument in ein Rasterdokument um. Die Signatur erfolgt dann auf den Daten des Raster-Images.

Die Forderung, dass die Prüfkomponente auch automatisch prüft, ob das zur Signatur verwendete Zertifikat zum Zeitpunkt der Signatur (*so die Interpretation des Autors*) auch gültig und nicht gesperrt war (definiert in § 5), setzt bereits einen komplexen Zugriff auf das Zertifikatsverzeichnis und die Sperrliste der ausstellenden CA voraus.

§ 17 Abs. 3 SigG 2001 detailliert die Anforderungen weiter und Absatz 4 fordert den Einsatz von entsprechend zertifizierten Komponenten, z. B. eine SmartCard als Träger des Sicherheitstokens (mit dem verwendeten Schlüsselpaar) mit einer Zertifizierung (nach SigV § 15) – wiederum detailliert im Maßnahmenkatalog des BSI – nach ITSEC ›*E 4 hoch*‹. Dies setzt z. B. bereits eine semiformale Beschreibung der Komponenten und den Nachweis ihrer Sicherheit voraus – eine sehr zeitaufwändige und teure Evaluation. Auch hier muss das BSI wiederum die Eignung der benutzten Algorithmen und ihre Gültigkeitsdauer festlegen.

Die Signaturverordnung

Die Signaturverordnung (SigV) detailliert und konkretisiert die Vorgaben des Signaturgesetzes. Sie legt z. B. fest, welche Voraussetzungen für die Erteilung einer PCA nach SigG für die Ausstellung von qualifizierten Zertifikaten erfüllt sein müssen. Sie beschreibt, welche Dokumentation die PCA zu erstellen hat und wie lange diese Dokumentation aufzubewahren ist. Ebenso ist das Vorgehen beim Einstellen der Tätigkeit einer PCA definiert. Zusätzlich sind eine Reihe von technischen und organisatorischen Details festgelegt, so z. B. Anforderungen an die PSE (SmartCard).

Zur Signaturverordnung siehe [[SigG]] (s. S. 702).

8.4.4 Signaturgesetze anderer Ländern

Nach Deutschland haben alle EU-Staaten Signaturgesetze verabschiedet – teilweise erst stimuliert durch eine entsprechende EU-Richtlinie aus dem Jahr 1997 – und wie Deutschland bereits wieder novelliert. Finnland sieht die Ausgabe einer Personalausweiskarte mit digitaler Identifikation vor, die dann auch für elektronische Signaturen genutzt werden kann.

Eine aktuelle Übersicht zum Stand der verabschiedeten nationalen Signaturgesetze ist in [[Hof_1]] (s. S. 706) zu finden.

In den USA haben die meisten Bundesstaaten ein Gesetz zur elektronischen Signatur verabschiedet – teilweise mit sehr unterschiedlichen Anforderungen.

Das deutsche SigG sieht vor, dass *elektronische Signaturen* aus EU-Staaten gleichrangig behandelt werden können,* wenn das Urheberland ein dem deutschen SigG ähnliches Gesetz verabschiedet hat und bei der Erstellung der Signatur dessen technische und gesetzliche Vorgaben eingehalten wurden.

* *§ 23 SigG 2001*

8.4.5 Offene Punkte zur elektronischen Signatur

Bisher liegen weder gründliche Erfahrungen mit großen (z. B. nationalen) PK-Infrastrukturen vor, noch nennenswerte Erfahrungen hinsichtlich der Bewertung von elektronisch signierten Dokumenten vor deutschen Gerichten. Beides werden die Jahre 2002–2006 bringen.

Der Aufbau eine kompletten (nennenswert großen) PKI in einem Unternehmen ist aufwändig und für die Nachweispflicht allein oft wirtschaftlich nicht zu rechtfertigen. Hier können teilweise jedoch Synergien mit anderen Maßnahmen genutzt werden – etwa bei der Einführung digitaler Firmenausweise, der Einführung von SSO-Systemen (*Single-Sign-On*) und der damit verbundenen Erhöhung des IT-Sicherheitsniveaus. Die hohen Kosten der PKI-Komponenten verhindern – zusammen mit den nachfolgend angesprochenen Interoperabilitätsproblemen – dass die Systemanbieter PKI-Komponenten kurzfristig vollständig in ihre Lösungen integrieren.

Die Interoperabilität von PKI-Komponenten und selbst zwischen deutschen CAs lässt bisher noch sehr zu wünschen übrig. Es ist damit noch nicht selbstverständlich, dass Sie die Gültigkeit eines eingehenden elektronisch signierten Dokuments problemlos automatisiert überprüfen können. Hier versucht man in Deutschland mit der Interoperabilitätsspezifikation ISIS-MTT Abhilfe zu schaffen.* Bis diese implementiert ist und greift, dürfte es jedoch 2005 werden. Selbst dann ist erst eine nationale (deutsche) Lösung und noch keine EU-weite oder gar weltweite Interoperabilität geschaffen – just diese ist aber für das Fortkommen des eCommerce förderlich.

* *Siehe [[ISIS-MTT]] (s. S. 707).*

Für viele Szenarien bleibt neben den Details der elektronischen Signaturen die Formatfrage ein Handicap für den praktischen Einsatz. Wie z. B. will ein Finanzbeamter ein ihm vorgelegtes Dokument auf Authentizität prüfen, wenn er nicht einmal mit seinen Arbeitsmitteln dessen Inhalt anzeigen kann? Schließlich ist der logische Inhalt immer die erste Stufe einer Prüfung und die Gültigkeit der Signatur dabei nachrangig. Die bisher vorliegenden Vorschriften lassen dass Thema des geeigneten Formats aber vollständig aus!

Eine verständliche und sehr qualifizierte Betrachtung zur Langzeitarchivierung elektronisch signierter Dokumente liefert [Roßnagel-3] (s. S. 701).

Es gibt zahlreiche weitere solcher offenen Fragen. Man wird in PKI-Projekten deshalb noch eine ganze Weile in aller Regel auf externe Fachkräfte und Berater zurückgreifen und mit längeren Projektzeiträumen rechnen müssen.

Falsche wäre es jedoch, dieses Thema zu ignorieren und auf die *goldenen Lösungen* zu warten – es könnte zu lange dauern.

8.5 Datenschutz personenbezogener Daten – BDSG

Wesentliche rechtliche Aspekte bei der Speicherung personenbezogener Daten liefert das Bundesdatenschutzgesetz (§ 28 BDSG). Nach § 35 Abs. 1 BDSG kann ein Betroffener verlangen, dass falsche Daten, die seine Person betreffen, gelöscht bzw. korrigiert werden. Ist die Rechtsgrundlage der Speicherung nicht oder nicht mehr gegeben (z. B. nach Auflösung eines Vertragsverhältnisses oder wenn das *berechtige Interesse der speichernden Stelle* nicht mehr gilt), so sind die Daten ebenso zu löschen (§ 35 Abs. 2 Nr. 3 BDSG).

BDSG = *Bundesdatenschutzgesetz*

Bei Mikrofilm und WORM, bei denen neben dem einzelnen Personeneintrag auf dem Datenträger noch zahlreiche weitere Daten stehen, die weiterhin benötigt werden, ist dies technisch nicht ohne weiteres möglich. Hier muss das System die Möglichkeit bieten, ein Datum oder Dokument als gelöscht bzw. ungültig zu markieren. Dies muss nicht unbedingt auf dem Datenträger selbst geschehen, sondern kann auch in der Datenbank erfolgen. Das als *gelöscht* markierte Datum darf dann jedoch nicht mehr im normalen Betriebsmodus bzw. der darauf aufsetzenden Anwendung sichtbar sein.

Bei Datenübertragungen auf neue Datenträger (z. B. bedingt bei einem System- oder Datenträgerwechsel) sollte das Übertragungsprogramm sicherstellen, dass das gelöschte Datum/Dokument nicht mitübertragen wird. Dies ist eine systemtechnische Anforderung an die Lösung. Zusätzlich sollte automatisch ein Protokoll erstellt werden. Eine gesetzliche Verankerung der letzten beiden Punkte gibt es jedoch nicht.

Liegt es bei normalen Belegdaten aus dem Bereich der Finanzbuchhaltung in der Regel im Eigeninteresse eines Unternehmens, die Daten vertraulich zu behandeln, so gelten für personenbezogene Daten zusätzlich die gesetzlichen Bestimmungen aus dem BDSG. Diese weichen bei DM-Systemen nicht von jenen eines normalen IT-Betriebs ab, erstrecken sich aber natürlich über den gesamten, eventuell längeren Aufbewahrungszeitraum der Daten. Zusätzlich ist hier bei der Vernichtung der Papiervorlagen darauf zu achten, dass die Vorschriften des Datenschutzes eingehalten werden. Wird die Vernichtung (z. B. als Teil einer externen Erfassung oder Entsorgung) per Outsourcing erledigt, so ist der Auftragnehmer entsprechend (in jedem Fall schriftlich) zu verpflichten.

Die erhöhten Sicherheitsanforderungen gelten natürlich auch für eventuell ausgelagerte Sicherungen. Wird ein gesamter Datenträger ausgesondert, ist er physikalisch unlesbar zu machen.

In diesem Buch nicht weiter betrachtet ist die Frage, welche personenbezogenen Daten überhaupt erfasst, wie lange sie gespeichert und unter welchen Bedingungen sie weitergegeben werden dürfen. Zu beachten sind hier neben dem BDSG auch das TKDSG (bei Telekommunikation), das TDDSG (bei Telediensten) sowie weitere spezifische Datenschutzgesetze, etwa bei Versicherungen, Ärzten und Krankenhäusern.

Bei der Speicherung personenbezogener Daten in elektronischen Archiven, die fast immer in ein Rechnernetz eingebunden sind, ist organisatorisch und systemtechnisch dafür zu sorgen, dass nur berechtigte Personen Zugang zu den personenbezogenen Daten erhalten.

Erfolgt die Archivierung personenbezogenen Daten im Outsourcing-Verfahren, so sind hier spezielle rechtliche Aspekte zu beachten (siehe [[dms-asp]] (s. S. 700).

Ein besonderes Augenmerk ist auf die Übertragung der Daten in Netzen zu legen. Dies gilt für lokale (LANs) und verstärkt für öffentliche Netze. Zu einfach lassen sich diese Daten durch ein Netzmonitorprogramm abhören. **Es ist davon auszugehen, dass dies auch wirklich passiert –** wenn auch oft ungezielt! Diese Daten müssen deshalb chiffriert übertragen werden und sollten, soweit möglich, auch chiffriert gespeichert werden.

Es ist zu überprüfen, ob die Verarbeitung personenbezogener Daten nicht die Benennung eines Datenschutzbeauftragten erforderlich macht – z. B. dann, wenn mehr als 5 Personen im Unternehmen mit der Verarbeitung personenbezogener Daten zu tun haben.* Ist ein solcher vorhanden, sollte er bei DMS-Projekten mit einbezogen werden.

** Siehe [[BDSG]] (s. S. 700).*

Die Novellierung des BDSG im Mai 2001* hat eine Reihe von Anforderungen verschärft und insbesondere Verletzungen des Datenschutzes zum Straftatbestand gemacht!

8.6 Urheberrecht – Copyright

Schließlich spielt das *Urheberrecht* bei der Erfassung und Speicherung eine Rolle und zwar dort, wo Dokumente erfasst oder genutzt werden, die durch das Urheberrechtsgesetz (UrhG) geschützt sind. Ein gesonderter Copyright-Vermerk zum Schutz der Urheberschaft ist hierbei im Dokument nicht erforderlich.

UrhG = Urheberrechtsgesetz

Geschützte Werke im Sinne des Urheberrechts sind gemäß § 1 UrhG *Werke der Literatur, Wissenschaft und Kunst*. Hierzu zählen (§ 2 UrhG):

- ❏ *Sprachwerke wie Reden, Schriftwerke und Computerprogramme*
- ❏ *Werke der Musik*
- ❏ *pantomimische Werke* und *Tanzkunst*
- ❏ *Werke der bildenden Künste einschließlich der Werke der Baukunst und der angewandten Kunst und Entwürfe solcher Werke*
- ❏ *Lichtbildwerke* und *Filmwerke* (und ähnlich geschaffene Werke)
- ❏ *Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen***

*** Hierzu gehören auch Datensammlungen und -zusammenstellungen in Datenbanken.*

Erfolgt die Speicherung nur für *eigene Zwecke*, so ist dies nach deutschem Recht bisher ohne eine Genehmigung des Urhebers und ohne eine Vergütung an diesen zulässig (§ 53 UrhG) – selbst dann, wenn, wie in Büchern und Zeitschriften üblich, dieses explizit im Dokument untersagt wird.

Mitte 2002 wird die BRD voraussichtlich das UrhG novellieren und damit an die Urheberschutz-Richtlinien der EU vom Februar 2001 anpassen. Das private Kopierprivileg wird dabei wesentlich eingeschränkt werden.

Als *eigene Zwecke* wird dabei der private Gebrauch betrachtet, bei dem sich kein direkter finanzieller Vorteil aus der Speicherung ergibt und bei dem die Daten nicht in Umlauf außerhalb des Bereichs gebracht werden. Die einschlägige Passage aus § 53 UrhG lautet:

»*(2) Zulässig ist, einzelne Vervielfältigungsstücke eines Werkes herzustellen oder herstellen zu lassen*

1. *zum eigenen wissenschaftlichen Gebrauch, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist,*
2. *zur Aufnahme in ein eigenes Archiv, wenn und soweit die Vervielfältigung zu diesem Zwecke geboten ist und als Vorlage für die Vervielfältigung ein eigenes Werkstück benutzt wird,*
3. *zur eigenen Unterrichtung über Tagesfragen, wenn es sich um ein durch Funk gesendetes Werk handelt,*
4. *zum sonstigen eigenen Gebrauch,*
   a) *wenn es sich um kleine Teile eines erschienenen Werkes oder um einzelne Beiträge handelt, die in Zeitungen oder Zeitschriften erschienen sind,*
   b) *wenn es sich um ein seit mindestens 2 Jahren vergriffenes Werk handelt.*

   …

(5) Die Vervielfältigungen dürfen weder verbreitet noch zu öffentlichen Wiedergaben genutzt werden. …«

Dieses freie Kopierrecht (für private oder interne Zwecke) **besteht nicht für Computerprogramme!**

! *Das private Kopierprivileg besteht nicht für Computerprogramme!*

Es gibt weitere Bereiche, für die legal und kostenfrei kopiert werden darf (z. B. für eine Verwendung vor Gericht, in Sammlungen für Kirchen, den Schul- oder Unterrichtsgebrauch), wobei jedoch auch dort Einschränkungen zu beachten sind. Es ist gestattet, z. B. **eigene, private** Pressearchive anzulegen, sofern deren Inhalt nicht Externen zugänglich gemacht wird.

Bei Firmen-internen Pressearchiven wird dieses Kopierprivileg sehr viel kritischer bewertet. So entschied der I. Zivilsenat des Bun-

desgerichtshofs, dass urheberrechtlich geschützte Beiträge aus Zeitungen und Zeitschriften – dies ist weitgehend der gesamte Zeitungsinhalt – auch in unternehmensinternen elektronischen Pressearchiven **nur** mit Zustimmung des Rechtsinhabers genutzt werden dürfen.*

* *Urteil vom 10.12.1998 (I ZR 100/96)*

Geschützte Texte, Bilder und andere Vorlagen dürfen frei kopiert, archiviert und auch wirtschaftlich vermarktet werden, wenn die Schutzfrist des Urheberrechts abgelaufen ist. Das Urheberrecht erlischt nach deutschem Recht 70 Jahre nach Tod des Urhebers (§ 64 UrhG). Sie dürfen also einen 100 Jahre alter Roman erfassen und kommerziell auswerten. Wird ein nachgelassenes Werk nach Ablauf von 60, aber vor Ablauf von 70 Jahren nach dem Tod des Urhebers veröffentlicht, so erlischt das Urheberrecht erst zehn Jahre nach der Veröffentlichung (§ 64 Abs. 2 UrhG).

Komplizierter wird das Urheberrecht, wenn ein Bild oder ein anderes geschütztes *Werk* erfasst, verändert und danach ohne Zustimmung des Urhebers verteilt/vermarktet wird. Das Ausmaß und die Art der Änderung bestimmen hierbei, ob es sich um ein unzulässiges Kopieren oder um eine neue künstlerische Arbeit handelt. In solchen Fällen sollte man versuchen, die Zustimmung des Rechteinhabers einzuholen.** Hier wird die Sache so kompliziert, dass wir sie in diesem Rahmen nicht ausreichend detailliert und verständlich darstellen können.

** *Bei vielen Werken liegt das Verwertungsrecht nicht mehr beim Urheber, sondern bei einem Verlag oder einer Verwertungsgesellschaft.*

Auf die Rechte, Pflichten und Anforderungen, die sich aus der Veröffentlichung noch geschützter Werke ergeben (oder einer Bereitstellung in einem öffentlichen oder halböffentlichen Archiv), soll hier nicht weiter eingegangen werden.

Kompliziert kann das Urheberrecht bei Multimedia-Werken hinsichtlich der Autorenvergütung werden, wenn Komponenten mehrerer Quellen eingesetzt werden. Hierfür sind handhabbare Konzepte erst in der Entstehung und bedürfen einer internationalen Anerkennung.

Wie in anderen Bereichen auch, unterscheiden sich die nationalen Urheberrechte. Stärker als in vielen anderen Rechtsbereichen gibt es hier aber internationale Abkommen, denen sich praktisch alle westlichen und der größte Teil der übrigen Länder angeschlossen haben.*** Diese Gesetze und Abkommen befinden sich zudem im Fluss. So wird in den USA aktuell von der Medienindustrie versucht, das Copyright in extremem Umfang auszudehnen und so zu gestalten, dass das private Kopierprivileg praktisch nicht mehr existiert. Es ist zu befürchten, dass dies in den internationalen Abkommen integriert werden wird. Der Anfang 2002 vorliegende Endwurf zur Novellierung des deutschen UrhG zeigt dies deutlich.

*** *Siehe hierzu [[WIPO]] (s. S. 710).*

8.7 Bildschirmarbeits-Verordnung

Die seit 1989 verabschiedete EU-Richtlinie 89/391/EWG ist seit Dezember 1996 auch in nationales Recht in Form der *Bildschirmarbeits-Verordnung* umgesetzt.* Ziel der Verordnung ist der Gesundheitsschutz der Beschäftigten. In ihr werden teils konkrete und teils schwammig formulierte Anforderungen an Gestaltung und Überwachung der Bildschirmarbeitsplätze gestellt. Die Verordnung gilt nicht für Notebooks, Registrierkassen, Schreibmaschinen oder für Bildschirme an Maschinen oder nur gelegentlich benutzten Arbeitsplätzen.

Nach dem Arbeitsschutzgesetz ist bei Betrieben mit mehr als 10 Mitarbeitern zunächst ein Gutachten für die Bildschirmarbeitsplätze zu erstellen. Die Analyse ist zu dokumentieren.**

Alle elektronischen Installationen und Geräte müssen den geltenden VDE-Bestimmungen entsprechen. Sie unterliegen im Bereich der gesetzlichen Unfallversicherung der Prüfverpflichtung nach der UVV ›*Elektrische Anlagen und Betriebsmittel*‹. Hierzu zählen auch betrieblich genutzte Privatgeräte.

Der folgende Text enthält eine Zusammenstellung der sicherheitstechnischen und ergonomischen Anforderungen und Fakten als Gestaltungshinweis für alle betroffenen Personen und Organisationseinheiten.

** Diese als ›Bildschirmarb.VO‹ bezeichnete Verordnung ist z. B. bei Berufsverbänden erhältlich.*

*** Die Grundsätze gelten auch für Unternehmen mit weniger als 10 Mitarbeitern; diese müssen jedoch keine Gutachten erstellen und keine Dokumentation anfertigen.*

Ergonomische Anforderungen

Die Arbeitsmittel müssen in ihren Abmessungen so gestaltet sein, dass eine gesunde Arbeitshaltungen möglich ist. Zum gesunden Sitzen gehören (siehe Abb. 8-1):

- ❏ Die richtige Einstellung der Rückenlehne, so dass die Wirbelsäule in allen Sitzpositionen gut abgestützt wird.
- ❏ Das Ausnutzen der gesamten Sitzfläche bis zur Rückenlehne.
- ❏ Das vollflächige Aufsetzen der Füße (ggf. mit Fußstütze) bei einem Winkel von mehr als 90° zwischen Unter- und Oberschenkel.
- ❏ Das Einnehmen einer abwechselnd vorgeneigten, aufrechten und zurückgelehnten Sitzhaltung.
- ❏ Ein zwanglos aufgerichteter Oberkörper und entspannt herabhängende Oberarme.
- ❏ Ein Winkel von mehr als 90° zwischen Ober- und Unterarm.
- ❏ Die Einstellung der richtigen Sitzhöhe unter Berücksichtigung der Arbeitshöhe.

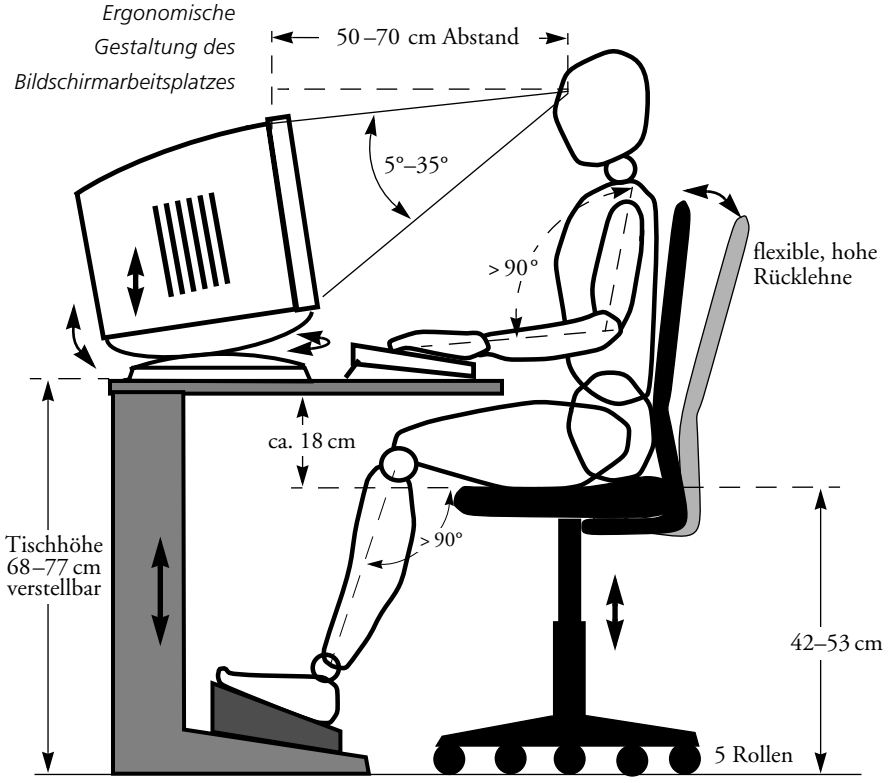
⇨ Übergangsfristen: *Geräte, die nicht Leben oder Gesundheit gefährden, aber den ergonomischen Anforderungen nicht entsprechen, müssen ersetzt werden. Die Übergangsfrist dazu lief Ende 1999 ab!*

Um z. B. am Bildschirmarbeitsplatz so sitzen zu können, müssen die Werte für Sitzhöhe, Sitztiefe, Tischhöhe, Beinraumgröße, Greifraum, Arbeitsflächengröße, Sehabstand, Konzeptplatzierung, Tastaturhöhe, Bildschirmhöhe usw. aufeinander abgestimmt werden. Das erfordert ergonomische Sachkenntnis und die Möglichkeit der Höhen- und Tiefenanpassung. Die Schreibtische müssen ausreichend groß sein.

Die für Scanner-Arbeitsplätze benötigten 19"- oder 21"-Monitore nehmen viel Platz ein! Man sollte sich hier überlegen, statt dessen 18"- oder 19"-Flachbildschirme einzusetzen, zumal diese kontrastreicher und augenschonender sind. Die Bildschirme sollen in jedem Fall entspiegelt und die Lichtquelle so aufgestellt sein, dass sie weder blenden noch sich im Monitor oder auf der Arbeitsfläche spiegeln.

Die ergonomischen Anforderungen an Bildschirmarbeitsplätze gelten auch für alle weiteren Arbeitsmittel und Arbeitsgegenstände. Bildschirm, Tastatur, Arbeitsvorlagen und weitere Geräte (z. B. Scanner) müssen so angeordnet werden, dass entsprechend der jeweiligen Arbeitsaufgabe für die Beschäftigten eine möglichst geringe Belastung entsteht.

Abb. 8-1
Ergonomische Gestaltung des Bildschirmarbeitsplatzes



Sichtbare Flächen dürfen nicht glänzen, und insbesondere die Arbeitsflächen dürfen nicht zu hell oder zu dunkel sein. Da diese Gestaltungskriterien auch für Bildschirme gelten, sind bevorzugt Bildschirme mit dunkler Schrift auf hellem Grund (Positivdarstellung) einzusetzen.

Um belastende Entfernungsanpassungen für das Auge weitgehend zu vermeiden, sind alle im zentralen Sehraum aufgestellten Arbeitsmittel in einem möglichst einheitlichen, individuell als angenehm empfundenen Sehabstand anzuordnen. Als Richtwert kann ein Sehabstand von 50 cm bis 70 cm gelten, der jedoch nicht als fester Wert zu verstehen ist. § 6 der Bildschirmarbeits-Verordnung fordert nach G37* eine Untersuchung der Augen und des Sehvermögens der Arbeitnehmer** (auf Kosten des Arbeitgebers) und zwar:

- ❏ vor Beginn einer Bildschirmarbeit und
- ❏ danach in regelmäßigen Abständen (d.h. etwa alle 3–5 Jahre)***
- ❏ beim Auftreten von Sehbeschwerden, die eventuell auf die Bildschirmarbeit zurückzuführen sind

** Siehe [G37], auf Seite 701.*

*** Diese darf auch von Augenoptikern durchgeführt werden.*

**** 3 Jahre etwa bei Mitarbeitern ab 45 Jahren.*

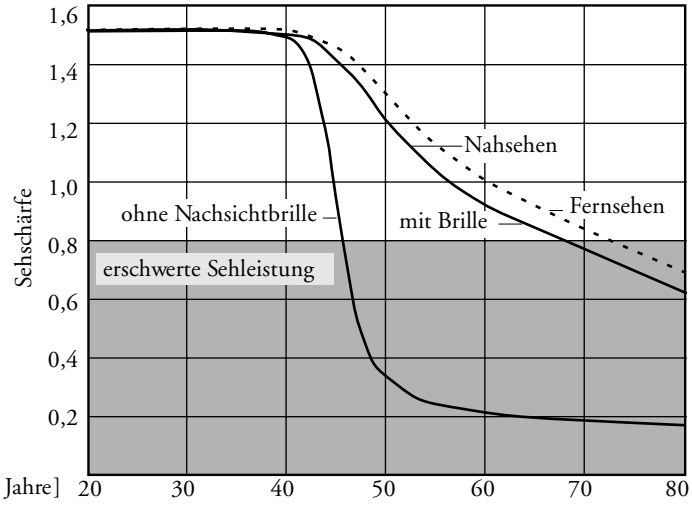


Abb. 8-2 Entwicklung des menschlichen Sehvermögens über das Lebensalter. Die stärksten Veränderungen treten zwischen 40 und 55 Jahren auf. Quelle: [[Dudek]], (s. S. 700)

Die Darstellung auf dem Bildschirm muss auch im seitlichen Gesichtsfeld eine flimmerfreie Wahrnehmung gewährleisten. Reflexionen und Spiegelungen auf der Bildschirmoberfläche sollten unbedingt vermieden werden.

Desweiteren werden Anforderungen an die Gestaltung des Bildschirms im Hinblick auf die Zeichengestaltung, die Zeichenleuchtdichte und die Formatierung der Information auf dem Bildschirm gestellt. Ebenso wird eine bestimmte Gestaltung der Tastatur ge-

fordert, wobei dabei die Eigenschaften und die Anordnung der Tasten wichtig sind.

Die Auswahl und Gestaltung der Büromöbel muss nach technisch-ergonomischen Gesichtspunkten erfolgen. Bei der Einrichtung von Bildschirmarbeitsplätzen sind störende, unnötig belastende Umgebungseinflüsse zu vermeiden. Dieses Problem tritt häufig dann auf, wenn in Arbeitsräumen nachträglich Bildschirmarbeitsplätze eingerichtet werden. Die geltenden Richtwerte für Beleuchtung, Raumklima und Lärm müssen eingehalten werden.*

* Siehe Seite 409.

Neben der ergonomischen Gestaltung der Bildschirmarbeitsplätze sollte auch der ergonomische Aspekt der Tätigkeit berücksichtigt werden. Diese Empfehlung geht von der Erkenntnis aus, dass unterschiedliche Tätigkeiten (*Mischarbeit*) in vielen Fällen eine individuelle Gestaltung der Arbeit ermöglichen und Arbeitsvorgänge zusammenhängend abgewickelt werden können.

Aus arbeitswissenschaftlicher Sicht ist der Erholungswert mehrerer kurzer Unterbrechungen der Tätigkeit, die überwiegend Blickkontakt zum Bildschirm erfordern, ungleich größer als der von wenigen langen Pausen. Deshalb sollten kurze Unterbrechungen dieser Tätigkeiten nicht aufgespart werden dürfen, um dafür den Arbeitsplatz früher verlassen zu können.**

** Quelle: [BAGUV]; (s. S. 700).

Die wesentlichen Parameter lassen sich damit wie folgt zusammenfassen:

Einige der hier aufgeführten Werte sind Empfehlungen und keine gesetzlichen Forderungen.

Sitzhaltung des Menschen
möglichst aufrechter Oberkörper
Schultern entspannt
Ober- und Unterarme im rechten Winkel
Ober- und Unterschenkel > 90 °
Kopf gerade ausgerichtet mit leichter Neigung von 15–20° nach unten

Tisch
höhenverstellbar zwischen 68 cm und 77 cm
dünne Tischplatte für viel Beinfreiheit
Minimalgröße des Tisches: 80 cm × 160 cm (für IT-Tätigkeiten)

Stuhl
5 Rollen
hohe Rückenlehne, beweglich, höhenverstellbar
Stütze der Rückenlehne in Gürtelhöhe
feste Sitzfläche
Sitzhöhe verstellbar zwischen 42–53 cm

Monitor höhenverstellbarer Drehfuß, neigbar
Bildfrequenz minimal 73 Hz, empfohlen ≥ 85 Hz
(bei TFT genügen 60–70 Hz)
Augenabstand mindestens 50 cm
schwarzer Text auf hellem Hintergrund
reflexions- und blendfrei
strahlungsarm (TCO 99)
oberste Informationszeile etwas unter Augenhöhe
mittlere Leuchtdichte ≥ 100 cd/m^2
möglichst ≥ 17" bei Windows-Anwendungen
Aufstellung möglichst im rechten Winkel zum Fenster

Tastatur separat vom Monitor frei beweglich
Tastaturhöhe maximal 30 mm (möglichst flach)
deutliche Beschriftung, leichter Anschlag
Tastaturneigung verstellbar, 6 –18°
Belegung möglichst DIN 2137
Ablage für Handballen vor oder auf der Tastatur

Beleuchtung
blendfrei, Tageslichtfarben
minimal 500 Lux
gleichmäßige Lichtverteilung
allgemeine Beleuchtung durch Einzelplatzbeleuchtung ergänzen

Arbeitsumgebung
Lautstärke am Arbeitsplatz max. 55 dB
relative Luftfeuchtigkeit: 40–65% (50 % optimal)
Raumtemperatur 21–22° C (maximal 26° C)*
Luftgeschwindigkeit 0,1–0,15 m/s am Arbeitsplatz
Reflexionsgrad der Decke: 0,7–0,85
Reflexionsgrad der Wände: 0,5–0,65
Reflexionsgrad des Bodens: 0,2–0,40
Reflexionsgrad der Arbeitsfläche: 0,2–0,50
jede direkte und indirekte Blendung vermeiden

* *und nur bei hohen Außentemperaturen*

8.8 Weitere Gesetze und Verordnungen

Verantwortlich für die korrekte Gestaltung eines Systems und seines Betriebs ist nicht der DMS-Anbieter, sondern der Betreiber!

Neben den bereits aufgeführten Gesetzen gibt es eine ganze Reihe weiterer Gesetze und Verordnungen, die im Einzelfall eventuell berücksichtigt werden müssen. Es liegt in der Regel in der Verantwortung des DMS-Projektleiters sich zu informieren, da die DM-Lösungsanbieter nicht alle betreffenden Vorschriften kennen können und vielfach die Anwendung eines DM-Systems auch nach der Erstabnahme noch auf andere Unternehmensbereiche ausgeweitet wird. Die wesentlichen zu ermittelnden Punkte sind die in den Gesetzen und Vorschriften festgelegten *Aufbewahrungsformen und -fristen* sowie eventuell zusätzlich bestehende Sicherheits- bzw. Vetraulichkeitsanforderungen.

So gelten z. B. für Krankenhäuser sehr lange Aufbewahrungsfristen, die sich aus Rechtsansprüchen von Patienten im Rahmen von Kunstfehlerprozessen ergeben können. Hier gilt eine Verjährungsfrist von 30 Jahren. Wissenschaftliche Zwecke und die Dokumentation der Krankengeschichte erfordern teilweise wesentlich längere Aufbewahrungsfristen. Auch gilt für Patientendaten natürlich eine sehr hohes Maß an Datenschutz.

*Auch versandte Daten (z. B. CDs und eMails) müssen **mehrfach (2-fach)** auf Viren geprüft werden, da Sie sonst für den entstehenden Schaden beim Empfänger haften!*

Weitere Anforderungen ergeben sich indirekt aus dem Produkthaftungsgesetz. Sie können es erforderlich machen, dass Konstruktionspläne, Rezepturen, Produktionsdaten, Prüfberichte, Verfahrensanleitungen, Reparaturanleitungen und Handbücher, Betriebs- und Gebrauchsanleitungen und ähnliche produktbezogene Informationen über den vollständigen Lebenszyklus eines Produktes hinweg aufbewahrt werden. Dies kann bei langlaufenden Produkten zu sehr langen Aufbewahrungsfristen führen, die insbesondere zum Zeitpunkt der Archivierung noch gar nicht festzuliegen brauchen.

Einige Anforderungen ergeben sich nicht durch den Gesetzgeber, sondern auch aus Vorschriften und Gepflogenheit von Branchen, Organisationen und Unternehmen selbst.

In der Pharmaindustrie gelten spezielle Regeln für Dokumente aus den Bereichen Forschung, Produktion und Antragsdokumentation, die sich weitgehend an den Vorgaben der ***Federal Drug Administration*** (FDA, USA) orientieren.

Man sollte sich bei DMS-Projekten sowohl mit der Rechtsabteilung im Hause als auch mit der Innenrevision abstimmen. Die Rechtslage ist oft weder schwarz noch weiß und eine gute (dokumentierte) Argumentation, Prozessorganisation und -dokumentation kann bei kritischen Anwendungen oft helfen.

8.9 Zusammenfassung rechtlicher Aspekte

Sieht man einmal von personenbezogenen Daten ab, so beziehen sich die rechtlichen Anforderungen an die Archivierung von Belegdaten im kommerziellen Umfeld weniger auf die Vertraulichkeit der Daten, sondern stärker auf das Unterbinden von Manipulationen und eine *ordnungsgemäße Ablage* sowie bei eingehenden Rechnungen auf den *Nachweis der Authentizität*. Die Anforderungen an eine *ordnungsgemäße* Ablage lassen sich vereinfacht wie folgt zusammenfassen:

- Unzulässige Änderungen der Unterlagen müssen verhindert werden. Dies geschieht durch
  - Systemeigenschaften,
  - Verfahren (z. B. fehlende Änderungsfunktionen),
  - die Art der Speicherung (d. h. auf 1-mal-beschreibbaren Medien),
  - schriftliche Arbeitsanweisungen an das Betreiberpersonal und
  - weitere Erläuterungen in der Verfahrensbeschreibung.
- Kein Zugang Unbefugter – insbesondere zu vertraulichen Daten und zu kritischen DM-Operationen.
- Abruf der Daten muss möglich sein
  - problemlos,
  - zeitnah,
  - in korrekter Reihenfolge,
  - über den gesamten geforderten Aufbewahrungszeitraum hinweg.
- Eine bildliche Übereinstimmung zwischen Original und Kopie ist bei Buchungsbelegen und eingehenden Handelsbriefen zu gewährleisten. Für ausgehende Handelsbriefe reicht eine inhaltliche Übereinstimmung.
- Protokollierung von Korrekturen und Umkopieren (und eventuellen Konvertierungen) von Daten/Dokumenten.
- Die Einhaltung der gesetzlichen Vorschriften muss (organisatorisch) kontrolliert werden.
- Dem Prüfer muss eine Verfahrensdokumentation vorgelegt werden können, aus der er den Ablauf des Verfahrens erkennen kann. Zusätzlich muss für ihn eine Prüfung ohne spezielle Hilfsmittel möglich sein. Dies impliziert, dass Belege und andere Informationen auf Verlangen ausgedruckt werden können.

Beachten Sie jedoch zusätzlich die speziellen Anforderungen an vorsteuerrelevante Belege (siehe Kapitel 8.1.1) und die Beweisproblematik elektronischer Dokumente im Zivilrecht bei Verträgen und Urkunden.

Besonderes Augenmerk muss der Dokumentensicherheit gelten:

- Bei aufbewahrungspflichtigen und juristisch relevanten Dokumenten ist sicherzustellen, dass die Dokumente vollständig erfasst und korrekt attributiert werden. Nur so können sie später korrekt abgerufen werden. Zusätzlich ist dafür zu sorgen, dass nur vertrauenswürdiges, entsprechend geschultes Personal eventuell notwendige kritische Operationen* ausführt. Dazu reicht in der Regel der bloße Passwortschutz für den Rechnerzugang nicht. Hier sollte ein zusätzliches Anmelden des Anwenders zur DM-Anwendung erforderlich sein. Das DM-Rechteprofil normaler DM-Anwender darf solche Operationen nicht zulassen.

- Vertrauliche Daten – etwa Personaldaten – müssen zusätzlich geschützt werden.** Diese Daten sollten nur chiffriert übertragen werden!

* *Hierzu zählen z. B. das Löschen, Umkopieren oder Um-Attributieren von Dokumenten.*

** *Hier ist zusätzlich zu prüfen, ob die Daten überhaupt erfasst und wie lange sie gespeichert werden dürfen.*

Da viele dieser Vorschriften recht ungenau und vielseitig interpretierbar sind, bleibt es letztendlich dem Steuer- und dem Wirtschaftsprüfer überlassen, ob ein System als ›*ordnungsgemäß*‹ akzeptiert wird. Diese sollten deshalb bei Einführung optischer Belegarchivierung informiert und eventuell konsultiert werden. Bei Systemen, welche die zuvor beschriebenen Anforderungen erfüllen, ist jedoch nicht mit Problemen zu rechnen, da sie inzwischen bereits verbreitet sind.

Ermitteln Sie selbst, welche speziellen Aufbewahrungsfristen und -formen für Ihre Dokumente gefordert werden. Berücksichtigen Sie dabei auch eventuelle indirekte Forderungen, welche sich z. B. aus Produkthaftung und spezifisch Ihr Unternehmen betreffenden Vorschriften ergeben können und dokumentieren Sie diese (z. B. als Teil der *Verfahrensdokumentation*).***

*** *Siehe Kapitel 9.8.*

Vergessen Sie nicht, den Betriebsrat und den betroffenen Fachbereich rechtzeitig in die Planung einzubeziehen.

Der Einsatz von elektronischen Signaturen und Zeitstempel, sowohl zum Urhebernachweis (bei eingehenden Dokumenten) als auch zum Nachweis, dass keine Veränderungen stattgefunden haben, wird kontinuierlich zunehmen. Denn seit den Jahren 2000/2001 haben sowohl die öffentlichen Stellen als auch die Industrie diese Thematik aufgegriffen (z. B. unter den Themenbereichen eGovernment, B2B-Procurement, B2C-Security). Auch Banken und Kreditkartengesellschaften forcieren den Einsatz der Technik beim eShopping/ePayment, um die Sicherheit zu erhöhen und Betrug im Internet zu reduzieren.

8.10 Code of Practice – die 10 Archivregeln der VOI

Der VOI (*Verband Organisations- und Informationssysteme e.V.*)* ist eine Vereinigung deutscher Anbieter von DM-Systemen und DMS-Komponenten. Er erarbeitete u.a. Richtlinien für eine *ordnungsgemäße Archivierung* im Sinne des Steuer- und Handelsrechts. Darin wurden 10 Maxime für eine GoBS-konforme Handhabung solcher Dokumente aufgestellt. Sie werden bei der VOI *Code of Practice* genannt:**

* *Siehe [[VOI]] (s. S. 710).*

** *Diese Regeln sind an den in England gültigen ›Code of Practice‹ angelehnt (siehe Seite 414 und Seite 700).*

1. Jedes Dokument muss unveränderbar archiviert werden.
2. Kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verlorengehen.
3. Jedes Dokument muss mit geeigneten Retrieval-Techniken wiederauffindbar sein.
4. Es muss genau das Dokument wiedergefunden werden, dasgesucht worden ist.
5. Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
6. Jedes Dokument muss in genau der gleichen Form, in der es erfasst wurde, wieder angezeigt und gedruckt werden können.
7. Jedes Dokument muss *zeitnah* wiedergefunden werden können.
8. Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur (des Archivs) bewirken, sind so zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
9. Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.
10. Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen (BDSG, HG, AO) sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.

Neu sind inzwischen die Anforderungen aus dem GDPdU und § 14 IV UStG hinzugekommen.

Siehe dazu die Abschnitte 8.1.4 –8.1.5.

8.11 Juristische Positionen anderer Staaten

Information zu einigen DMS-spezifischen Rechtsthemen ist für verschiedene Länder auf den Internet-Seiten von PROJECT-Consult zu finden unter: www.project-consult.de.

Wie bereits erwähnt, sind die Vorschriften bezüglich der Archivierung von Dokumenten landesspezifisch. Eine schnelle internationale Vereinheitlichung ist hier nicht abzusehen, wobei innerhalb der EU allmählich einige Vereinheitlichungen stattfinden – so z. B. bei den Signatur-, Datenschutz- und Steuergesetzen. Die EU betätigt sich, was das Thema *eCommerce* betrifft, durchaus als Treiber für neue, moderne Gesetze. Im Regelfall ist dabei eine einmal verabschiedete EU-Richtlinie innerhalb von 18 Monaten in nationales Recht umzusetzen.

Jedoch ist auch hier genau hinzuschauen, da zuweilen auch kleine Unterschiede nationaler Umsetzungen relevant sein können. So sieht z. B. die EU-Richtlinie (77/388/EWG) zur »*Vereinfachung, Modernisierung und Harmonisierung der mehrwertsteuerlichen Anforderungen an die Rechnungsstellung*« im Prinzip die *fortgeschrittene Signatur* für elektronische Rechnungen als ausreichend an, lässt den EU-Staaten jedoch gewisse Freiräume, innerhalb derer Deutschland z. B. nicht nur die qualifizierte, sondern gleich die *qualifizierte und akkreditierte Signatur* verlangt.

Zu [Skupsky] siehe Seite 702.

Eine recht ausführliche Diskussion der rechtlichen Aspekte für den amerikanischen Markt ist in [Skupsky] zu finden.

Die Beweiskraft eines elektronischen Dokuments wird in anderen Ländern teilweise weit stärker akzeptiert, als bisher in Deutschland. So sind in den USA elektronische Dokumente als Nachweise in Zivilprozessen weitgehend uneingeschränkt anerkannt, sofern für sie das benutzte Speicherverfahren und Dokumentenformat eine hohe Dokumentenechtheit sicherstellt.*

** Basis hierfür ist in den USA nach [Geis-3] die ›Rule 1001 Abs. 2‹ der ›Uniform Rule of Evidence‹.*

In England gestattet der ***C**ivil **E**vidence **A**ct* (CEA, von 1995) ein elektronisches Dokument als Beweismittel. Von Interesse ist hier insbesondere Section 8 und Section 9 der CEA.

Zum ›Code of Practice‹ siehe [CodeP] (s. S. 700).

In England wurde von einer Reihe von Foren und Normungsgremien der ›*Code of Practice for Legal Admissibility of Information Stored on Electronic Document Management Systems*‹ erarbeitet. Er soll als Grundlage für eine *rechtssichere elektronische Archivierung* im europäischen Rahmen dienen. In einer erweiterten allgemeinen Form sollen dabei die verschiedenen rechtlichen Rahmenbedingungen der EU in Form von Anhängen aufgenommen werden.

*** Zu [Geis-3] siehe Seite 701.*

Auch in der Schweiz erkennen Gerichte solche Dokumente als Beweismittel an. Basis ist hier nach [Geis-3] Artikel 962 Abs. 4 des Schweizer Obligationsrechts (OR).** Eine gute Übersicht zu den verschiedenen Signaturgesetzen pflegt S. van der Hof (siehe hierzu [[Hof_1]]).