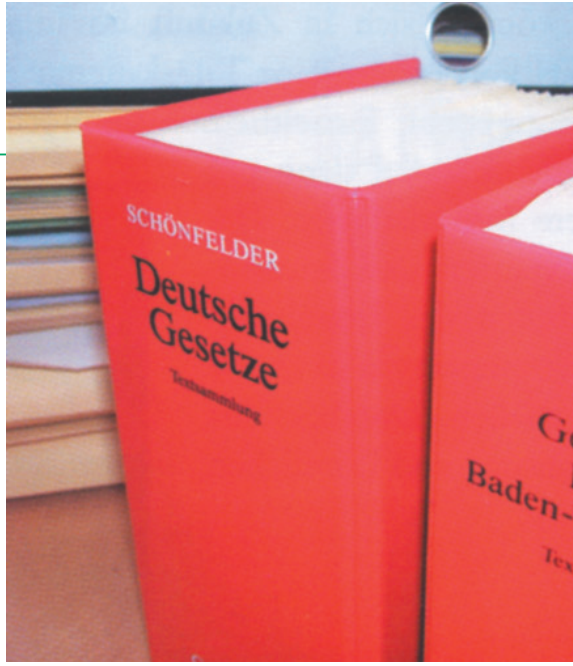

Ganz nach Vorschrift:

Compliance bei der Datenarchivierung

Wer die juristische Sachlage kennt, vermeidet Probleme bei der Bewältigung der unternehmensinternen Datenflut

Tatsache ist: Die Mehrheit der Unternehmen setzt die rechtlichen Bestimmungen zur Aufbewahrung elektronischer Daten nur halbherzig um. Rund zwei Drittel der Firmen hat noch nicht einmal innerbetrieblich festgelegt, wie elektronische Daten aufzubewahren sind (Computerwoche vom 20/2006). Gründe dafür sind hauptsächlich in den Kosten und dem komplexen Zusammenspiel von juristischen, technischen und betriebswirtschaftlichen Vorgaben zu suchen. Eine Schonfrist gibt es jedoch nicht: Wer nicht oder nur unsachgemäß archiviert, riskiert gravierende Haftungsrisiken für Geschäftsleitung und IT-Administration. Grund genug also, Archivierung nicht nur unter technischen, sondern auch strategischen Gesichtspunkten zu betrachten.

Was sagt das Handelsgesetzbuch?

§ 238 HGB verpflichtet Kaufleute zur Buchführung und Aufbewahrung von Handelsbriefen, die mit dem jeweils gesandten Original übereinstimmen. Um als Handelsbrief zu gelten, reicht bereits ein entfernter, lockerer Zusammenhang mit betrieblichen Interessen aus. Sämtliche Schriftstücke sind als Handelsbriefe anzusehen, die der Vorbereitung, Durchführung und dem Abschluss eines Geschäfts dienen (z. B. Angebote, Auftragsbestätigungen, Lieferscheine, jedoch nicht Werbeschreiben und Prospekte) oder auch der Rückgängigmachung (z. B. Reklamationsschreiben) – auch E-Mails (*Kasten 1*).

Aufbewahrungsanforderungen

Bestimmte Unterlagen, wie u. a. Handelsbücher, Abschlüsse, Buchungsbelege oder Handelsbriefe, sind nach § 257 HGB geordnet aufzubewahren. Das Gesetz schreibt weder ein Ordnungs- oder Buchführungssystem vor noch legt es Speichertechnologien oder Aufzeichnungsverfahren fest. Für das elektronische Archivierungsverfahren gibt § 239 HGB lediglich einen Kriterienkatalog vor: Die gespeicherten Dokumente müssen unveränderbar, reproduzierbar und jederzeit verfügbar sein. Dabei ist entscheidend, dass eine ordnungsgemäße, qualifizierte und geordnete Ablage sowie sichere Aufbewahrung der elektronischen Dokumente während des gesamten Aufbewahrungszeitraums erfolgt. Ausnahmen gelten nur für Eröffnungsbilanzen sowie Jahres- und Konzernabschlüsse, die auch als Originale in Papierform aufzubewahren sind.

Aufbewahrungsfristen

Für Buchungsbelege, Handelsbücher, Inventare, Jahres- und Konzernabschlüsse ist eine Aufbewahrungsfrist von zehn Jahren vorgesehen. Für alle übrigen Dokumente wie Handelsbriefe gelten sechs Jahre. Die Frist beginnt mit dem Schluss des Kalenderjahres, in dem die Unterlagen erstellt bzw. die Handelsbriefe verschickt oder empfangen wurden.

Kasten 1:

Handelsgesetzbuch (HGB)

§ 238 HGB	*– Pflicht zur Buchführung betrifft jeden Kaufmann*
§ 239 HGB	*– Einzelheiten zur ordnungsgemäßen Führung der Handelsbücher*
§ 257 HGB	*– Aufbewahrungsanforderungen und Aufbewahrungsfristen bis zu 10 Jahren*

Steuerrecht

§ 140 AO	*– Buchführungsrecht*
§§ 145, 146 AO	*– Buchführung und Aufzeichnungen*
§ 147 AO	*– Aufbewahrung von Unterlagen, Aufbewahrungsfristen bis zu 10 Jahren*
§ 14 IV UStG	*– Prüfbarkeit digitaler Unterlagen, z. B. Rechnungen*
GDPdU	*– Datenzugriff und Prüfbarkeit digitaler Unterlagen*
GoBS	*– Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme*

Nach Ablauf können die Unterlagen vernichtet werden.

Was ist steuerrechtlich zu beachten?

Steuerrechtlich müssen alle Kaufleute die Anforderungen an die Aufbewahrung und die Prüfung von Geschäftsunterlagen in §§ 145–147 Abgabenordnung (AO) einhalten, wobei die gleichen Fristen und Regeln gelten wie gemäß HGB. Einzelheiten dazu sind in den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" – kurz GDPdU – erläutert, die das Bundesfinanzministerium 2001 als Regelwerk für die Finanzbeamten zur elektronischen Steuerprüfung herausgegeben hat: Wurden Daten mit einem Datenverarbeitungssystem erzeugt, hat die Finanzbehörde das Recht, Einsicht zu nehmen und das System zur Prüfung zu nutzen. Für die Online-Kommunikation – also den E-Mail-Verkehr – bedeutet dies in der Praxis: Unternehmer sind nicht nur dazu verpflichtet, E-Mails gesetzeskonform zu archivieren. Sie müssen auch gewährleisten, dass den Betriebsprüfern alle betriebswirtschaftlich und steuerrechtlich relevanten E-Mails samt Anhängen jederzeit verfügbar gemacht und von diesen maschinell ausgewertet werden können.

Die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) des Bundesfinanzministeriums vom 07.11.1995 beziehen sich auf alle aufbewahrungspflichtigen elektronischen Daten und konkretisieren die Anforderungen an ihre Revisionssicherheit: Wie wird mit gescannten Dokumenten umgegangen? Wie müssen originär elektronische Daten verarbeitet werden? Wie muss ein internes Kontrollsystem implementiert sein? Auch wenn diese Vorschriften bereits seit über zehn Jahren existieren, sind sie in punkto elektronische Archivierung für Wirtschaftsprüfer, Finanzverwaltung und IT-Anwender relevanter den je. Insbesondere Steuerprüfer geben sich nicht wie bisher mit Papier zufrieden, sondern prüfen elektronisch und legen beim Steuerpflichtigen so manche Lücke in der GoBS-Erfüllung offen.

Der Knackpunkt bei elektronischen Rechnungen?

Nach § 14 Abs. 3 Umsatzsteuergesetz (UStG) darf bei elektronischen Rechnungen die Vorsteuer nur dann abgezogen werden, wenn die Echtheit und inhaltliche Unversehrtheit der Rechnung gewährleistet ist. Technisch brauchen diese Rechnungen eine qualifizierte Signatur mit Anbieterakkreditierung nach § 15 Abs. 1 Signaturgesetz (SigG), sonst erkennt das Finanzamt den Vorsteuerabzug nicht an. Diese Vorgaben gelten übrigens auch für elektronische Tickets – sei es für Bahnfahrten, Flüge oder Konzerte.

Elektronische Rechnungen sind gemäß der GDPdU beim Absender und Empfänger „revisionssicher" zu archivieren. Daher müssen gleichzeitig auch die Dokumentation der Signaturprüfung, Signaturprüfschlüssel, Zertifikat und eventuell weitere Kryptographie-Schlüssel aufbewahrt werden.

Existieren Insiderverzeichnisse?

Gemäß § 15b des Wertpapierhandelsgesetzes (WpHG) sind börsennotierte Unternehmen und ihre Dienstleistungsunternehmen (z.B. ein Übersetzungsbüro) verpflichtet, Verzeichnisse über Mitarbeiter zu führen, die bestimmungsgemäß Zugang zu Insiderinformationen haben. Egal, ob das Verzeichnis in Papierform oder elektronisch geführt wird, die Daten müssen lückenlos, jederzeit verfügbar und innerhalb angemessener Frist einsehbar sein. Die Finanzdienstleistungsaufsicht (BaFin) befürwortet jedoch die elektronische Speicherung und Übermittlung. Die Daten sind sechs Jahre bereitzuhalten – mit jeder Aktualisierung beginnt diese Frist erneut.

Was steckt in Spezialregelungen?

Spezialrechtliche Vorgaben zur elektronischen Archivierung betreffen zumeist börsennotierte Unternehmen und finden sich insbesondere im Geldwäschegesetz (§ 9), der Allgemeinen Verwaltungsvorschrift für das Rechnungswesen in der Sozialversicherung (§ 22 SRVwV) sowie

Kasten 2:

Die verflixten Sieben – Tipps zur technischen Umsetzung der elektronischen Archivierung:

1. Die elektronische Archivierung erfolgt zweckmäßig in einem auf Industriestandards basierenden Archiv und in einem ISO-genormten Datenformat (TIF, PDF)
2. Die zu archivierenden Dokumente sind unveränderbar und im Kontext mit übrigen Dokumenten zu betreffenden Geschäftsfällen aufzubewahren.
3. Das Archivierungssystem muss über effektive Schutz- und Sicherheitsmechanismen verfügen. Unbefugte dürfen insbesondere zu vertraulichen Daten keinen Zugang haben. Vertrauliche Daten (z.B. Personaldaten) müssen verschlüsselt gespeichert werden.
4. Unzulässige Änderungen der elektronischen Dokumente, auch durch Berechtigte, müssen verhindert werden. Dies kann durch Systemeigenschaften, und Art der Speicherung erreicht werden.
5. Der Abruf der Daten muss problemlos, zeitnah, in korrekter Reihenfolge und über den gesamten geforderten Aufbewahrungszeitraum hinweg erfolgen.
6. Die Archivierung sollte sich einfach benutzen und betreiben lassen.
7. Die elektronischen Daten und E-Mails sind zentral zu speichern – auch die von mobilen Geräten (Notebooks mit UMTS-Karten, PDAs, Blackberry etc.).

in Regelungen für Banken und Krankenhäuser und Ärzte. Letztere Regelungen schreiben sogar eine 30-jährige Aufbewahrungspflicht vor (z. B. § 6 Abs. 1 Krankengeschichtenverordnung, § 28 Abs. 4 Röntgenverordnung sowie § 43 Abs. 3 Strahlenverordnung).

In der Pharmabranche gelten spezielle Regelungen für Dokumente aus den Bereichen Forschung, Produktion und Antragsdokumentation, die sich weitgehend an den Vorgaben der Federal Drug Administration (FDA, USA) orientieren. Für Unternehmen, die an US-Börsen notiert sind, greifen mit Sarbanes Oxley (SOX) und der Securities and Exchange Commission (SEC) auch hierzulande weitreichende Archivierungspflichten für E-Mails und elektronische Kommunikation.

Kasten 3:

Bei der Erstellung eines Archivierungskonzepts spielen folgende Aspekte eine Rolle:

- Welche Geschäftsunterlagen müssen aus betriebswirtschaftlichen und gesetzlichen Gesichtspunkten sowie auf Grund vertraglicher Vereinbarungen aufbewahrt werden (Form, Gründe, Dauer)?
- Welche Anforderungen bestehen an die Sicherheit und das Archivierungssystem (technische Lösungsmöglichkeiten, Infrastruktur)?
- Wie sollen die Prozesse in Sachen Archivierung und Zugriff aussehen und in die operativen Geschäftsprozesse integriert werden?
- Wer sind die Stakeholder mit Interessen an Archivdaten und an wen werden die Verantwortlichkeiten delegiert?
- Wie werden die Archive bereinigt bzw. die Dokumente nach Ablauf der Aufbewahrungsfrist vernichtet?
- Welche internen Arbeitsanweisungen sind erforderlich?
- Welche Kontrollen müssen vorhanden sein, um einen sicheren und vertraulichen Archivierungsprozess zu gewährleisten?

Was schreibt KonTraG zur Archivierung vor?

Gemäß dem Gesetz zur Kontrolle und Transparenz in Unternehmen (KonTraG) gehört zum Risikomanagement einer Aktiengesellschaft auch die Verpflichtung zur rechtskonformen Archivierung von elektronischen Daten. Insbesondere muss dafür gesorgt sein, dass ausreichende Speicherkapazität sowie entsprechende Schutzvorkehrungen gegen Datenverlust bestehen. Vorstand und Aufsichtsrat sind insofern verpflichtet, geeignete Schutzmaßnahmen für die IT-Sicherheit ihrer geschäftskritischen Systeme und Daten zu konzipieren, umzusetzen sowie regelmäßig zu kontrollieren und aktualisieren. Letztendlich gilt das Risikomanagement für Geschäftsleiter und Kontrollgremien sämtlicher Gesellschaftsformen.

Welche Gefahren lauern?

Verlust der Vorsteuerabzugsberechtigung

Elektronische Nachrichten aller Art sind geschäftskritische Unterlagen und daher sorgsam zu behandeln und zu verwalten. Vor Vernichtung von Originalunterlagen sollte man sich immer fragen, ob eine Aufbewahrung aus Beweisgründen notwendig ist. Bei Rechnungen sind die Originale zur Geltendmachung des Vorsteuerabzugs gemäß § 15 UStG notwendig.

Fehlende Beweiskraft im Gerichtsprozess

Originale sind auch als Beweise in einem Gerichtsprozess von Bedeutung: So zum Beispiel, wenn ein Anspruch nur durch Vorlage des Originals zu beweisen ist (z. B. Vollmacht, Wertpapier etc.). Ist eine Partei nicht in der Lage, die für sie beweispflichtigen Tatsachen vorzulegen, obwohl diese elektronisch dokumentiert sein müssten, kann sie in einem Zivilprozess schon allein aus diesem Grund unterliegen.

Negative wirtschaftliche Auswirkungen

Datenverlust – selbst wenn er nur von temporärer Dauer ist – kann gravierende wirtschaftliche Auswirkungen für das Unternehmen haben. Eine mangelnde Hochverfügbarkeit von Daten – etwa im Supportbereich – kann zu Schadensersatzansprüchen durch Vertragspartner oder sogar zu erheblichen Vertragsstrafen führen. Der Imageschaden bei den betroffenen Kunden kann deutlich größer sein.

Drohende Strafen und Bußgelder

Die Verletzung der ordnungsgemäßen Buchführung kann dazu führen, dass die Finanzbehörden eine Steuerschätzung auf Basis der bekannten Besteuerungsgrundlagen (§ 162 Abs. 2 AO) durchführen, die mit Sicherheit eher zu hoch als zu niedrig ausfällt. Zudem kann die Finanzverwaltung die Aufbewahrungspflicht durch Zwangsgeld erwirken (§ 328 Abs. 1 AO) oder den Vorwurf der Steuerhinterziehung (§ 370 AO) oder leichtfertigen Steuerverkürzung (§ 378 AO) erheben. Im Falle einer Verurteilung drohen Geld- und Freiheitsstrafen bis zu fünf Jahren.

Verstöße gegen die GDPdU können mit 5000 Euro Bußgeld wegen Steuergefährdung (§ 379 AO) oder 50000 Euro im Falle der Steuerordnungswidrigkeit (§ 377 AO) oder schlichtweg mit bis zu 25000 Euro Zwangsgeld (§ 328 AO) geahndet werden.

Persönliche Haftung der Geschäftsleitung

Kommt der Vorstand einer Aktiengesellschaft seinen Pflichten des Risikomanagements nicht nach droht eine persönliche Haftung auf Schadensersatz als Folge der durch das KonTraG eingeführten neuen Vorschrift des § 93 Abs. 2 AktG.

Kasten 4:

Top 3 der typischsten Compliance-Fehler:

Hürde 1: Wenn Mitarbeiter Hausputz im E-Mail-Postfächer machen
Wird eine E-Mail-Nachricht vom Benutzer gelesen und dann gleich gelöscht, sind die meisten Archivsysteme schon ausgetrickst: Mitarbeiter löschen oft aus Unkenntnis der Rechtslage ihre E-Mail-Konten nach eigenem Ermessen oder archivieren die Informationen in veränderter Form oder nach eigenen Ordnungsprinzipien, wodurch sie ungewollt rechtliche Probleme für ihr Unternehmen provozieren.

Lösung:
Technisch sollte eine Kopie aller Nachrichten in einer eigens dafür angelegten Mailbox abgelegt werden. Organisatorisch wenden entsprechende Firmenrichtlinien ab, dass persönliche Archivierungsregeln aufgestellt werden. Statt die Geschäftskorrespondenz zeitaufwändig auf ihre Archivierungsrelevanz hin zu filtern und Mitarbeitern eventuell mit der Einstufung als aufbewahrungspflichtig überfordert sein, lassen sich die Prozesse vereinfachen und sichern, indem die gesamte Geschäftskorrespondenz archiviert wird. Kommt es später zu einer Überprüfung oder einem Gerichtsprozess, können speziell berechtigte Personen nach den relevanten elektronischen Dokumenten für den konkreten Einzelfall suchen und diese reproduzieren.

Hürde 2: Wenn sich Berufliches mit Privatem mischt
Werden auch private E-Mails von Mitarbeitern archiviert, kollidiert grundsätzlich das vollständige Protokollieren und Indexieren mit dem persönlichen Datenschutz der Mitarbeiter und dem Fernmeldegeheimnis. Gestattet oder duldet ein Unternehmen, dass seine Mitarbeitern ihre betrieblichen E-Mail-Konten auch zu privaten Zwecken nutzen, wird dieses Unternehmen gegenüber seinen Mitarbeitern zum Telekommunikationsdienstleister im Sinne des Telekommunikationsgesetz (TKG). Dies hat zur Folge, dass das Unternehmen den strengen Pflichten des Fernmeldegeheimnisses unterliegt. Nur mit der ausdrücklichen Einwilligung des Mitarbeiters und unter Berücksichtigung seiner Datenschutzinteressen kann das Unternehmen die Inhalte wie auch die näheren Umstände seiner E-Mail-Kommunikation archivieren und darauf zugreifen.

Lösung:
Die Einwilligung kann entweder über eine geeignete betriebliche Policy oder Betriebsvereinbarung zum Umgang mit E-Mails erfolgen oder auch im individuellen Arbeitsvertrag. Rechtlich ist es am einfachsten, die private Nutzung des betrieblichen E-Mail-Kontos zu verbieten. Auch wenn dies auf den ersten Blick als unzeitgemäß erscheint, sollte die tatsächliche Belastung für den Mitarbeiter nicht sehr groß sein, da doch unzählige kostenlose E-Mail-Anbieter existieren, die über Internet-Schnittstellen auch vom Arbeitsplatz abrufbar sind, ohne die betrieblich erforderlichen Archivierungsmaßnahmen zu beeinträchtigen.

Hürde 3: Wenn für den Datenschutz die erforderlichen Sicherheitsmaßnahmen fehlen:
Elektronische Archivierungssysteme erlauben zumeist nicht die erforderlichen Sicherungsmaßnahmen, um Datenschutzrechte oder sonstige rechtliche oder vertragliche Vertraulichkeitsregeln einzuhalten. Zum Beispiel gilt für die Aufbewahrung der Insiderverzeichnisse (§ 15 WpHG), dass nur die Personen Zugriff darauf haben dürfen, die im Unternehmen für die Führung des Verzeichnisses verantwortlich (z. B. Diese Regelung wird noch dadurch verschärft, dass die Vorstandsmitglieder im Zweifelsfall beweisen müssen, dass sie alle Maßnahmen ergriffen haben, um entsprechende Schäden zu vermeiden. Dazu gehören organisatorische Vorgaben, wie innerbetriebliche Archivierungsrichtlinien, Verfahrensdokumentationen, Administratorrechte, Systemeinstellungen sowie die Vergabe von Zugriffsrechten, als auch technische Aufwendungen, wie der Einsatz von Archivierungssoftware, Verschlüsselungstechniken, Datensicherung, Sabotage- und Ausfallschutz.

Haftung der leitenden (IT-)Mitarbeiter

Aber auch bei leitenden Mitarbeitern – wie z. B. IT-Security-Managern und IT-Administratoren – drohen Regressansprüche seitens des Unternehmens. Mangelnde Sorgfalt bei der Archivierung stellt eine Pflichtverletzung des Arbeitsvertrages dar und führt zu entsprechenden Schadensersatzansprüchen, die nur nach den Grundsätzen der „schadensgeneigten Arbeit" ausnahmsweise zu einer Haftungsfreistellung oder zu einer Minderung der Schadensersatzpflicht führen können. Bei Vorsatz bzw. grober Fahrlässigkeit wird von einer uneingeschränkten Haftung ausgegangen; im Falle einer leichten Fahrlässigkeit gibt es eine Schadensteilung. Daneben können Pflichtverletzungen arbeitsrechtlich eine Abmahnung und im wiederholten Fall eine Kündigung zur Folge haben.

Der erste Schritt zur Compliance?

Entwicklung einer Archivierungsstrategie

Geschäftsleitung und IT sind gefragt, zusammen mit Sachkundigen (z. B. Recht, Steuern) eine fundierte Archivierungsstrategie zu entwickeln. Je nach Unternehmen gilt es dabei, die organisatorischen und technischen Anforderungen für die Archivierung zu ermitteln und die Rahmenbedingungen für das Archivie-

rungskonzept festzulegen (*Kasten 3*). Dabei sind auch die betriebswirtschaftlichen Auswirkungen und Kosten der Archivlösungen zu berücksichtigen. Da Archivlösungen in der Anschaffung nicht gerade billig sind, sollten sie möglichst den funktionalen Bedürfnissen entsprechen, umfassend global im Unternehmen eingesetzt werden und schon allein wegen der langen Aufbewahrungsfristen höchst migrationsfreundlich sein.

Autor und Quelle Kastentexte:
Dr. Manfred Anduleit, Justiziar und Syndikusanwalt der Utimaco Safeware AG – The Data Security Company.

Kasten 4 (Fortsetzung):

Vorstand) oder beauftragt sind (z. B. Compliance-Mitarbeiter). Daraus folgt, dass auch die Dateien mit Insiderinformationen vertraulich aufbewahrt werden müssen, mit denen die im Insiderverzeichnis geführten Personen arbeiten. Außerdem muss sichergestellt werden, dass nur die im Insiderverzeichnis aufgeführten Personen tatsächlich Zugriff auf diese Dateien mit Insiderinformationen haben. Gleiches gilt auch bei sonstigen sensiblen Dokumenten (z. B. Personaldaten, Buchhaltung etc.), die elektronisch archiviert werden.

Lösung:
Um die Datenschutz- und Vertraulichkeitsverpflichtungen erfüllen zu können, sollten technische Hilfsmittel greifen: Spezielle IT-Technologien und Datenverschlüsselungslösungen helfen, dass nur berechtigte Personen und nur in begründeten Fällen Zugriff auf archivierte Inhalte haben. Diese sollten vom Datenschutzbeauftragten im Unternehmen eingerichtet und überwacht und begleitende organisatorische Maßnahmen etabliert werden.