Verfahrensdokumentation

Rechtsfragen

Felix v. Bredow
Dr. Ulrich Kampffmeyer

P R O J E C T C O N S U L T
Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH

Hamburg 2002

Verfahrensdokumentation

Von Dr. Ulrich Kampffmeyer

Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH
Managing Partner der PROJECT CONSULT International Ltd.
Mitglied des Executive Committee und des Board of Directors der AIIM Europe
Mitglied des DLM-Monitoring Committee der Europäischen Kommission

und Felix v. Bredow

Berater der PROJECT CONSULT Unternehmensberatung GmbH

Inhalt

Einleitung

Manche halten die rechtlichen Anforderungen an eine revisionssichere Archivierung für ein Hindernis bei der Einführung von elektronischen Dokumenten-Management- und Archivsystemen. Dabei sind Verfahrensdokumentationen selbstverständlich: auch für die Papierablage von kaufmännischen Belegen, die unter das Handelsgesetzbuch (HGB) und die Allgemeine Abgabenordnung (AO) fallen, ist eine Verfahrensdokumentation erforderlich.

Beim Umgang mit elektronischen Dokumenten kommen heutzutage weitere Anforderungen hinzu. Traditionell wurden der Dokumentenbegriff vom Gesetzgeber aus der herkömmlichen papierbasierten Welt abgeleitet. Daher stand auch immer das Papierdokument im Vordergrund. Abgeleitet aus diesem Umstand stand die Reproduktion des bildhaften Charakters eines Dokuments für die elektronische Archivierung immer im Vordergrund. Zur Zeit ist aber zu beobachten, dass sich genau dieser herkömmliche Dokumentbegriff wandelt. Der Wandel wird durch die Bemühungen des Gesetzgebers unterstrichen, die elektronische Signatur zu etablieren. Genau in diesem Kontext entstehen nun Dokumente, die nicht mehr in Papierform reproduzierbar sind. Eine elektronische Signatur ist nämlich nicht ausdruckbar. Weiterhin hat das Finanzamt nun im Falle einer Außenprüfung das Recht, steuerlich relevante Informationen direkt über die Systeme des zu prüfenden Unternehmens zu recherchieren. Und dieses solange die entsprechenden Unterlagen elektronisch vorgehalten werden müssen.

Diese sich ändernden Rahmenparameter ergeben zwar nicht unbedingt neue Anforderungen an eine Verfahrendokumentation, sie machen aber deutlich, dass das

© PROJECT CONSULT GmbH 2002

Thema elektronische Archivierung zukünftig immer stärker als Pflicht verstanden werden wird.

Rechtliche Grundlagen

Es gelten immer noch veraltete gesetzliche Regelungen, die zum Teil aus dem vorherigen Jahrhundert stammen. Beispiele hierfür sind die Zivilprozessordnung (ZPO) und das Bürgerliche Gesetzbuch (BGB). In diesen Gesetzen wurde noch bis Mitte 2001 durchgehend von einem Dokument in Papierform als rechtlich anzuerkennendes Original ausgegangen. Eine aus einem elektronischen System reproduzierte Kopie trägt natürlich nicht die Originalunterschrift und hat in der Regel auch noch keine Farbwiedergabe. In einem Prozess unterliegt ein solches Dokument bei der Beweisanerkennung als „Objekt des Augenscheins“ der freien richterlichen Zulassungsentscheidung.

Die Zeiten haben sich geändert: besonders durch die Internettechnologie entstehen immer mehr Dokumente mit Vertrags- oder kaufmännischem Charakter ohne Papierform und ohne manuelle Unterschrift. Durch das Signaturgesetz (SigG) wurden die Grundlagen für elektronisch unterzeichnete und rechtskräftige Dokumente längst geschaffen. Das Verfahren ist jedoch aufwendig, erfordert autorisierte Zertifizierungsstellen und hat sich auch aus Kostengründen noch nicht durchgesetzt. Die lange geforderte Anpassung des BGB ist inzwischen erfolgt. Damit ist sich die „Schriftform“ zur „Textform“ gewandelt. Inzwischen haben die Gerichte selbst begonnen – wie z. B. in Hamburg – auch elektronisch zu arbeiten. Anträge und Schreiben von Anwälten werden digital akzeptiert und gesamte Verfahren workflowbasiert in den Behörden abgearbeitet. Dies verringert natürlich auch für den Beweisführenden das Risiko, dass seine aus digitalen Systemen reproduzierten Dokumente nicht anerkannt werden. Zumindest dann, wenn der gesamte Entstehungs-, Speicherungs- und Reproduktionsprozess nachvollziehbar dokumentiert ist und Verfälschungen ausgeschlossen werden können, ist das Prozessrisiko inzwischen sehr klein geworden. Auch hier kann zukünftig eine Verfahrensdokumentation die Beweiskraft von digitalen Dokumenten absichern.

Durch die Steuerreform im Jahr 2000 haben sich Änderungen in der Allgemeinen Abgabenordnung ergeben, die den Geltungsbereich der Archivierungspflicht erweitert. Durch die GDPdU, der Grundsätze des Datenzugriffs und der Prüfbarkeit digitaler Unterlagen, erfolgt eine eindeutige Regelung zur Archivierung elektronischer Dokumente, die unter Handels- und Steuerrecht fallen. Die neuen Regelungen sollen die qualifizierte elektronische Signatur, die Bevorzugung nur einmal beschreibbarer digital-optischer Speicher, den direkten recherchierenden Zugriff auf Daten- und Dokumentenbestände beim Steuerpflichtigen und den Wegfall der Mikroverfilmung für originär digitale Belege einschließen. Damit gelten für Archiv- und Dokumentenmanagement-Lösungen die in HGB und GoBS festgelegten, nachvollziehbaren und überprüfbaren Regeln.

Die GDPdU räumt den Prüfern damit weitgehende Rechte ein, die auch die Bereitstellung lesbarer Datenträger zur Auswertung im Amt einschließen.

Das Recht der Prüfung nach HGB §§146 und 147 bestand schon immer, jedoch wird nun mit klaren Worten beschrieben, dass ein datenbankgestützter Zugriff für die Behörden möglich ist. Die GDPdU verweist ausdrücklich auf die GoBS, in der die Regeln für die Erstellung und Pflege von Verfahrensdokumentationen geregelt sind.

© PROJECT CONSULT GmbH 2002

Die Diskussion, welche Dokumente steuerlich relevant sind und welche nicht soll an dieser Stelle nicht geführt werden. Deutlich wird aber, dass all diejenigen sich mit dem Thema elektronischer Archivierung auseinandersetzen sollten, bei denen relevante elektronische Dokumente erzeugt und vorgehalten werden. Zu diesem Kreis gehören sicherlich Unternehmen, die bislang auf Mikrofilm-Techniken vertraut haben, Buchhaltungs- und ERP-Systeme wie SAP im Einsatz haben und die entweder den Einsatz der elektronischen Signatur planen oder damit rechnen müssen, zukünftig elektronisch signierte Rechnungen zu erhalten. Elektronische Archivsysteme müssen dann derart ausgelegt werden, dass ein Prüfer vom Finanzamt nur die Informationen sehen und auswerten kann, die als steuerlich relevante Informationen klassifiziert worden sind. Hier sind grundsätzliche Überlegungen zum eigenen Berechtigungskonzept und zur eigenen Ablagesystematik anzustellen.

Folgende Dokumentformate müssen zukünftig langfristig verfügbar und teilweise maschinell auswertbar vorgehalten werden können.

Dokumenttyp	Zulässiges Format
gescannte Seiten	TIFF (s/w), JPG2000 (Farbe)
digitales Fax	TIFF
Farbbilder	JPEG2000
eMail-Dateien	Auf ASCII basierend (z. B. XML, MIME), bei elektronischer Signatur alle im Originalformat Für Anhänge siehe andere Dokumenttypen
Screen-Dumps	Nicht als Bilddatei, sondern als Druckstrom auf ASCII basierend (z. B. XML), damit maschinenauswertbar
Datenstrom	Auf ASCII basierend (z. B. XML), damit maschinenauswertbar
Output-Dateien	Auf ASCII basierend (z. B. XML), damit maschinenauswertbar Layoutinformationen eventuell zusätzlich als TIFF, PDF oder JPG2000
Multimedia-Objekte	Soweit aufbewahrungswürdig alle in Frage kommenden Vorzugweise Wandlung in langfristig stabiles Format
Sprachdateien	Soweit aufbewahrungswürdig alle in Frage kommenden Vorzugweise Wandlung in langfristig stabiles Format
digitales Video	Soweit aufbewahrungswürdig alle in Frage kommenden Vorzugweise Wandlung in langfristig stabiles Format
Office Dokumente	Soweit aufbewahrungswürdig und nicht steuerlich relevant PDF, TIFF, JPG2000 Wenn steuerlich relevant Originalformat oder Wandlung in maschinenauswertbares neutrales Format (z. B. XML)

© PROJECT CONSULT GmbH 2002

Der Betrieb von solchen Systemen ist in einer Verfahrensdokumentation niederzulegen. Für die Archivierung von Dokumenten entsprechend HGB und GoBS gibt es eindeutige und nachvollziehbare - und damit auch überprüfbare – Regeln, die folgenden Grundsätzen unterliegen:

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

Archivierungsgrundlagen

Die Anforderungen an elektronische Archivsysteme sind im Prinzip selbstverständlich. Sie orientieren sich an den derzeitigen gesetzlichen Regelungen, die z.B. im HGB, AO, GoS, GoBS, BDSG und anderen Ortes niederlegt sind.

Verantwortung von Anbieter und Kunde

Bei der Betrachtung der Anforderungen an eine revisionssichere Archivierung sind unterschiedliche Verantwortlichkeiten zu unterscheiden:

- Die Verantwortung des Herstellers von optischen Medien, Laufwerken und Jukeboxen für das ordnungsgemäße technische Funktionen seiner Komponenten,
- die Verantwortung des Systemintegrators, der aus herkömmlichen DV-Komponenten, Datenbanken, optischen Speichersystemen und eigener Software eine Archivlösung bereitstellt und
- die Verantwortung des Anwenders selbst, der einen ordnungsgemäßen Betrieb nach den Vorgaben des Herstellers und des Systemintegrators sicherstellen muss.

Da bei der Erstellung und dem Betrieb eines Archivsystems in der Regel mehrere Beteiligte vorhanden sind, kommt der Trennung und der Zuordnung der Verantwortlichkeiten eine besondere Bedeutung zu.

Zehn Merksätze zu elektronischen Archivsystemen

1. Merksatz: Jedes Dokument muss unveränderbar archiviert werden.

Der erste Merksatz der revisionssicheren Archivierung ist, dass jedes Dokument unveränderbar archiviert werden muss. In diesem Zusammenhang gibt es immer die Argumente, dass zur Sicherstellung dieser Forderung der Einsatz von

© PROJECT CONSULT GmbH 2002

optischen Speichern ausreicht. Wenn man es aber genau nimmt und sich auch die Firmware und Betriebssoftware solcher Systeme betrachtet, erhält man schon an dieser Stelle eine ganze Reihe von Anforderungen, wie die Medien selber, wie die Objekte auf den Medien abgesichert werden müssen, um diese Grundanforderung zu erfüllen. Die Anforderung der Revisionssicherheit schließt die Fälschungssicherheit ein.

2. **Merksatz: Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.**

   Bezog sich der erste Merksatz eher auf die Medien, so betrifft der zweite Merksatz die Systeme. Es darf auf dem Weg in das Archiv und im Archiv selbst nichts verloren gehen. Das gleiche gilt natürlich auch für die Haltbarkeit der Medien und die Konsistenz der Verwaltungsinformationen.

   Aus diesem Merksatz leiten sich eine Reihe weiterer Anforderungen an die Auslegung von Archivsystemen ab. Der Anwender vertraut einem technischen System seine wichtigsten Informationen an und muss daher durch Sicherheitskopien, gegebenenfalls auch durch Verdopplung oder Spiegelung der Archivkomponenten für eine ausreichende Sicherheit bei der Verfügbarkeit sorgen. Dieser Sicherheitsaspekt kann Archivsysteme sehr kostenintensiv werden lassen und der Anwender muss sich im Vorfeld überlegen, welchen Wert eigentlich seine gespeicherte Information hat.

3. **Merksatz: Jedes Dokument muss mit geeigneten Retrievaltechniken wiederauffindbar sein.**

   Ein ganz wichtiger Satz ist, dass jedes Dokument mit geeigneten Retrievaltechniken wiederauffindbar sein muss. Es wird ja nicht um des „Speicherns Willen“ archiviert, sondern um Informationen möglichst schnell und ohne Medienbruch wieder bereitstellen zu können. Hier ist natürlich nicht nur eine Anforderung an den Anbieter gegeben, sondern auch an den Anwender, der sich über Verschlagwortung und Indizierung sehr genaue Gedanken machen muss, um hinterher sicherstellen zu können, dass er seine Informationen wiederfindet. Häufig sind die Probleme inkonsistenter oder unzureichender Indizierung eher ein Grund, warum Dokumente nicht wiedergefunden werden, denn technische Probleme.

4. **Merksatz: Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist.**

   Die nächste Forderung leitet sich aus dem vorherigen Merksatz ab. Es muss genau das Dokument wiedergefunden werden, welches gesucht worden ist. Wenn man an die Anforderungen von HGB/AO denkt, geht es nicht darum, irgendeinen Lieferschein oder irgendeine Rechnung zu reproduzieren, sondern genau diejenige, die gesucht wird. Auch hier verbirgt sich natürlich eine Forderung an die Konsistenz von Systemen dahinter. Es muss sichergestellt sein, dass kein Index „verrutscht“ ist - es darf somit nicht das vorherige oder das Folgedokument aufgefunden werden, sondern genau dasjenige, das gespeichert wurde. Wie bei dem dritten Satz ist auch hier wieder der Anwender gefordert, der dafür zu sorgen hat, dass keine Fehler bei der Erfassung auftreten.

© PROJECT CONSULT GmbH 2002

5. **Merksatz: Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.**

   Eine ganz harte Anforderung ist auch, dass kein Dokument während seiner vorgesehenen Lebensdauer zerstört werden darf. Vorgesehene Lebensdauer heißt nicht, dass Archive eingerichtet werden sollen, um diese endlos wachsen zu lassen und Informationen über Jahrhunderte zu speichern. Vielmehr muss ein vernünftiges Archivsystem natürlich auch eine Entsorgungsmöglichkeit bieten. Während einer definierten Lebenszeit darf ein Dokument jedoch nicht zerstört werden können. Das heißt natürlich auch, dass man von vornherein an Sicherheitskopien denken muss.

6. **Merksatz: Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.**

   Eine weitere sehr wichtige Forderung lautet, dass jedes Dokument in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können muss. Beliebige kriminelle Aktivitäten können dabei natürlich nicht unterbunden werden. Bei Faksimiles könnte man einwenden, dies stelle kein Problem dar, da meistens standardisierte TIFF-Dokumente archiviert werden. Ganz anders ist die Situation jedoch, wenn man beispielsweise an Dateien aus Büroautomatisierungsumgebungen, wie WinWord, Mail-Programmen und andere denkt, wo man ständig Veränderungen von Formaten rechnen muss oder die Dokumente sogar aktive, dynamische Verbindungen auf andere Komponenten haben. Hier ist es besonders schwierig einheitliche Formate zu finden und sicherzustellen, dass das archivierte Dokument genau dem ursprünglichen Zustand entspricht.

   In reinen Archivsystemen ist das Problem dadurch gelöst, dass jede neue Version auch als neues Dokument archiviert wird - der Anwender muss sich dann unter Umständen durch längere Hitlisten quälen um das gesuchte Dokumente in der richtigen Version zu finden. Bei dynamischen Dokumentenmanagementsystemen wird dieses Problem durch eine Versionsverwaltung gelöst. Für die Anzeige unterschiedlicher Formate gibt es heute eine Reihe von „Viewer“-Modulen, die ohne Veränderung der Originaldatei das Dokument so aufbereiten, dass es wieder angezeigt werden kann. Allerdings kann nicht ausgeschlossen werden, dass Formatinformationen fehlen oder aus einer Seite durch einen veränderten Umbruch zwei werden.

   Das gleiche Problem wie beim Anzeigen gilt natürlich auch für das Drucken. Auch hier existiert die 1:1 -Reproduktions-Forderung, d.h. das gedruckte Dokument muss hinsichtlich Format, Inhalt, Qualität, Form und Aussehen mit dem Original übereinstimmen. Hier bereiten bereits die heute üblichen Drucker Probleme, da sie nicht formatfüllend drucken. Es gibt immer eine Verkleinerung und „weiße Ränder“. Sind Drucker zudem nicht parametrisier- und vernünftig steuerbar, verschärft sich das Reproduktionsproblem. Sollen neue Drucker für ein Archivsystem beschafft werden, muss in jedem Fall getestet werden, ob die bereits archivierten Dokumente verlustfrei ausgedruckt werden können. Das Druckerproblem besteht für Dateien aus Büroautomationsanwendungen mehr noch als für Faksimiles, die als Pixel-Image ausgegeben werden.

7. **Merksatz: Jedes Dokument muss zeitnah wiedergefunden werden können.**

© PROJECT CONSULT GmbH 2002

Ein Gedanke, der häufig vergessen wird und der sich auch aus den Anforderungen des HGB/AO ergibt, ist dass jedes Dokument zeitnah wiedergefunden werden können muss. Spätestens dann, wenn der Anwender die Betriebs- oder Wirtschaftsprüfer im Hause hat, die bestimmte Belege haben wollen, warten diese nicht zwei Monate, bis ein Vollrecovery durchgelaufen ist. Die Anforderung ist, dass man die Dokumente wirklich Adhoc wiederfinden kann. Beim schnellen Wiederauffinden und Reproduzieren liegt auch einer der wesentlichen Vorteile der digitalen Archivierung gegenüber der analogen.

8. **Merksatz: Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.**

   Wichtig ist auch, dass alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, derart zu protokollieren sind, dass die Wiederherstellung des ursprünglichen Zustandes stets eindeutig möglich ist. Dies ist auch sicherzustellen, wenn z.B. in der Verwaltungsdatenbank ein Feld wegfällt, wenn zwei Felder zusammengeführt werden, zusätzliche Felder hinzukommen oder Dokumentenbestände aufgeteilt werden. Die ursprüngliche Struktur ist zu sichern und bei Bedarf wiederherzustellen. Diese Anforderung sichert auch, dass auf ältere Dokumente nach Veränderungen der Zugriffsdatenbank z.B. durch eine Optimierung, weiterhin zugegriffen werden kann.

   Hierfür sind geeignete Tools und Verfahren seitens des Anbieters bereitzustellen. Es liegt in der Betriebsverantwortung des Anwenders, diese auch ordnungsgemäß einzusetzen. Die entsprechenden Verfahren sollten daher auch in die allgemeine Verfahrensbeschreibung zum Betrieb des Archivsystems aufgenommen werden.

9. **Merksatz: Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.**

   Das Thema Migration ist für elektronische Archive besonders wichtig. Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist. Ständig ändern sich Hard- und Software, Datei- und Dokumentenformate sowie Strukturen und Organisation von Unternehmen. Auf der anderen Seite steht die Anforderung nach einer langfristigen Informationsverfügbarkeit. Um diese zu gewährleisten, muss die Migration von Archivsystemen bei Veränderungen von Betriebssystemen, Hardwarekomponenten und Anwendungssoftware berücksichtigt werden. Häufig ist es auch für den Betrieb eines elektronischen Archivsystems wirtschaftlicher, nach einigen Jahren die noch benötigten Informationen auf neue Medien umzukopieren. Die Softwarezyklen haben sich heute auf etwa neun Monate reduziert. Wie die Hersteller bei diesen kurzen Zyklen und der Komplexität der Software überhaupt noch in der Lage sind, lauffähige, qualitätsgesicherte Produkte auf den Markt zu bringen, ist schwer vorstellbar. Insbesondere die Hersteller von Archivsoftware unterliegen besonderen Anforderungen an die Sicherheit und langfristige Verfügbarkeit ihrer Produkte. Archivhersteller müssen einerseits Langfristigkeit verkaufen, d.h. eine mindestens zehnjährige Sicherheit für die Archive sicherstellen, und daneben die Systeme so auslegen, dass man mit

© PROJECT CONSULT GmbH 2002

geeigneten und einfachen Mitteln auf neue Hardware-, Softwareplattformen und Komponenten ohne Informationsverluste migrieren kann.

Dies bedeutet jedoch nicht, dass der Anbieter auf eigenes Risiko und eigene Kosten die Migration sicherstellen muss. Der Anwender muss selbst seine IT-Strategie festlegen und langfristig absichern. Dem Anbieter obliegt es jedoch, geeignete Tools und Verfahren für die Migration bereitzustellen. Vorteile haben alle diejenigen Anbieter, die bereits Migrationsprojekte durchgeführt haben.

Es empfiehlt sich bereits bei den Vertragsverhandlungen zwischen Anbieter und Anwender festzulegen, wie unterschiedliche Migrationen durchgeführt werden können, wer welchen Teil der Kosten trägt und wann eine Migration nach Meinung des Anbieters in jedem Fall sinnvoll oder sogar notwendig ist.

10. **Merksatz: Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen (BDSG, HGB/AO etc.) sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.**

Die letzte Anforderung hängt mit den gesetzlichen Bestimmungen zusammen. Gesetzliche Bestimmungen, wie das BDSG - Bundesdatenschutzgesetz, beinhalten ein paar Sätze, die der revisionssicheren Archivierung eigentlich widersprechen. Hierzu gehört, dass man personenbezogene Daten auf Anforderung nicht wirklich physikalisch löschen muss. HGB/AO sind allgemein bekannt, aber es gibt daneben in der Regel auch eine Reihe von betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz. Diese sind nicht nur für die aktuelle Version eines Archivs bei der Installation, sondern über die gesamte Lebensdauer eines solchen Archivs zu garantieren. Auch das ist sowohl für den Anwender aber auch für den Hersteller eine sehr teure Forderung, weil man sich von vornherein in der Architektur und Systemauslegung Gedanken über Entwicklungen machen muss, die man heute eigentlich noch gar nicht richtig abschätzen kann.

Dem Anbieter kann hierbei nicht die alleinige Verantwortung auferlegt werden. Der Betrieb des Archivsystems liegt nach der Abnahme in der Verantwortung des Kunden. Dieser muss entsprechend den zuvor mit dem Anbieter vereinbarten Regeln das System betreiben - andernfalls kann er es ja auch nicht einsetzen. Die einzuhaltenden gesetzlichen und haus-internen Bestimmungen sowie die darauf abgestimmten Sicherheits- und Protokollverfahren sind während der Einführungsphase in der Verfahrensbeschreibung zu definieren.

Kunde und Anbieter gehen bei der Installation von elektronischen Archiven eine langfristige und auf Vertrauen basierende Beziehung ein. Der Anwender muss das Vertrauen besitzen, dass das System so installiert, dokumentiert und wie in der Verfahrensbeschreibung beschrieben läuft, der Anbieter seinerseits muss darauf vertrauen können, dass der Anwender ausreichend qualifiziertes Personal bereitstellt und die technischen Vorgaben einhält, um das Archivsystem betreiben zu können. Aus diesem Grund ist es ratsam, offen auf beiden Seiten mögliche Probleme oder Engpässe zu diskutieren und durch geeignete personelle und technische Maßnahmen die notwendige Sicherheit des Verfahrens zu gewährleisten.

© PROJECT CONSULT GmbH 2002

Es lassen sich sicherlich noch weitere Merksätze hinzufügen. Damit ein elektronisches Archivsystem wirklich als sicher und langfristig verfügbar bei einem Anwender eingesetzt werden kann, sind zumindest die genannten Forderungen zu erfüllen.

Verfahrensdokumentation

Der Gesetzgeber verlangt eine, von Anwender und Hersteller gleichermaßen einzuhaltende, Verfahrensbeschreibung zum Betrieb eines revisionssicheren Archivsystems. In der Verfahrensbeschreibung wird neben den funktionalen Anforderungen des Anwenders auch die technische Beschreibung des Systems definiert. Anhand der Verfahrensbeschreibung soll die Revision prüfen können, dass alle rechtlichen Vorschriften zur Archivierung von Dokumenten auf elektronischen oder optischen Speichermedien eingehalten werden. Ein weiterer Aspekt ist die Nachvollziehbarkeit bei späteren Systemveränderungen. Durch die Beschreibung von Abläufen, Schnittstellen und die Definition von Aufzeichnungsformaten kann eine geordnete Migration vorgenommen werden.

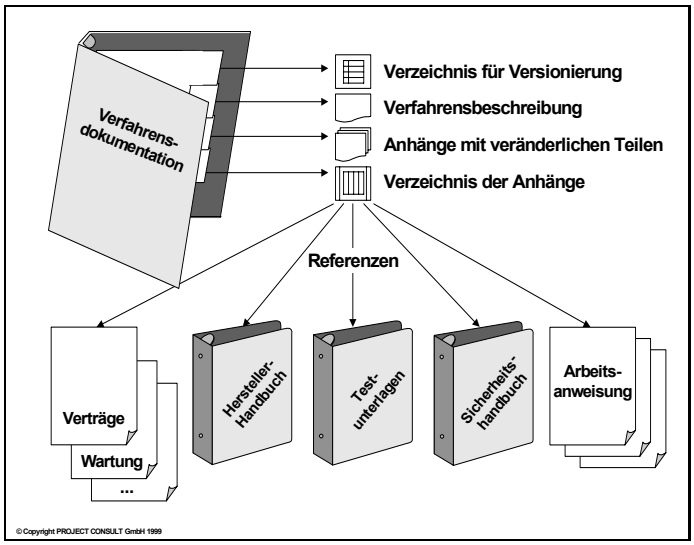

Abbildung 1 Aufbau einer Verfahrensdokumentation

Die aus steuerrechtlicher und buchhalterischer Sicht gefassten Anforderungen bedürfen einer Umsetzung in eine prüfbare Verfahrensbeschreibung, die auch die technischen Komponenten eines Archivsystems berücksichtigt.

Im allgemeinen ist die Verfahrensbeschreibung nicht isoliert, sondern im Zusammenhang mit Qualitätssicherungs-, Test- und Abnahmeverfahren zu betrachten, da sie parallel bearbeitet bzw. durchgeführt werden und eng miteinander verknüpft sind.

Bevor eine Verfahrensbeschreibung erstellt wird, sind die Aufgaben der Beteiligten festzulegen. Es sollte genau definiert werden, welche Aufgaben vom

- Anwender als Zulieferung,
- Anwender und Anbieter gemeinsam,
- Anbieter allein

© PROJECT CONSULT GmbH 2002

übernommen werden. Die schriftliche Ausarbeitung der Verfahrensbeschreibung erstellt der Anbieter. Dem Kunden obliegt die Aufgabe, zu prüfen, ob alle Anforderungen vom Anbieter erfüllt werden und die Verfahrensbeschreibung alle notwendigen Bestandteile enthält.

Bestandteile einer Verfahrensbeschreibung

Die im folgenden beschriebenen Bestandteile geben einen Überblick über alle Inhalte einer kompletten Verfahrensbeschreibung, bzw. Verfahrensdokumentation im Sinne der GoBS. Der Anbieter sollte verständlich und vollständig auf alle Bestandteile eingehen und Beschreibungen zu allen dort aufgezählten Merkmalen liefern. Schwerpunkte sind individuell zu setzen, wobei auf die Beschreibung des Datenschutzes, der Datenbank, der Archivkomponenten und der Ausfallsicherheit (Restart, Recovery) des Systems besondere Aufmerksamkeit gelegt werden sollte. Diese Anforderungen sind zwingend vom Anbieter zu beschreiben, um eine Anerkennung des Archivierungsverfahrens erreichen zu können.

Um den Anforderungen an eine revisionssichere Archivierung sowie einer geordneten Migration in ausreichender Form nachkommen zu können, wird die Erarbeitung einer in mehrere Punkte gegliederten Verfahrensbeschreibung vorgeschlagen.

Allgemeines Verfahren

Im allgemeinen Verfahren erfolgt eine kurze Beschreibung des Anwenders und dessen Geschäftszweck. In diesem Teil der Verfahrensbeschreibung sind weiterhin die betroffenen Bereiche, die Aufgabenstellung, die Einbindung in die vorhandene Organisation sowie die Aufbau- und Ablauforganisation kurz zu skizzieren. Dies ist zumindest für den Bereich zu beschreiben, in dem das System betrieben wird.

Rechtsgrundlagen

Die Basis für die zu beachtenden Rechtsgrundlagen sollten in der Projektdokumentation beschrieben werden. Archivierungspflichtig sind alle Unterlagen, die gemäß HGB und AO als solche bezeichnet werden. Des weiteren sind die Grundsätze ordnungsmäßiger Buchführung (GoS), ordnungsmäßiger Speicherbuchführung (GoBS) und das Bundesdatenschutzgesetz (BDSG) zu beachten.

Bei der elektronischen Archivierung kommen den Aufbewahrungsfristen und der Datensicherheit eine große Bedeutung zu. In der Verfahrensbeschreibung ist vom Anbieter eindeutig darzulegen, wie deren Sicherstellung erfolgt.

Grundsätzlich sollten folgende Punkte enthalten sein:

- langfristige Verfügbarkeit, also Sicherstellung des Betriebes,
- Vorhandensein eines Migrationskonzeptes zur langfristigen Darstellung der gespeicherten Informationen,
- vollständige und fälschungssichere Speicherung von Informationen,
- bildliche Übereinstimmung mit dem Original, wo der Gesetzgeber es fordert,
- Darstellung der Informationen in angemessener Zeit,

© PROJECT CONSULT GmbH 2002

- Art und Weise des unter bestimmten Bedingungen erforderlichen Löschens oder Sperrens von Informationen

Die Entscheidung, welche Dokumente in einem Archivsystem gespeichert werden sollen, muss jedes Unternehmen für sich treffen. Nach herrschender Rechtsauffassung stellt der Ausdruck von Dokumenten aus dem System - ob als Text oder Image - keine Urkunde dar (ZPO). Diesem Umstand ist durch geeignete Maßnahmen (z.B. Aufbewahrung von Urkunden im Original) Rechnung zu tragen. Falls der Einsatz einer elektronischen Unterschrift geplant ist und dies vom Anbieter realisiert werden kann, sind die Ausführungen des §126 BGB und des §4 Verbraucherkreditgesetz zu beachten.

Aus den vorstehenden Gründen ist das Verfahren zur Einführung durch Rechtsabteilung und Revision abzusichern. Gegebenenfalls ist das Verfahren der Oberfinanzdirektion anzuzeigen. Diese spricht erfahrungsgemäß eine Empfehlung aus bzw. gibt eine unverbindliche Erklärung ab und/oder nimmt das Verfahren zur Kenntnis.

Datenschutz

In einem Dokumentenmanagementsystem werden umfangreiche personen- oder abteilungsbezogene Datenbestände verwaltet. Zur Einhaltung der Bestimmungen des Datenschutzgesetzes sind geeignete technische und organisatorische Maßnahmen zu treffen. Sie müssen gewährleisten, dass Unbefugte keinen Zugriff auf Daten bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung haben. Deshalb ist es unabdingbar, die Zugriffsmöglichkeiten z.B. auch durch bauliche Maßnahmen (z.B. Schließanlage) und eine Benutzerverwaltung (zentral oder produktspezifisch) zu regeln. Die Benutzerverwaltung muss Vertretungen und Ersetzungen von Personen und Rollen sowie deren Rechten erlauben.

Einen wichtigen Punkt des Datenschutzes kann die Problematik des Löschens von personenbezogenen Daten darstellen. Diese können nach der Archivierung normalerweise nur noch logisch gelöscht werden. Hier muss entschieden werden, ob diese Art der Löschung ausreicht. Andernfalls kann nur durch Migration der Medien (Umkopieren der nicht gelöschten Bereiche) eine echte Löschung der Daten erfolgen.

Im Bereich Datenschutz sind weiterhin folgende Punkte zu berücksichtigen:

- Einführung von betrieblichen Richtlinien
- Bilden von Benutzergruppen, Funktionsklassen
- Einrichten von Benutzerprofilen
- Protokollierung von Änderungen der Benutzerdaten durch die Benutzerverwaltung
- Individuelle Zugriffssteuerung, z.B. auf Teilbereiche des Systems oder Bereiche anderer Benutzergruppen
- Vergabe von Zugriffsrechten, z.B. Recherchieren, Anzeigen oder Verändern von Informationen, Datenbankzugriff
- Zugriffssicherung durch Passwortschutz

© PROJECT CONSULT GmbH 2002

- Eingabe einer User-ID
- Bildschirmschoner mit Passwort
- Login grundsätzlich, nach kurzfristigem Verlassen und Remote
- Beschränkung der Anzahl Fehlversuche beim Anmelden
- Keine unverschlüsselten, über das Betriebssystem zugänglichen Daten auf dem Arbeitsplatzrechner
- Client-Absicherung, z.B. ohne Diskettenlaufwerk, Schloss und Schlüssel am Client
- Virenschutz
- Schutz der Arbeitsplätze und Server, z.B. geschlossener Raum, Schließanlage, Klimaanlage etc.
- Zugangskontrollen zum Rechenzentrum, zu Jukeboxen und Offline-Medien
- Datenschutz bei Datentransfer über Leitungen (z.B. ISDN) durch Verschlüsselung
- Der Umfang der Sicherungsmaßnahmen am Clienten ist in starkem Maß von der technischen Realisierung abhängig und im Einzelfall mit dem Anbieter abzustimmen.

Datenzugriff und Außenprüfung

Durch die Regelungen des StSenkG und der GDPdU hat das Finanzamt zukünftig das Recht, steuerrelevante Daten und Dokumente im Falle einer Außenprüfung elektronisch zu prüfen. Grundsätzlich sind drei Formen der Prüfung vorgesehen:

- die eigenständige Recherche beim Steuerpflichtigen mit Unterstützung durch das Personal des Steuerpflichtigen (Unmittelbarer Zugriff)
- Zurverfügungstellung von Auswertungen durch den Steuerpflichtigen entsprechend den Vorgaben des Prüfers (Mittelbarer Zugriff)
- die Mitnahme von Medien mit allen Daten und Dokumenten für die Prüfung im Finanzamt (Datenträgerüberlassung)

Im Bereich Datenzugriff und Außenprüfung muss daher folgendes beschrieben werden:

- Beschreibung der Zugriffsmöglichkeiten durch den Finanzprüfer
- Beschreibung und Definition der Prüfungsrelevanten Bestände
- Berechtigungskonzept zum ausschließlichen Zugriff auf die relevanten Informationen durch den Prüfer. Hier müssen vor allem die im Bereich Datenschutz beschriebenen Bestandteile berücksichtigt werden
- Möglichkeiten zum Löschen von Informationen. Da zur Zeit noch keine Haftungsregelungen für Datenverlust, der durch den Prüfer zu verantworten ist, beschrieben sind, sollten hier die entsprechenden Mechanismen beschrieben werden, die Streitfall für Klärung sogen können.

© PROJECT CONSULT GmbH 2002

Organisation

Bezüglich der Anforderungen an die Organisation zur Einführung und zum Betrieb des Dokumentenmanagementsystems sind folgende Punkte zu beachten:

- Das gesamte Verfahren ist im Einklang mit den Verantwortlichen für das Unternehmen oder den betroffenen Bereich einzuführen.
- In der Aufbauorganisation sind die Rollen im System mit Abgrenzung der Zuständigkeiten zu schaffen.
- Die Ablauforganisation soll das Verfahren durch Dienstanweisungen und Arbeitsanweisungen sicherstellen.
- Beim Einsatz von DV-Programmen ist die Ordnungsmäßigkeit der Verarbeitung sicherzustellen und die Rechtmäßigkeit der Verfahren nachzuweisen. Unbefugte Eingriffe in den Arbeitsablauf dürfen nicht möglich sein.
- Nicht jeder Benutzer ist berechtigt, Auswertungen im System zu erstellen.
- Das technische Umfeld (Systemkomponenten, Zugangskontrollen etc.) ist aufzubauen.

Vorgangsdefinition

In der Vorgangsdefinition ist auf die Behandlung und Bearbeitung von Dokumenten wie gescannte Images, Fax und selbsterzeugte Dokumente näher einzugehen. Der Begriff „Vorgang“ ist in diesem Zusammenhang als Arbeits- und Systemprozess im Rahmen der Archivierung zu sehen. Informationen, die in das System gelangen, bestehen grundsätzlich aus zwei Teilen - einerseits aus den eigentlichen Inhalten, die archiviert werden sollen, und andererseits aus den Zugriffsinformationen (Index), die zum Wiederfinden der Dokumente benötigt werden. Neben der Beschreibung der Übernahme von Inhalten und Zugriffsinformationen in das System sind deren Aufbau und Formate offen zu legen. Die Bearbeitungsstufen müssen durch eine eindeutige Vorgangsidentifizierung protokolliert werden und nachvollziehbar sein. Hierbei ist sicherzustellen das jedes gespeicherte Dokument über definierte Zugriffskriterien wiederauffindbar ist und genau die Information, die gesucht wurde, bereitgestellt wird.

Scannen

Der Prozess „Scannen“ muss in seinen einzelnen Bearbeitungsschritten beschrieben werden. Dies kann in Stichpunkten oder z.B. als Folgeplan geschehen und ist individuell anzupassen. In die Beschreibung sollten u.a. einfließen:

- der Scanvorgang selbst
- Qualitätssicherung
- Unveränderbarkeit des Scanergebnisses
- Indizierung
- Ergänzen der Images und Daten
- Ersetzen der Images und Daten

© PROJECT CONSULT GmbH 2002

- Löschen von Images und Daten
- Neuordnen von gescannten Seiten
- Speicherung der Images auf der Jukebox
- Verwaltung und Konsistenz der Einträge in der Indexdatenbank

Transport im System

In diesem Teil der Verfahrensbeschreibung werden sowohl die Transporte in das Archiv als auch aus dem Archiv, sowie die Speicherhierarchie beschrieben. Hier muss deutlich werden, wie der Anbieter den vollständigen, fehlerfreien und unveränderbaren Transport jeder Art von Informationen in seinem System sicherstellt.

Bei der Erfassung und der Übertragung in das Archiv kommt der sicheren Übergabe der Dokumente an das DMS eine große Bedeutung zu. Die Beschreibung des Transports (Datenfluss) ist für jede Dokumentenübernahme, sei es durch Scannen, als selbsterzeugte Datei, über Fax, Drucken mit und ohne Archivierung, zu erstellen. Beim Output tritt neben die Sicherheit noch die Möglichkeit zur schnellen Suche nach archivierten Dokumenten. Abgesehen von der Beschreibung des Datenflusses sollte dieser Bestandteil der Verfahrensbeschreibung folgende weitere Punkte beinhalten:

- wie bei Systemausfällen dem Datenverlust vorgebeugt wird,
- ob und wie eine mehrfache Speicherung durchgeführt wird,
- wodurch eine schnelle Suche nach Dokumenten gewährleistet wird,
- ob und wie Dokumente auf den Arbeitsplätzen redundant zwischengespeichert werden können,
- Protokollierung der Vorgänge,
- Verfahren zum Wiederanlauf,
- Möglichkeiten der Auslastungskontrolle.

Datenbank

Unter der Datenbank wird hier die integrierte Referenzdatenbank (Indexdatenbank) verstanden, die zum einen die Indexmerkmale der abgelegten oder archivierten Dokumente, zum anderen die für die Verwaltung der Dokumente notwendigen Merkmale enthält. Die Indexdatenbank enthält festgelegte Grundinformationen (Grundindex und ‘Unique Identifier’) für einen eindeutigen Zugriff und die Verwaltung der Dokumente.

Die Dokumente auf den optischen Speichermedien müssen so archiviert werden, dass die Indexdatenbank bei Datenverlust wiederhergestellt werden kann. Um ein hohes Maß an Sicherheit zu erzielen, wird vorausgesetzt, dass die Datenbank alle Aktionen vollständig protokolliert (Logging). Des weiteren ist in der Verfahrensbeschreibung auf die Problemfelder

- Wiederanlauf,
- Recovery/Teilrecovery,

© PROJECT CONSULT GmbH 2002

- Reorganisation,
- Konsistenzabgleich bei mehrfacher Datenhaltung,
- Im- und Export von Daten,
- Teilen und Auslagern von Tabellen,
- Einspielung von Datensicherungen,
- Statistikmöglichkeiten und
- Migrationskonzept der Datenbank (gleicher oder anderer unterstützter Hersteller), insbesondere bei spezifischen Erweiterungen näher einzugehen. Sämtliche Änderungen und Ergänzungen, die an Dokumenten vorgenommen werden, sind in Protokollen zu dokumentieren.

Hard- und Softwarekomponenten

In diesem Teil der Verfahrensbeschreibung ist das technische Umfeld einschließlich der Systemarchitektur zu skizzieren. Bei der Hardware sollte eine Unterscheidung nach spezifischer Hardware (Server, Clients, Scanner, Drucker) und Spezialkomponenten (Medien, Laufwerke, Jukeboxen) erfolgen.

Spezifische Hardware

Hier ist die Ausstattung der Hardware zu erläutern. Die einzelnen Komponenten sind mit ihren Grundspezifikationen darzustellen. Auch die Betriebsbedingungen gehören dazu.

Medien

Für die Archivierung der Dokumente ist der Einsatz von optischen Speichern vorzusehen. Das Überschreiben der Daten muss durch ein entsprechendes Aufzeichnungsverfahren ausgeschlossen werden. Die Beschreibung der einzusetzenden Medien sollte folgende Aspekte berücksichtigen:

- Art und Typ des Mediums
- Aufzeichnungsverfahren, Formatierung, Sicherung der Informationen
- Sicherstellung gegen Überschreiben („Schwärzen“) von Informationen
- Verfügbarkeit
- Kompatibilität
- Datenorganisation auf den Medien, z.B. Gruppierung, sequentielles Schreiben etc.
- Gewährleistung
- Haftung
- Wiederherstellung (Duplizieren, Recovery von Medien)
- Alternative Lieferanten

Laufwerke

Die wichtigsten Laufwerksspezifikationen sind folgende:

© PROJECT CONSULT GmbH 2002

- Hersteller
- Art der Laufwerke
- Betreibung, Aufzeichnungsverfahren
- Betriebsbedingungen (Strom, Klima, etc.)
- Schnittstellen
- Austausch
- Verfügbarkeit
- Kompatibilität über mehrere Generationen
- alternative Lieferanten
- Gewährleistungszeitraum
- Lieferzusagen für Ersatzteile über den Gewährleistungszeitraum hinaus

Jukeboxen

Es wird davon ausgegangen, dass die angebotenen Laufwerke in entsprechende Jukeboxsysteme eingesetzt werden können. Wegen der Vielzahl der möglichen Kombinationen von Laufwerken und Jukeboxen sollte sich der Anbieter auf nachstehende Angaben beschränken:

- Hersteller
- Art, Typ
- Anzahl und Konfiguration der Laufwerke
- Schnittstellen-, Betriebs- und Steuersoftware
- Betriebsbedingungen (Gewicht, Klima, Strom etc.)
- Offline-Medienverwaltung
- Logische und physikalische Verwaltung der Medien
- Zugang, Zugriff, Remote-Maintenance
- Caching
- Verfügbarkeit, Kompatibilität
- Liefer- und Wartungsgarantien
- Verfügbarkeitszeitraum von Ersatzteilen

Softwarekomponenten

Es ist zu beschreiben, welche Softwarekomponenten als

- Betriebssoftware (Version, Patch-Level, spezifische Erweiterungen)
- Basissoftware (Treiber)
- Anwendungssoftware (Client- und Server-Dienste)
- Werkzeuge zur Systemverwaltung

© PROJECT CONSULT GmbH 2002

angeboten werden.

Verfügbarkeit

Die langfristige Verfügbarkeit der Komponenten ist vom Anbieter sicherzustellen. Darunter fallen u.a. folgende Punkte:

- Zeitraum der Verfügbarkeit
- Kompatibilität der Komponenten
- Offenheit gegenüber anderen Herstellern
- Verwendung von Standards bei Formaten und Kompressionsverfahren
- Versionsmanagement
- Update-Garantien

Drucken

Das Drucken von Dokumenten sollte lokal und über Netzwerkdrucker möglich sein. Weiterhin sollte die Ausgabe die Möglichkeit der Kennzeichnung als Kopie, sowie Angaben (Index, Bearbeiter, Datum etc.) zu dem ausgegebenen Dokument als Aufdruck enthalten können.

Sicherheit des Systems

Da eine hohe Verfügbarkeit aller Komponenten von entscheidender Bedeutung ist, sollte das System so ausgelegt werden, dass z.B. bei Ausfällen einzelner Rechner die Funktionalität des Systems weiterhin gegeben ist. In der Verfahrensbeschreibung muss der Anbieter darstellen, durch welche Maßnahmen eine hohe Systemverfügbarkeit gewährleistet werden kann. Dies betrifft sowohl die redundante Auslegung von Komponenten, als auch Möglichkeiten zum Wiederanlauf (Restart) und zur Wiederherstellung (Recovery). Hierbei ist zu beachten, dass die Ausfallsicherheit in starkem Maße von der Qualität der eingesetzten Hardware abhängig ist. Werte zur Ausfallsicherheit in Prozent und Lebensdauer sind vom Hersteller anzugeben und möglicherweise sogar vertraglich festzulegen.

Backup-Konzept

Durch ein Datensicherungskonzept lassen sich gespeicherte Dokumente vor einem Verlust durch Hardware-Schäden oder andere Einflüsse schützen. Vom Anbieter ist zu beschreiben, welche Arten der Datensicherung im System vorgesehen sind und welche Komponenten einer Sicherung unterliegen sollten. Zusammen mit dem Anwender ist ein Verfahren zur Durchführung von Datensicherungsmaßnahmen aufzustellen bzw. an eine vorhandene Systematik anzupassen und in der Verfahrensbeschreibung zu dokumentieren.

Restart

Die Restart-Routinen sollen sicherstellen, dass aufgetretene Fehler oder Systemausfälle zu keinem Verlust und keinen Inkonsistenzen des Dokumentenbestandes führen und in kürzester Zeit wieder behoben werden können. Bei der Darstellung des Wiederanlaufes sollte für den Ausfall jeder einzelnen Komponente angegeben werden können, mit welchem Aufwand und

© PROJECT CONSULT GmbH 2002

nach welcher Dauer die Aufnahme eines eingeschränkten sowie des vollständigen Betriebes wieder möglich ist. Hierzu gehört ebenfalls die Darstellung, wie nach einem Systemabsturz die Konsistenz des gesamten Systems wiederhergestellt werden kann (Transaktionen zurücksetzen, unvollständige Dokumente löschen, Abgleich Archiv mit Datenbank etc.).

Recovery

Recovery bedeutet die Wiederherstellung eines Teiles oder aller Indexdaten. Beim Recovery sind die Möglichkeiten des

- Teilrecovery, z. B. nach Archiv, Zeitraum, Medium, Dokumentenklasse, und des
- Vollrecovery für die Gesamtwiederherstellung im Katastrophenfall zu berücksichtigen. Der Anbieter muss dem Anwender seine Recovery-Konzepte aufzeigen. Diese Prozesse sind zusammen mit Aufwänden, Zeiten und Absicherung zu beschreiben. Es sollte hier für jede „Recovery-Art“ getrennt eine derartige Beschreibung erfolgen, um so eine bessere Einschätzung über die Bedeutung eines entsprechenden Ausfalls zu ermöglichen.

Formate

Um eine langfristige Lesbarkeit der archivierten Dokumente sicherzustellen, sollten grundsätzlich nur Standardformate und Standardkomprimierungsverfahren eingesetzt werden. Für die langfristige Planung und Entwicklung sind vom Anbieter die benötigten Formate offen zu legen.

Qualität

Da die Einführung mit erheblichen Kosten verbunden sein kann, muss vom Anwender bei der Anbieterauswahl besondere Aufmerksamkeit auf die Qualität bei

- der Software,
- der Lesbarkeit und Reproduzierbarkeit von Dokumenten,
- der Dokumentation des Verfahrens,
- der Modularität,
- der Updatefähigkeit,
- der Wartbarkeit und
- den Tools zur Pflege des Systems

gelegt werden. Der Anbieter sollte in der Lage sein, eine Bescheinigung über die Durchführung der Qualitätssicherung nach ISO 9000 liefern zu können. Qualität kann aber auch durch Testverfahren und Abhandlung aufgetretener Fehlerquellen nachgewiesen werden. Der Anbieter muss seine Maßnahmen zur internen und externen Qualitätssicherung darlegen.

Betrieb

In diesem Teil der Verfahrensbeschreibung sind die vom Anwender zu berücksichtigenden Voraussetzungen zu nennen, damit das System ordnungsgemäß arbeitet, z.B.:

- Mindestpersonal zur Aufrechterhaltung des Betriebs

© PROJECT CONSULT GmbH 2002

- Qualifikation der Mitarbeiter
- Aufgabentrennung zum Schutz vor Manipulationen
- Festlegung einer einheitlichen Nomenklatur
- Benutzerhilfen und -führung
- Individuelle Menüsteuerung entsprechend den Zugriffsberechtigungen
- Prozess für Freigabe und Abschluss von Vorgängen
- Beschreibung der Funktion Löschung

Wartung

Es ist zu prüfen, inwieweit und in welchem Umfang Verträge mit Anbietern oder Herstellern zur laufenden und präventiven Wartung von Hard- und Software abgeschlossen werden müssen. Bei der Ausgestaltung der Verträge sollten präventive Arbeiten, die vom Anwender selbst vorgenommen werden können und in entsprechenden Handbüchern dokumentiert sind, berücksichtigt werden. Werden vom Anwender weitere Wartungsarbeiten übernommen, sollte dies ebenfalls schriftlich vereinbart werden, um bei Gewährleistungs- und Garantiefällen die Zuständigkeiten eindeutig nachweisen zu können. In jedem Fall muss jedoch eine Mindestwartung zur Sicherstellung des Betriebes und der Datensicherheit bereitgestellt werden. Bei der Planung eines Verfahrens zur Durchführung von Wartungsarbeiten ist darauf zu achten, dass der laufende Betrieb möglichst ungestört bleibt. Der Anbieter muss hier die Aufgaben, Abgrenzungen und Intervalle der Wartung beschreiben.

Migration

Bei der Einführung ist eine langfristige Planung zur Erhaltung der Betriebsbereitschaft, Datensicherheit und Verfügbarkeit der Archivdaten notwendig. Aufgrund der schnellen technologischen Entwicklung ist davon auszugehen, dass in Zukunft Änderungen im Hard- und Softwarebereich in relativ kurzen Abständen eintreten werden und deshalb ein Migrationskonzept unerlässlich machen. Migration bedeutet die Überführung von Dokumenten bedingt durch den Wechsel

- in ein höherwertiges System/Versionswechsel,
- der Systemart,
- des Herstellers.

In der Verfahrensbeschreibung muss der Anbieter eine eindeutige und fundierte Migrationszusage abgeben und das Verfahren der Migration beschreiben. Hierbei kann auch eine Aufteilung von Zuständigkeiten zwischen Anwender und Anbieter erfolgen. Die Zusage sollte auch für eingesetzte fremde Produkte bei Nichtverfügbarkeit einer Folgeversion - sofern deren Einsatz zur Aufrechterhaltung des Betriebes notwendig ist - gelten. Falls der Anbieter dieses Produkt nicht selbst vertreibt, sollte er ein funktional vergleichbares Produkt eines Drittherstellers anbieten.

© PROJECT CONSULT GmbH 2002

Anforderungen an die Prüfung der Ordnungsmäßigkeit eines Verfahrens

Die Prüfung der Ordnungsmäßigkeit eines elektronischen Archivierungsverfahrens bedarf neben der Erstellung der Verfahrensbeschreibung einer Reihe von Prüfungen.

Die formale Prüfung vergleicht die Verfahrensbeschreibung mit der System- und Anwendungsdokumentation. Sie prüft insbesondere ob die Verfahren des Scannens oder Datenimports gegen Veränderung abgesichert sind, die Indizierung konsistent und eindeutig und das zielgerechte Wiederfinden mit einer originalgetreuen Reproduktion gewährleistet ist.

Die praktische Prüfung am System prüft zunächst die Übereinstimmung der Verfahrensbeschreibung und der Dokumentation mit dem Programmsystem. Ferner werden Tests zur Erfassung, Indizierung, Recherche und Reproduktion durchgeführt, die mit der Verfahrensbeschreibung und der Dokumentation übereinstimmen müssen. Die Ergebnisse müssen auch in Ausnahmesituationen mit versuchten Eingriffen in das System immer konsistent, vollständig und richtig sein. Besonders wird geprüft, ob das System gegen unberechtigte Zugriffe, Veränderungen der Indizierung, Verfälschung von Dokumenten und Fehlbedienung ausreichend abgesichert ist. Ein weiterer Punkt der Prüfung ist das verlustfreie und konsistente Wiederanlaufen nach einem Störungsfall. Ein test der Recoveryverfahren muss die vollständige, richtige und konsistente Wiederherstellung des Systems im Störungsfall sicherstellen. Vorgabe ist, dass unter keinen Bedingungen ein Dokument verloren gehen, verändert oder nicht wiedergefunden werden darf. Tests des Ausdrucks stellen die Übereinstimmung der Reproduktion mit dem erfassten Original in Größe, Form, Inhalt, Qualität und Originalitätscharakter fest.

Die Prüfung ist von sachkundigen, neutralen Dritten durchzuführen, d.h. weder vom Anwender noch vom Hersteller oder Systemintegrator. Im Prüfungsdokument oder Zertifikat sind das Verfahren der Prüfung, benutzte Dokumentation, Testmaterial, Testfälle und die Ergebnisse festzuhalten. Das von technisch versierten Fachleuten zu erstellende Dokument sollte von einem zugelassenen Wirtschaftsprüfer formal bestätigt und gegengezeichnet werden.

Checkliste

Die folgende Checkliste gibt einen kurzen Überblick über Struktur und Inhalt einer Verfahrensdokumentation:

Bestandteile einer Verfahrensdokumentation für DMS- und Archivsysteme zur Speicherung kaufmännischer Daten und Dokumente		
Allgemeine Beschreibung des Einsatzgebietes	Einsatzgebiet der Lösung	z. B. Installationsort des Systems, Beschreibung des Aufgabenfeldes des betroffenen Bereiches etc.
	Beschreibung der allgemeinen Organisation	z. B. Aufbauorganisation, Organigramm des Betreibers, Ablauforganisation, Anwendungsfeld der Lösung etc.
Beschreibung der Lösung	Beschreibung der sachlogischen Lösung	z. B. Beschreibung der zu archivierenden Dokumente und Daten einschließlich deren Rechtscharakter, Vorgehensweise bei der Behandlung der Dokumente vor der Verarbeitung, Erläuterung des internen Kontrollsystems in Zusammenhang mit der sachlogischen Lösung, Ordnung der Dokumente
	Umsetzung der Anforderungen nach GDPdU	z. B. Beschreibung der prüfungsrelevanten Bestände, Berechtigungen, Zugriff und

© PROJECT CONSULT GmbH 2002

Bestandteile einer Verfahrensdokumentation für DMS- und Archivsysteme zur Speicherung kaufmännischer		
		Löschen von Informationen
	Programmtechnischer Ablauf der Lösung	
	Identität der Beschreibungen mit dem eingesetzten Programm	
Systembeschreibung	Netzinfrastruktur	z. B. Konfigurationsdaten des Netzes, Systemauslegung, Systemkonfiguration
	Spezielle Hardwarekomponenten	z. B. optische Speichermedien, Laufwerke, Jukeboxen, Scanner, Server, Clients, Drucker
	Standard-Softwarekomponenten	z. B. Betriebssystemumgebung, Standardmodule der Anwendung, Version, Zusammenwirken mit anderer Software
	Individuelle Programmteile der Lösung	z. B. Version, eingebundene Softwareprodukte, Funktionalität, Parametrisierungsmöglichkeiten
Beschreibung des Internen Kontrollsystem (IKS)	Internes Kontrollsystem	z. B. Zugangskontrollmechanismen, Login-Mechanismen, Definition der Benutzerprofile, maschinelle Kontrollen, Benutzerverwaltung mit Zuständigkeiten und Verantwortungsbereichen, Beschreibung der archivierungsrelevanten Arbeitsabläufe, Beschreibung der Protokollierung von Änderungen, des logischen Löschens, etc.
	Datensicherheit	z. B. Datensicherungskonzept, Recoveryverfahren
	Daten- und Zugriffsschutz	z. B. Protokollierung von Änderungen der Benutzerdaten durch die Benutzerverwaltung, Vergabe von unterschiedlichen Zugriffsrechten
	Datenintegrität	z. B. verlustfreie Restart- und Recoveryverfahren, eindeutige Zuordnung von Indizes zu Dokumenten
Beschreibung der relevanten Prozesse	Scannen	z. B. vollständiger Ablauf des Scanvorgangs, Qualitätssicherung, Erstellung von Journalen, Aussonderung von im Original aufzubewahrenden Dokumenten
	Erfassung von originär digitalen Dokumenten	z. B. Ablauf des Erfassungsverfahrens, Charakter der zu erfassenden Dokumente, Aufbewahrungsfristen
	Transport im System	Beschreibung des Datenflusses, der Vorbeugung gegen Datenverlust, Konsistenzsicherung
	Indizierung und Datenbank	Konfiguration der Datenbank, vollständiger Ablauf des Indizierungsprozesses, Zugriffssicherungsverfahren
	Archivierung	vollständiger Ablauf des Archivierungsprozesses, Formate und Verfahren der Speicherung von Dokumenten, Standards
	Visualisierung und Reproduktion	Möglichkeiten der Reproduktion einschließlich deren Formate und Qualität, Qualitätsmaßstab
	Protokollierung	z. B. Login und Nutzungsjournale, Auswertung, Archivierung und Retrieval der Journale
	Sonstige Bestandteile und Anlagen	
	Verzeichnis der gültigen technischen Dokumentationen,	

© PROJECT CONSULT GmbH 2002

Bestandteile einer Verfahrensdokumentation für DMS- und Archivsysteme zur Speicherung kaufmännischer		
	Handbücher etc.	
	Betriebsvoraussetzungen	z. B. Pflege, Wartung, Medien- und Datensicherung
	Betreiberdokumentationen	z. B. Betriebskonzept
	Anbieterdokumentationen	z. B. Systemdesign, Dokumentation der eingesetzten Tools wie Recovery, Restart, etc.
	Vertragsrelevante Dokumentationen	z. B. Wartungsvertrag, Abnahmeerklärung
	Arbeitsanweisungen	z. B. Wartung, Scanvorgang mit Vor- und Nachbereitung, Ändern und Löschen von Indizes, Fehlerbehandlung, Notfallmaßnahmen
	Migration	z. B. Migrationsfähigkeit des Systems, Migration der Datenbank
	Aktuell eingestellte Parameter, Benutzerberechtigungen und Dokumentenklassen mit Aufbewahrungsregeln und Aufbewahrungsfristen	
Test- und Abnahmeprotokolle		

Literaturverzeichnis

Der vorliegenden Artikel orientiert sich an folgenden Quellen:

- **Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)**, Bundesministerium der Finanzen, Bundessteuerblatt Nr. 18**,** 45. Jahrgang, Bonn, 14. Dezember 1995
- **Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)**, BMF-Schreiben vom 16. Juli 2001
- **Gesetz zur Senkung der Steuersätze und zur Reform der Unternehmensbesteuerung (Steuersenkungsgesetz-StSenkG),** Bundesgesetzblatt Teil 1 Nr. 46**,** ausgegeben zu Bonn am 26. Oktober 2000
- **Restart, Recovery und Konsistenzsicherung von elektronischen Archivsystemen** von Dr. Ulrich Kampffmeyer, PROJECT CONSULT GmbH (überarbeitete Mitschrift des Vortrages am 13.11.1995), erschienen in VOI NEWS, Ausgabe 1/96, Februar 1996, 4. Jahrgang
- **Anforderungen an Verfahrensbeschreibungen für Archivsysteme mit digitalen optischen Speichern** von Dr. Ulrich Kampffmeyer, PROJECT CONSULT GmbH, VOI Kompendium Band 2, Rechtsinitiative, Juni 1996
- **Grundsätze der Verfahrensdokumentation nach GoBS „Code of Practice“ zur revisionssicheren Archivierung**, VOI-Schriftenreihe Kompendium Band 4, Karl-Georg Henstorf, Dr. Ulrich Kampffmeyer, Jan Prochnow; 1999
- **Grundsätze der elektronischen Archivierung „Code of Practice“ zum Einsatz von Dokumenten-Management- und elektronischen Archivsystemen**, VOI-Schriftenreihe Kompendium Band 3, Dr. Ulrich Kampffmeyer, Jörg Rogalla; 1997

© PROJECT CONSULT GmbH 2002