PRAXIS
WissenDatenVisionen2017

Herstellererklärung

GoBD mit der WDV 2017
Version 11.03-01-37NET

inkl. Unternehmenscheckliste

Version 1.0 vom 11.11.2017

TÜV PROFI CERT 70 900 503

TÜV PROFI CERT 70 900 503

ICH BIN HILFREICH.

Produktinformationen	
Beschreibung	**Herstellererklärung GoBD**
Abteilung	Dokumentation
Verfasser	Beate Volkmann
Version	1.00
Erstelldatum	11.11.2017

Versions-Änderungsliste

Version	Ersteller	Änderungsdatum
1.0	Beate Volkmann - Erstellung	11.11.2017

PRAXIS
EDV- Betriebswirtschaft- u. Software Entwicklung AG
Lange Str. 35
99869 Pferdingsleben (Thüringen)

Tel.: +49 (0) 36258 - 566-0
Fax: +49 (0) 36258 - 566-40
E-mail: info@praxis-edv.de
www.praxis-edv.de

1 Allgemeine Konformitätserklärung

Wir erklären hiermit, dass das Produkt WDV 2017 mit allen Modulen und Zusatzprogrammen (unter der Voraussetzung, dass *PRAXIS* EDV-Betriebswirtschaft und Software-Entwicklung AG Hersteller des jeweiligen Zusatzprogrammes ist) in allen Programmabläufen, Funktionen und Prozessabbildungen, in welchen rechtliche und/oder steuerrechtliche Anforderungen erfüllt werden müssen, den gesetzlichen Vorschriften entspricht.

Als Basis hierfür gelten in der jeweils gültigen Fassung für Deutschland, soweit sie die Buchführung betreffen:

1. Handelsgesetzbuch (HGB)
2. Abgabenordnung (AO)
3. Umsatzsteuergesetz (UStG)
4. Grundsätze ordnungsmäßiger DV-gestützter Buchführungssystem (GoBS) laut Schreiben des deutschen Bundesministeriums der Finanzen vom 7.11.1995
5. Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) laut Schreiben des deutschen Bundesministeriums der Finanzen vom 14.11.2014

In Ergänzung der gesetzlichen Vorschriften, unterliegt die Herstellung von Software-Erzeugnissen den allgemeinen Qualitätsstandards der PRAXIS EDV-Betriebswirtschaft und Software-Entwicklung AG, im speziellen der DIN EN ISO 9001 sowie den Richtlinien nach ITIL – IT Infrastructure Library.

Die im Rahmen unseres Qualitätsmanagements definierte Prüfung auf Ordnungsmäßigkeit unserer Softwareprodukte entspricht den Vorgaben und Regularien gemäß IDW PS 880.

Die obigen Regelungen setzen Qualitätsstandards der eingesetzten Software implizit voraus: Qualität der Dokumentation und Funktionalität (über Entwicklung, Installation, Vorhandensein und Korrektheit von Funktionen) und die Zuverlässigkeit und Sicherheit der Programme und Daten.

Die Zertifizierungsstelle des TÜV Hessen ist akkreditiert, mit der Marke TÜV PROFICERT Managementsysteme in Unternehmen nahezu aller Branchen zu zertifizieren. Wir haben uns von diesem Institut prüfen lassen und dürfen das Zertifikat TÜV PROFICERT für unsere integrierte Archivierung WDV als Ergänzung zu unserem bestehenden Zertifikat nach der Norm DIN EN ISO 9001 tragen.

Als Microsoft Silver Independent Software Partner haben wir für die WDV eine ISV-Zertifizierung erlangt, die die Kompatibilität der WDV auf verschiedenen Microsoft Plattformen sowie aktuellen Server- und Office-Lösungen bestätigt und sicherstellt.

In Ergänzung zu dieser Konformitätserklärung gelten unsere Allgemeinen Geschäfts-bedingungen in der jeweils aktuellen Form.

2 Vorbemerkungen zur Herstellererklärung

Seit 01.01.2017 sind sämtliche Unternehmen in Deutschland verpflichtet, Ihre Buchführung nach den Regelnd der GoBD zu führen.

Die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ – kurz GoBD umfassen zahlreiche Vorgaben zur Buchführung sowie der Aufbewahrung von Daten und Belegen.

Die Grundsätze beziehen sich auf die Buchführung inklusive der dazu gehörigen Datenverarbeitungssysteme (Haupt-, Vor- und Nebensysteme).
Konkret bedeutet dies, dass eine kaufmännische Software herangezogen wird, um steuerlich relevante Dokumente, Dateien, Geschäftsvorfälle und Belege bereitzustellen.

Aufbewahrungspflichtig sind neben Unterlagen in Papierform alle weiteren Unterlagen wie Daten, Datensätze und elektronische Dokumente.
Alle Unternehmensbereiche, in denen betriebliche Abläufe digital ausgeführt werden, werden in eine Prüfung mit einbezogen. Sämtliche buchhalterischen Aufzeichnungen und Unterlagen, die zum Verständnis und zur Überprüfung für die Besteuerungen dienen, müssen lückenlos, transparent und nachvollziehbar sein. Dies gilt auch für historische Geschäftsvorfälle.

Die WDV 2017 gehört in dieser Klassifizierung zu den sog. „Vorsystemen“, wobei auf die integrierte Archivierung als wesentlicher Erfüllungsbestandteil der GoBD ein wesentlicher Focus zu legen ist.

Für Ihre Sicherheit

Da es keine konkreten Vorgaben oder Zertifikate durch die Finanzbehörden gibt, unterziehen wir Archivierung der WDV regelmäßig einer Prüfung durch den TÜV, um höchstmögliche Sicherheit für die GoBD-Konformität zu schaffen.

Die WDV 2017 mit der Archivierung ermöglicht die sichere Aufbewahrung der relevanten Daten und schützt diese vor Manipulation. So ist die lückenlose Nachvollziehbarkeit der über die WDV 2017 erfassten Geschäftsvorfälle garantiert.

Die vorliegende Herstellererklärung beschreibt die Aspekte zur Umsetzung der GoBD mit der WDV und weist zusätzlich auf wichtige betriebliche Aufgaben hin. In Ergänzung hierzu erhalten Sie eine Checkliste sowie eine Muster-Verfahrensanweisung als Leitfaden an die Hand.

Bitte beachten Sie, dass diese Herstellererklärung ausschließlich ein kleiner Bestandteil Ihrer GoBD-Dokumentation darstellt und dafür vorgesehen ist, in Ihre individuellen Unternehmens-Prozessbeschreibungen und Verfahrensdokumentationen integriert zu werden.

Pferdingsleben, November 2017

Uwe Wirth
Vorstand

Beate Volkmann
Vorstand

Inhaltsübersicht

3 Überblick und rechtliche Grundlagen

3.1 Über PRAXIS

Die *PRAXIS* EDV-Betriebswirtschaft- und Software-Entwicklung AG wurde 1990 in Gotha / Thüringen gegründet und hat seit 1995 seinen Sitz in Pferdingsleben im Landkreis Gotha. Seit Frühjahr 2001 trägt das Unternehmen in die Rechtsform AG.

Wir sind Hersteller von Software- Lösungen und Anwendungen für Unternehmen der Steine- und Erden-, Schüttgut- und Baustoff- Industrie für den gesamten deutschsprachigen Raum.

Spezialisiert sind unsere Anwendungen auf

- das klassische CRM und ERP Geschäft für diese Branchenbereiche,
- integrierte kaufmännische Prozesse wie Vertrieb, Abrechnung, Controlling, Dokumentenmanagement und Archivierung, Mesonic Finanzbuchhaltung,
- Logistik- Lösungen für optimale Baustoffversorgung der Baustellen,
- Entwicklung und Integration spezifischer Module auf Basis firmApp Technologie,
- integrierte technische und technologische Lösungen im Waagen-, Anlagen, und Steuerungs- und Logistikbereich.

In unserem Unternehmen sind durchschnittlich 30 Mitarbeiter beschäftigt. Die Software-Entwicklung unserer Produkte erfolgt im eigenen Hause, ebenso der Vertrieb sowie die Software- Wartung und erforderliche Service- Leistungen.

Mit über 2000 Anwendern in Deutschland, Österreich und der Schweiz sind ist die Branchensoftware WDV in der Schütt-, Veredelungs- und Baustoff-Industrie stark vertreten.
Durch die gesellschaftliche Integration in der BSM Business Software für den Mittelstand eG erweitert das Systemhaus elementar mit über 200 Fachkräften in den unterschiedlichsten Spezialbereichen die Kompetenz bundesweit. Im April 2014 wurde das Kompetenz-Center mit der SMC Software GmbH aus München für den bayrischen und österreichischen Markt gegründet.

3.2 Zielsetzung und Anwendungsbereich der Herstellererklärung

- Die vorliegende Herstellererklärung beschreibt Aspekte zur Umsetzung, wie die Behandlung der GoBD in der WDV 2017 mit integrierter Archivierung berücksichtigt ist.

- Bitte beachten Sie, dass Sie mittels einer individuellen Verfahrensdokumentation Ihre unternehmensinternen Verfahren und Maßnahmen beschreiben müssen, die für die Belegablage von handels- und/oder steuerrechtlichen Belegen in Ihrem Unternehmen gelten.

- Diese Ausarbeitung basiert auf der Struktur der GoBD-Checkliste für Dokumenten-management-Systeme des Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom)

3.3 Rechtliche Grundlagen

- Die Aufbewahrungsfrist von Belegen beträgt 10 Jahre für Handelsbücher, Inventare, Lage-berichte, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsan-weisungen und sonstigen Organisationsunterlagen, Belege für Buchungen in den vom Kaufmann nach § 238 Abs. 1 HGB zu führenden Büchern (Buchungsbelege), vgl. § 257 Abs. 4 i.V.m. § 257 Abs. 1 Nr. 1, 4 HGB, § 147 Abs. 3 i.V.m. § 147 Abs. 1 Nr. 1, 4, § 5 AO.

- Nach § 14b UStG sind ein Doppel aller ausgestellten Rechnungen sowie alle erhaltenen Rechnungen aufzubewahren. Dabei sind gem. § 14 Abs. 1 S. 2 ff. UStG die Echtheit der Herkunft, die Unversehrtheit ihres Inhalts und ihre Lesbarkeit über den gesamten Aufbewahrungszeitraum sicherzustellen und durch ein einzurichtendes innerbetriebliches Kontrollverfahren zu gewährleisten.

- Die Aufbewahrungsfrist von Belegen beträgt 6 Jahre für empfangene Handels- oder Geschäftsbriefe und Wiedergaben der abgesandten Handels- oder Geschäftsbriefe und sonstige Unterlagen, vgl. § 257 Abs. 4 i. V. m. § 257 Abs. 1 Nr. 2,3 HGB, § 147 Abs. 3 i. V. m. § 147 Abs. 1 Nr. 2, 3, 5 AO. Handelsbriefe sind nur Schriftstücke, die ein Handelsgeschäft betreffen (§ 257 Abs. 2 HGB).

- Belege, welche nicht ausschließlich in digitaler Form aufbewahrt werden dürfen, insbesondere auch Eröffnungsbilanzen und Abschlüsse gem. § 147 Abs. 2 AO sowie ggf. Zollbelege gem. § 147 Abs. 2 i.V.m. Abs. 1 Nr. 4a AO, müssen und werden - auch im Falle einer zusätzlichen Digitalisierung - im Original aufbewahrt.

- Die Aufbewahrungspflicht beginnt – auch bei abweichenden Wirtschaftsjahren - mit dem Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Handelsbuch gemacht, das Inventar aufgestellt, der Handelsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist (§ 257 Abs. 5 HGB, § 147 Abs. 4 AO).

- Die Aufbewahrungsfrist läuft gem. § 147 Abs. 3 Satz 3 AO dann nicht ab, soweit und solange die Unterlagen für Steuern von Bedeutung sind, für welche die Festsetzungsfristen (ein oder vier Jahre, § 169 Abs. 2 Satz 1 AO) noch nicht abgelaufen ist. Die Regelung der Ablaufhemmung des § 171 AO wird bei der Bestimmung der Fristdauer berücksichtigt.

- Es muss davon ausgegangen werden, dass die Finanzverwaltung die Anschaffungsbelege für abnutzbare Wirtschaftsgüter gem. GoBD, Absatz. 81, als Ursprungsbelege für sogenannte „Dauersachverhalte“ (AfA-Buchungen auf Basis der AfA-Bemessungsgrundlage) wertet. Weil die Finanzverwaltung insofern die Anschaffung und die Abschreibungen als einen wirtschaftlichen Geschäftsvorfall interpretiert, sollten die Anschaffungsbelege zur Risikovermeidung über den gesamten Zeitraum der Abschreibung aufbewahrt werden. Maßgeblich für die Berechnung der Aufbewahrungsfrist ist bei dieser Interpretation das letzte Jahr der Abschreibung.

- Alle aufbewahrungspflichtigen Unterlagen, zu denen auch die Belege gehören, sind systematisch, vollständig, zeitgerecht und geordnet im Sinne der allgemeinen Ordnungsmäßigkeitsanforderungen der GoBD abzulegen und unverändert aufzubewahren. Das gilt auch beim Einsatz von IT und auch für digitale oder digitalisierte Belege (vgl. auch GoBD, Absatz. 22 ff.). Bei der Führung der Bücher und Aufzeichnungen sowie der Aufbewahrung von Unterlagen wird die Form der Aufbewahrung, soweit die GoB beachtet werden, allerdings nicht konkret vorgeschrieben (§§ 238 Abs. 2, 257 Abs. 3 HGB, § 146 Abs. 5 AO, § 147 I Abs. 2 AO). Somit muss im konkreten Einzelfall ein Verfahren konzipiert, dokumentiert, umgesetzt und überwacht werden, das alle handels- und steuerrechtlichen Anforderungen an die Belegablage erfüllt. Dieses Verfahren muss den gesamten Workflow (Arbeitsablauf) von der Belegentstehung bzw. vom Belegeingang und dessen Identifikation über die geordnete und sichere Ablage bis zum Ablauf der Aufbewahrungsfristen umfassen.

- Mittels einer unternehmensinternen Verfahrensdokumentation muss eine geordnete und sichere Belegablage dokumentiert und durch deren dauerhaften und ununterbrochenen Einsatz im Unternehmen sichergestellt werden. Das umfasst sowohl konventionelle

Papierbelege als auch digitale oder digitalisierte Belege, so dass darauf innerhalb einer angemessenen Frist ein Zugriff und eine Lesbarkeit bzw. Lesbarmachung möglich ist (§ 257 Abs. 3 HGB, § 147 Abs. 2 AO) sowie ein Datenzugriff durch die Finanzverwaltung im Falle einer Außenprüfung gewährleistet werden kann (§ 147 Abs. 6 AO).

- Die Lesbarmachung muss bei den empfangenen Handelsbriefen und den Buchungsbelegen dabei zu einer bildlichen und bei den anderen Unterlagen zu einer inhaltlichen Übereinstimmung mit dem Original führen und während der Dauer der Aufbewahrungsfrist verfügbar sein.

- Entgegen den handelsrechtlichen Regelungen bestimmt das Steuerrecht, dass die Belege im Geltungsbereich des Gesetzes, also im Inland, aufzubewahren sind (§ 146 Abs. 2 AO). Lediglich mit Zustimmung der Finanzverwaltung kann – nach schriftlichem Antrag des Steuerpflichtigen (§ 146 Abs. 2a AO) – eine Verlagerung in das Ausland erfolgen. Im Antrag ist der Aufbewahrungsort zu benennen. Für elektronische Rechnungen ist grundsätzlich eine Aufbewahrung im Gemeinschaftsgebiet (§ 1 Abs. 3 UStG) zulässig (§ 14b Abs. 2 UStG).

- Werden elektronische Dokumente mittels einer „Cloud-Lösung“ aufbewahrt, sollte daher darauf geachtet werden, dass der Standort der Rechner im Inland liegt oder zumindest bekannt ist, damit der erforderliche Antrag gestellt werden kann, wenn der Standort nicht im Inland liegt (§ 146 Abs. 2a AO).

- Bei der Wahl der Aufbewahrungsart und des Aufbewahrungsortes muss beachtet werden, dass die Unterlagen ausreichend gegen Verlust oder Untergang geschützt sind.

Wichtiger Hinweis:

Bitte beachten Sie, dass die *PRAXIS* EDV-Betriebswirtschaft- und Software-Entwicklung AG nicht zur steuerlichen Beratung befugt ist. Bitte betrachten Sie diese Dokumentation als Leitfaden, welcher für Ihr Unternehmen entsprechend konkretisiert und ergänzt werden muss!

Die Ausarbeitung erhebt keinen Anspruch auf steuerliche oder rechtliche Vollständigkeit. Sie basiert auf dem BMF-Schreiben vom 14.11.2014 sowie auf den resultierenden Regelwerken sowie den aufgeführten Literatur- und Quellnachweisen.

3.4 Relevante Unterlagen mit Belegfunktion

- Gegenstand der Belegablage sind alle originär in Papierform oder in digitaler Form eingehenden oder entstandenen bzw. vorliegenden Dokumente und Daten, die eine Belegfunktion im Sinne der handels- und/oder steuerrechtlichen Buchführungs- oder Aufzeichnungspflichten erfüllen und deshalb einer Aufbewahrungspflicht unterliegen.

- Auf eine vollständige Aufzählung der relevanten Belege muss aufgrund deren Vielfalt ebenso verzichtet werden wie aufgrund der Tatsache, dass die Bezeichnung eines Dokuments alleine nicht ausschlaggebend dafür ist, ob es eine Belegfunktion erfüllt oder nicht. Typische Dokumente mit Belegcharakter sind: Angebote, Aufträge, Lieferscheine, Eingangsrechnungen, Ausgangsrechnungen, Bar-Lieferscheine, Quittungen, Kontoauszüge, Verträge, Urkunden, Geschäftsbriefe, Einzahlungs- und Auszahlungsbelege.

- Wird in einem (Fremd- oder Eigen-)Beleg auf andere Unterlagen verwiesen, um den Buchungsvorfall verständlich zu machen, so gehören diese Unterlagen zwingend ebenfalls zu dem Beleg.

4 TÜV-Zertifikat der Integrierten Archivierung WDV 2017

TÜV PROFI CERT

ZERTIFIKAT

für

Integrierte Archivierung

Die Anforderungen hierfür sind in einem Kriterienkatalog für Systeme und Prozesse formuliert und die Konformität wurde in einem Audit überprüft. Dieses Zertifikat ist kein Nachweis für die Erfüllung aller gesetzlicher Vorschriften und / oder Produkteigenschaften.

PRAXIS
EDV- Betriebswirtschaft- und Software- Entwicklung AG

Lange Straße 35
D-99869 Pferdingsleben

Geltungsbereich:

Archivierung und Dokumentenmanagementsystem
in der Workflow Anwendung

Zertifikat-Registrier-Nr. **70 900 503** Zertifikat gültig von 2015-10-27 bis **2018-10-26**

Auditbericht-Nr. 4290 4680

TÜV HESSEN

Darmstadt, 2015-06-08
Zertifizierungsstelle des TÜV Hessen
– Der Zertifizierungsstellenleiter –

SEITE 1 VON 1.
Diese Zertifizierung wurde gemäß TÜV PROFiCERT-plus-Verfahren durchgeführt und wird regelmäßig überwacht.
Die aktuelle Gültigkeit ist nachprüfbar unter www.tuev-club.com. Originalzertifikate enthalten ein aufgeklebtes Hologramm.
TÜV Technische Überwachung Hessen GmbH, Rüdesheimer Str. 119, D-64285 Darmstadt, Tel. +49 6151/600331 Rev-DE-1301

5 Allgemeine Anforderungen der GoBD

Im BMF Schreiben vom 14.11.2014 werden die Allgemeinen Anforderungen für den Einsatz der GoBD unter Absatz 3 definiert.

- Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit (Absatz 3.1),

- Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung (Absatz 3.2)
  Diese spezifiziert bzw. untergliedert in folgende Unterpunkte:

  - Vollständigkeit (Absatz 3.2.1)
  - Richtigkeit (Absatz 3.2.2)
  - Zeitgerechte Buchungen und Aufzeichnungen (Absatz 3.2.3)
  - Ordnung (Absatz 3.2.4)
  - Unveränderbarkeit (Absatz 3.2.5)

Diese formulierten Anforderungen sollen sicherstellen, dass die Geschäftsvorfälle in der Buchhaltung vollständig, korrekt und nicht manipulierbar abgebildet werden und für die Dauer der gesetzlichen Aufbewahrungsfristen gewährleistet ist, dass diese ebenfalls vollständig nachvollziehbar sind.

Hieraus resultiert letztlich eine Vielzahl von Vorgaben, die von den Unternehmen erfüllt werden müssen.

5.1 Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit

Die Verarbeitung der einzelnen Geschäftsvorfälle sowie das dabei angewandte Buchführungs- oder Aufzeichnungsverfahren müssen nachvollziehbar sein. Die Buchungen müssen – wie bereits in der Vergangenheit auch – durch Belege nachgewiesen werden.
Die Aufzeichnung muss so erfolgen, dass eine progressive und retrograde Prüfbarkeit ermöglicht wird – d.h. dass einen sachverständiger Dritter (z.B. Betriebsprüfer) innerhalb angemessener Zeit die Geschäftsvorfälle in Entstehung und Abwicklung lückenlos nachvollziehbar sind.

Die progressive Prüfung beginnt beim Beleg, geht über die Grund(buch)aufzeichnungen und Journale zu den Konten, danach zur Bilanz mit Gewinn- und Verlustrechnung und schließlich zur Steueranmeldung bzw. Steuererklärung. Die retrograde Prüfung verläuft umgekehrt. Die progressive und retrograde Prüfung muss für die gesamte Dauer der Aufbewahrungsfrist und in jedem Verfahrensschritt möglich sein.

Die Nachprüfbarkeit der Bücher und sonst erforderlichen Aufzeichnungen erfordert eine aussagekräftige und vollständige **Verfahrensdokumentation**, die sowohl die aktuellen als auch die historischen Verfahrensinhalte für die Dauer der Aufbewahrungsfrist nachweist und den in der Praxis eingesetzten Versionen des DV-Systems entspricht.

Die Nachvollziehbarkeit und Nachprüfbarkeit muss für die Dauer der Aufbewahrungsfrist gegeben sein. Dies gilt auch für die zum Verständnis der Buchführung oder Aufzeichnungen erforderliche Verfahrensdokumentation.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Jede Erfassung in die Archivierung (Import, Scan, automatische Beleg-Ausgangs-Archivierung der von der WDV selbst erzeugten Belege wie z.B. Angebot / Auftrag / Lieferschein / Rechnung etc.) wird automatisch mit Datum und Uhrzeit, sowie dem Archiv-Nutzer im Archiv registriert und über die Beschlagwortung dokumentiert

- ✓ Jede Änderung ist nachvollziehbar über eine vollständige Versionierung der Dokumente; d.h. Änderungen werden in einer neuen Dokumentenversion mit Angabe von Datum / Zeit / Archiv-Nutzer gespeichert; das ursprüngliche Dokument bleibt unverändert bestehen – damit sind frühere Inhalte immer nachvollziehbar

- ✓ Es ist während der gesamten Aufbewahrungszeit die verlust- und fälschungssichere Aufbewahrung gemäß der gesetzliche vorgeschriebenen Aufbewahrungsfristen der Dokumente gewährleistet – unter Vorbehalt, dass der Anwender für den Fall eines technischen Defekts für Datensicherungen sorgt (siehe Punkt 6)

- ✓ Die WDV verwendet für die Belegarchivierung der steuerlich relevanten Daten geeignete Datenformate und Verfahren, so dass die Lesbarkeit der Dokumente für die Aufbewahrungsfrist gewährleistet ist.

- ✓ Manuelle Eingriffe auf die WDV- und Archiv-Datenbank vom Archiv-Benutzer sind ausgeschlossen; sämtliche Archivdokumente sind verschlüsselt und manipulationssicher gespeichert

b) Was gehört in Ihre DMS-Dokumentation bzw. Verfahrensanweisung

- ✓ Vollständige Dokumentation der individuellen System-Einrichtung sowie der Benutzerberechtigungen der WDV-Archivierung in Ihrem Hause; Erstellung einer Prozessbeschreibung und Verfahrensdokumentation, welche den Einsatz des DMS-Systems in Ihrem Hause dokumentiert (Verweis auf Pt. 9)

- ✓ Verfahrensanweisung zur Vorgehensweise und Dokumentation von Änderungen an Systemeinstellungen mit entsprechenden Freigaben durch berechtigte / verantwortliche Personen

- ✓ Implementierung von Regelungen zur Prüfung / Definition eines IKS (internes Kontrollsystem) für eine schnelle Behebung von technischen Fehlern im Störungsfall sowie zur Behandlung von ggf. sicherheitsrelevanten Vorfällen

Wichtig:
Sofern Sie den Service von PRAXIS beauftragen, eine Änderung Ihrer Systemeinstellungen durchzuführen, so ist diese Änderung in Ihrer Dokumentation mit entsprechender Änderungsverfolgung aufzunehmen. Änderungen von Einstellungen oder Berechtigungen werden nicht automatisch von der WDV protokolliert.

5.2 Grundsatz der Wahrheit, Klarheit und fortlaufenden Aufzeichnung

5.2.1 Vollständigkeit

Die Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen (Grundsatz der Einzelaufzeichnungspflicht). Eine vollzählige und lückenlose Aufzeichnung von Geschäftsvorfällen ist auch dann gegeben, wenn zulässigerweise nicht alle Datenfelder eines Datensatzes gefüllt werden.

Bezogen auf ein DMS betrifft der Grundsatz die lückenlose Erfassung aller rechnungsrelevanten Dokumente und Daten.

Die vollständige und lückenlose Erfassung und Wiedergabe aller Geschäftsvorfälle ist bei DV-Systemen durch ein Zusammenspiel von technischen (einschließlich programmierten) und organisatorischen Kontrollen sicherzustellen (z. B. Erfassungskontrollen, Plausibilitäts-kontrollen bei Dateneingaben, inhaltliche Plausibilitätskontrollen, automatisierte Vergabe von Datensatznummern, Lückenanalyse oder Mehrfachbelegungsanalyse bei Belegnummern).

Vollständigkeit und Lückenlosigkeit sind insbesondere mit Blick auf etwa vorhandene Schnittstellen von zentraler Bedeutung. Neben der Vollständigkeit von angelieferten Daten- und Dokumentbeständen geht es auch um vollständige Dokumente an sich, bspw. E-Mails inklusive der dazugehörigen Anhänge sowie um eine vollständige Indizierung von Dokumenten.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Die in der WDV erstellten (Ausgangs-) Belege werden automatisch in die Archivierung eingebracht; d.h. Angebote, Aufträge, Lieferscheine und Rechnungen sowie Rechnungsausgangsbücher zur Protokollierung der Datenübergabe an die Finanzbuchhaltung werden automatisch archiviert

- ✓ Entsprechende Prüflisten stellt die WDV bereit (z.B. Prüfliste „Lieferscheinversionen im Archiv“, COLD-Protokoll…); zusätzliche Prüflisten können auf Bedarf nach vorheriger Abstimmung erstellt werden

- ✓ Sämtliche Dokumente werden vollständig mit ALLEN enthaltenen Daten und Layouts ins Archiv eingestellt, so dass auch bei Stammdatenänderungen der jeweilige Original-Beleg beim Abruf aus dem Archiv ausgegeben wird. Ebenso verhält es sich mit Layout-Änderungen (Hintergrund), sofern sich über die Zeit der Briefbogen ändert. Damit ist sichergestellt, dass ein Dokument immer auf Basis der historischen Daten auf dem richtigen Briefbogen ausgegeben wird.

- ✓ Bei einer möglichen Übernahme von Dokumenten aus Fremdsystemen wird im Rahmen der Schnittstellenübergabe ein entsprechende Prüfprotokoll erstellt, anhand von welchem die vollständige und lückenlose Übernahme von Dokumenten aus Fremdsystemen nachvollzogen werden kann *(Option bei Schnittstellen)*

- ✓ Belege, die aus der WDV erzeugt werden, können nicht doppelt erfasst werden; sofern Änderungen an einem bestehenden Beleg vorgenommen werden, der bereits im Archivsystem vorhanden ist, wird für dieses Dokument eine neue Dokumentenversion erstellt. Damit kein z.B. keine Rechnungsnummer oder kein Lieferschein doppelt in der Archivierung vorhanden sein.

- ✓ Dokumente können in der WDV Archivierung vom Anwender nicht gelöscht werden

- ✓ Die Löschung von Daten nach Ende der Aufbewahrungsfrist (älter als 11 Jahre bzw. in Einzelfällen unter Berücksichtigung von längeren Aufbewahrungsfristen) erfolgt ausschließlich im 4- Augen Prinzip in Zusammenwirken mit einem Projekt-Ingenieur von PRAXIS nach vorheriger Abstimmung und Freigabe durch eine verantwortliche Person (Geschäftsleitung) des Anwenders

b) Was gehört in Ihre DMS-Dokumentation bzw. Verfahrensanweisung

- ✓ Erstellung einer Verfahrensanweisung zur Vorgehensweise bei manuellen Belegerfassungen oder Übernahme von Daten über Schnittstellen aus Fremdsystemen in die WDV-Archivierung.

- ✓ Definition von organisatorischen Regelungen zur Prüfung der Vollständigkeit (z.B. regelmäßige Prüfung, ob Anlieferungen von Fremdsystemen komplett verarbeitet wurden)

- ✓ Nutzung der Archiv-Suche als DMS-Funktion zur Kontrolle, ob Inhalte von bestimmten Indexfeldern / Beschlagwortungsfeldern eines Datenbestands lückenlos befüllt wurden.

- ✓ Implementierung eines übergreifenden Konzepts im Rahmen des internen Kontrollsystems (IKS) zur Sicherstellung der vollständigen und lückenlosen Erfassung.
  Von den hier genannten (und ggf. anderen) organisatorischen und/oder technischen Maßnahmen müssen die geeigneten ausgewählt und passend kombiniert werden

5.2.2 Richtigkeit

Geschäftsvorfälle sind in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften inhaltlich zutreffend durch Belege abzubilden (BFH-Urteil vom 24. Juni 1997, BStBl II 1998 S. 51), der Wahrheit entsprechend aufzuzeichnen und bei kontenmäßiger Abbildung zutreffend zu kontieren.

In diesem Zusammenhang hat das DMS sicherzustellen, dass die Dokumente und Daten den geforderten Grad der Übereinstimmung mit dem Original aufweisen – d.h. bildlich und inhaltlich müssen die Dokumente und Daten übereinstimmen. Die Belege dürfen nicht verloren gehen oder verfälscht werden.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Sämtliche von der WDV erzeugten Belege werden, wie bereits unter Punkt 5.2.1 aufgeführt, vollständig mit allen Original-Daten und dem Original-Layout archiviert.

b) Was gehört in Ihre DMS-Dokumentation bzw. Verfahrensanweisung

- ✓ Implementierung eines übergreifenden Konzepts im Rahmen des Internen Kontrollsystems (IKS) zur Sicherstellung der korrekten Erfassung (z. B.: Regelwerk für die Beschlagwortung / Indizierung von Dokumenten).
- ✓ Von den im IKS genannten (und anderen) organisatorischen und/oder technischen Maßnahmen müssen die geeigneten ausgewählt und passend kombiniert werden.
- ✓ In der Verfahrensanweisung ist eine entsprechende Fehlerbehandlung für fehlerhafte und unleserlich erfasste Seiten sowie fehlerhafte Dokumente und Dateien definiert sein sowie ein Regelprozess zum Umgang mit diese Daten festgelegt werden.

Weiterführende Verweise – siehe Punkt 7

- ⇨ Erfassung und Verarbeitung im DMS
- ⇨ Eingangsschnittstellen
- ⇨ Erfassung Fremdbelege über Scanner

5.2.3 Zeitgerechte Buchungen und Aufzeichnungen

Die zeitgerechte Buchung und Aufzeichnung betrifft in erster Linie die Buchhaltungsprogramme; das BMF Rundschreiben gibt vor, dass *jeder Geschäftsvorfall zeitnah d.h. möglichst unmittelbar nach seiner Entstehung in einer Grundaufzeichnung oder in einem Grundbuch zu erfassen ist* (Absatz 46), jedoch wird nicht jede Zeitspanne als bedenklich aufgeführt (Absatz 47) – *eine Erfassung von unbaren Geschäftsvorfällen innerhalb von zehn Tagen ist unbedenklich (vgl. BFH-Urteil vom 2. Oktober 1968, BStBl 1969 II S. 157; BFH-Urteil vom 26. März 1968, BStBl II S. 527 zu Verbindlichkeiten und zu Debitoren)….*
Bei zeitlichen Abständen zwischen der Entstehung eines Geschäftsvorfalls und seiner Erfassung sind daher geeignete Maßnahmen zur Sicherung der Vollständigkeit zu treffen.

Aus Sicht des DMS bedeutet die Anforderung nach Zeitgerechtheit, dass die Archivierung der Dokumente und Daten zum frühestmöglichen Zeitpunkt erfolgt, um mögliche Verluste und Manipulationen vor der Archivierung auszuschließen. Dies betrifft zum einen organisatorische Vorkehrungen, um zu archivierende Dokumente und Daten rechtzeitig dem Archivierungsprozess zuzuführen.

Generell ist diese Anforderung eher eine Aufgabe der allgemeinen Organisation und/oder der Gestaltung der ERP- und Fachsysteme. **Hier sind speziell Themenbereiche der WDV wie z.B. der Eingangsrechnungsworkflow mit PxFlow involviert**

Der Eingangsrechnungsworkflow überbrückt den Zeitraum nach physikalischem Eingang der Rechnung und tatsächlicher Verbuchung in der Finanzbuchhaltung, in dem das Dokument sofort nach Eingang gescannt und damit in das Archivsystem überführt wird. Für den Zeitraum der Rechnungskontrolle (zeitgesteuerter Workflow) ist das Dokument bereits unveränderbar im Archivsystem vorhanden – und die tatsächliche Buchung in der Buchhaltung erfolgt dann erst mit abgeschlossener Rechnungsprüfung. Damit ist die Anforderung nach Belegsicherung / Sicherung der Unverlierbarkeit eines Dokuments gewährleistet.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Die Archivierung in Verbindung mit dem PxFlow – Eingangsrechnungsworkflow stellt die zeitgerechte Überführung des Eingangsdokuments sicher; über die zeitliche Steuerung der Abarbeitung kann ebenfalls sichergestellt werden, dass die Buchungsübergabe des Datensatzes in die FIBU innerhalb der erforderlichen Zeitspanne erfolgt.

- ✓ Die WDV registriert automatisch Datum und Uhrzeit des Scann Vorgangs eines Eingangsdokumentes für die Archivierung; der Mitarbeiter gibt darüber hinaus das Datum der Rechnung (fachlich korrektes Datum) bei der Archivierung an.

b) Was gehört in Ihre DMS-Dokumentation bzw. Verfahrensanweisung

- ✓ Prozessbeschreibung und Verfahrensanweisung im Umgang mit der Verarbeitung von Eingangsrechnungen; ggf. mittels Einführung des PxFlow – Workflowgesteuerte Eingangsrechnungskontrolle *(optionales Modul in der WDV)*
- ✓ Konkrete Arbeitsanweisung für die Mitarbeiter zur zeitnahen Überführung von Dokumenten
- ✓ Im IKS müssen entsprechende Maßnahmen definiert sein, zur Kontrolle der vorgegebenen Arbeitsanweisung.

5.2.4 Ordnung

Die aufbewahrungspflichtigen Unterlagen müssen geordnet aufbewahrt werden (BMF Rundschreiben Kapitel 3.2.4 – Absatz 53 – 57. Insbesondere dürfen die geschäftlichen Unterlagen nicht planlos gesammelt und aufbewahrt werden.

Zur Gewährleistung der Ordnung bzw. Ordnungsmäßigkeit der Belege muss in einem DMS während der gesamten Aufbewahrungsfrist sichergestellt werden, dass die Dokumente klar strukturiert und jederzeit auffindbar sind. Hierzu zählen sowohl eine eindeutige Nummerierung (Index) wie auch ausreichende Indexstrukturen, die identifizierbar und klassifizierbar sind.

Eine eindeutige Zuordnung zum jeweiligen Geschäftsvorfall muss möglich sein. Hier müssen sowohl die retrograde wie auch die progressive Prüfbarkeit gewährleistet sein. Der Erhalt der Verknüpfung zwischen Geschäftsvorfall, Index und Dokument muss während der gesamten Aufbewahrungsfrist gegeben sein.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Mit Archivierung eines Ausgangs-Beleges wird dieser automatisch an den jeweiligen Datensatz der WDV angehangen – also verlinkt bzw. „verknüpft“.
- ✓ Sofern die Schnittstelle der Finanzbuchhaltung dies unterstützt, kann auch ein Archiv-Link an die Buchhaltung übergeben werden, so dass direkt aus dem FIBU- Buchungssatz heraus auf den Archivbeleg der WDV verlinkt werden kann *(Achtung: Funktion ist im Wesentlichen abhängig von der Schnittstelle bzw. dem Buchhaltungsprogramm)*
- ✓ Die WDV bietet flexible Gruppierungsmöglichkeiten, Dokumentenarten und Beschlagwortungsmasken an, um die elektronischen Ablagestrukturen optimal zu organisieren – d.h. es können zu den unterschiedlichen Dokumenten auch entsprechend angepasste Index-Strukturen vergeben werden.

- ✓ Dokumente werden ebenfalls automatisch in Form von elektronischen Kunden-, Lieferanten-, oder Baustellenakten verwaltet.
- ✓ Alle Ausgangsbelege werden automatisiert nach der vorgegebenen Definition der Masken beschlagwortet unter Verwendung / Zuordnung der jeweiligen Datensätze
- ✓ Bei Eingangsbelegen wird die Indexmaske dahingehend definiert, dass möglichst viele Daten-Konstanten verwendet werden, die der Anwender selektieren kann – und möglichst wenig Freitext verwendet werden muss.
- ✓ Über die verwendeten Datenkonstanten sind sofort Querverbindungen möglich (Suche nach Rechnung findet auch den Kunden / die Baustelle; Suche nach Baustelle findet auch die Rechnung).
- ✓ Es erfolgt eine Plausibilitätsprüfung bei der Eingabe von Datenfeldern, welche ggf. durch individuelles Customizing weitergehend spezifiziert werden können
- ✓ Nutzung von ggf. bereits bestehenden Daten zu eingehenden Dokumenten ist möglich (z.B. ZUGFeRD oder Beschreibungsdatei zum Dokument), muss im Einzelfall abgestimmt werden, da je nach Inhalt der Übermittelten beschreibenden Daten eine Übersetzung der gelieferten Daten erfolgen muss (z.B. Baustellennummer auf der Eingangsrechnung (fremd) entspricht Baustellennummer aus dem eigenen Datenstamm)

b) Was gehört in Ihre DMS-Dokumentation bzw. Verfahrensanweisung

- ✓ Definition der Indexstrukturen (Beschlagwortungsmasken) für die unterschiedlichen Belege – nach den Erfordernissen der buchhalterischen Gegebenheiten
- ✓ Es darf keine individuellen Ablagestrukturen geben; d.h. in der Verfahrensanweisung wird je Dokumententyp die Indexierung / Beschlagwortung einmalig definiert. Für Steuerrelevante Daten sind diese zwingend einzuhalten (Arbeitsanweisung)
- ✓ Im IKS müssen entsprechende Maßnahmen definiert sein, zur Kontrolle der Erfassung – ggf. 4 Augen-Prinzip für Qualitätssicherung

5.2.5 Unveränderbarkeit

Nach dem BMF-Rundschreiben vom 14.11.14 dürfen Buchungen und/ oder die dazugehörigen Dokumente nicht in Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist.

Veränderungen und Löschungen von und an elektronischen Buchungen oder Aufzeichnungen (vgl. Absatz 3 bis 5) müssen daher so protokolliert werden, dass die Voraussetzungen des § 146 Absatz 4 AO bzw. § 239 Absatz 3 HGB erfüllt sind (siehe auch unter 8). Für elektronische Dokumente und andere elektronische Unterlagen, die gem. § 147 AO aufbewahrungspflichtig und nicht Buchungen oder Aufzeichnungen sind, gilt dies sinngemäß.

Das bedeutet für DMS-Systeme, dass Dokumente, die in die Archivierung eingefügt wurden, nicht mehr ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden dürfen. (BMF-Schreiben Punkt 3.2.5 – Absatz 58-60).

Die Unveränderbarkeit muss auch die Historisierung von Meta- und Stammdaten betrachten (z.B. mit dem Dokument archivierte Beschreibungsdaten), so dass die Verknüpfung der Dokumente immer auf den jeweils korrekten Stammdatensatz erfolgt.

Das DMS System muss eine Protokollierung von Veränderungen und Löschungen von und an den Dokumenten und Aufzeichnungen ermöglichen – die Verknüpfung zum Geschäftsvorfall muss erhalten bleiben.

Änderungen sind grundsätzlich möglich und zugelassen, müssen nur nachvollziehbar sein. Die Nachvollziehbarkeit kann durch Hardware, Software oder organisatorische Regelungen erzielt werden.

Ebenfalls muss eine Nachvollziehbarkeit von Änderungen an Systemeinstellungen des DMS gefordert (z.B. Einstellungen der Archivierung, Indexstrukturen, Scan-Profile)

Implementierte Kommentarfunktionen (z.B. elektronische Notizzettel, zugefügte Kommentare aus PxFlow), die zum archivierten Dokument hinzugefügt werden können, dürfen die Nachvollziehbarkeit nicht beeinflussen.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Löschungen von Daten im Archiv sind vollständig ausgeschossen
- ✓ Sämtliche Änderungen von Archiv-Dokumenten werden in neuen Dokument-Versionen vorgenommen, so dass Veränderungen nachvollziehbar sind und über eine Änderungshistorie protokolliert werden
- ✓ Archivierte Beschreibungsdaten bleiben ebenfalls erhalten, genauso wie die Verknüpfung zum Belegdaten- bzw. Stammdatensatz.
- ✓ Über den Jahreswechsel und die damit verbundene jahresbezogene Abgrenzung bleiben die Stammdaten und Belege zum Archiv-Datensatz erhalten, womit die Verknüpfung zum richtigen Datensatz immer gewährleistet ist.
- ✓ Elektronische Notizzettel oder Kommentare werden dem Archivdokument übergeordnet angeheftet und beeinflussen die Nachvollziehbarkeit nicht.

- ✓ Technische Sicherheitsmechanismen zur Vermeidung einer unbefugten Veränderung von archivierten Dokumenten ist gewährleistet durch verschlüsselte Dokumentenablage und Hashwerten
- ✓ Zugriffseinschränkung in Form von Berechtigungssystemen bis zur Dateiebene (z.B. für Dokumente, die dem speziellen Datenschutz unterliegen (Verweis auf die DSGVO) für den Programmzugriff

b) Was gehört in Ihre DMS-Dokumentation bzw. Verfahrensanweisung

- ✓ Dokumentation von Änderungen an den Archiv-Einstellungen (Datenbankpfade, Berechtigungen, Einstellungen, Cold-Profile, Beschlagwortungsmasken)
- ✓ Sofern noch nicht vorhanden, muss eine Arbeitsanweisung erstellt werden, dass Personenkonten-Daten unterjährig nicht geändert werden dürfen; auch wenn es sich lediglich um eine Umfirmierung handelt. Dies sollte im Bereich der Buchhaltung eigentlich nichts neues sein, da eine ordnungsgemäße Abgrenzung der Buchungssätze zum Personenkonto gewährleistet sein muss.
- ✓ Dokumentation des Jahreswechsels – Protokollierung der archivrelevanten Änderungen.
- ✓ Verfahrensanweisung für die Datensicherung / Datenbereinigung von Vorjahresmandanten im Sinne der gesetzlichen Aufbewahrungspflichten
- ✓ Es wird empfohlen, die Archiv-Daten mindestens einmal jährlich mit einer Sicherung der WDV-Datenbank des Wirtschaftsjahres auf einen nicht wiederbeschreibbaren Datenträger zu brennen
- ✓ Zugriffsbeschränkung auf die Archiv-Daten über das Betriebssystem muss mittels administrativer Steuerung der Zugriffsberechtigung geregelt werden
- ✓ Klare Arbeitsanweisung für administrative Nutzer für die Behandlung von Archiv-Daten sowie Datenschutzvereinbarung für besonders schützenswürdige Daten.
- ✓ Im IKS müssen entsprechende Maßnahmen definiert sein, zur Kontrolle der Erfassung – ggf. 4 Augen-Prinzip für Qualitätssicherung

6 Anforderungen an den ordnungsmäßigen IT-Betrieb

6.1 Allgemeine Anforderungen

Nicht nur für die Erfüllung der Anforderungen der GoBD ist ein zuverlässiger, geregelter und nachvollziehbarer IT-Betrieb die Grundlage für einen heutzutage ordnungsmäßigen, störungsfreien Betriebsablauf, genauso wie für den ordnungsmäßigen IT-gestützten Betrieb von Buchführungs- und Aufzeichnungsverfahren.

Die allgemeinen Anforderungen ergeben sich aus dem BMF-Schreiben vom 14.11.17 zur GoBD konkret unter folgenden Punkten:

Punkt 6	Internes Kontrollsystem (IKS) – Absatz 100 - 102
Punkt 7	Datensicherheit – Absatz 103 - 106
Punkt 8	Unveränderbarkeit, Protokollierung von Änderungen – Absatz 107-112

Diese Anforderungen gelten für alle steuerrelevanten Systeme und dienen darüber hinaus der Betriebssicherheit des Unternehmens.

Die GoBD fordern, dass der Steuerpflichtige sein IT-System gegen Verlust (z. B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) zu sichern und gegen unberechtigte Eingaben und Veränderungen (Zugang- und Zugriffskontrollen) zu schützen hat (BMF-Schreiben Punkt 7 – Absatz 103-106.
Werden die Daten, Datensätze und elektronischen Dokumente nicht ausreichend geschützt und können daher nicht mehr vorgelegt werden, so ist die Buchführung nicht mehr ordnungsgemäß

Technische Themenbereiche sind hierbei z.B. Betrieb der Systeme gemäß den Betriebsvoraussetzungen und -bedingungen, Backup, Notfall-Abdeckung, Virenschutz, Restart- und Recovery-Fähigkeit.

Dazu ist ein ordnungsmäßiger IT-Betrieb ergänzend durch organisatorische Maßnahmen, wie Schulung der Mitarbeiter oder Arbeitsanweisungen für Systemadministration zu unterstützen.

Neben den technischen und organisatorischen Maßnahmen sind für einen ordnungsmäßigen IT-Betrieb schließlich auch die Dokumentation von Maßnahmen in Betriebskonzepten, Arbeitsanweisungen, Katastrophenfall (K-Fall)-Regelungen oder die Verfahrensdokumentation von Relevanz.

Die im folgenden aufgeführten Punkte sind durch die IT-Systemadministration bzw. durch die Organisation des Unternehmens zu gewährleisten und betreffen die WDV mit der Archivierung indirekt, da diese zu den schützens- und sicherungsrelevanten Daten gehören.

Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Zur Gewährleistung der Ordnungsmäßigkeit und Nachvollziehbarkeit der fachlichen Prozesse muss eine Definition und Beschreibung der steuerrelevanten, fachbezogenen Prozesse dokumentiert sein (ggf. bereits Bestandteil einer ISO-Zertifizierung oder eines WPK-Handbuchs). Diese Beschreibung betrifft alle IT-Systeme und nicht nur das DMS System.

- ✓ Zur Gewährleistung der Ordnungsmäßigkeit und Nachvollziehbarkeit der IT-Prozesse bedarf es einer Definition und Beschreibung der technischen Prozesse, die einen störungsfreien und verlässlichen Betrieb der Systeme gewährleisten. So z.B. der Prozess der Datensicherung sowie der Wiederanlaufprozess nach Systemstörungen

- ✓ Die Prozess-Dokumentationen des Unternehmens können auch in einen Betriebshandbuch oder QM-Handbuch oder einer anderen Art IT-naher Dokumentation enthalten sein.

- ✓ Es sollten in diesem Rahmen Kenngrößen definiert sein z.B. wie lange ein Geschäftsprozess / System vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse ausfallen darf (Recovery Time Ojective RTO)

- ✓ Ebenfalls sollte definiert sein, wieviel Datenverlust in Kauf genommen werden kann und wie viele Daten / Transaktionen zwischen der letzten Sicherung und dem Systemausfall höchstens verloren gehen dürfen (Recovery Point Objective RPO).

- ✓ Für das DMS bzw. die Archivierung sollte der Datenverlust gegen Null gehen weswegen sich an dieser Stelle gespiegelte Systeme empfehlen

- ✓ Die System-Konfiguration des/der Servers sowie des IT-Netzwerks und der Datensicherung muss auf die Anforderungen des Unternehmens abgestimmt und entsprechend konzipiert sein.

6.2 IT Infrastruktur und Rechenzentrumsbetrieb

Die technische Konfiguration der eingesetzten IT-Komponenten muss sichergestellt werden, um die Anforderungen der GoBD hinsichtlich Datenverfügbarkeit wie auch Vertraulichkeit (Datenschutz DSGVO) sicher zu stellen. Konkrete Vorgaben werden an dieser Stelle nicht gemacht, da sich die Anforderungen aus den jeweiligen Unternehmens-Größenordnungen erheblich unterscheiden können

Die ERP- und DMS-Server-Komponenten unterliegen i.d.R. den gleichen Sicherheitsanforderungen, wie andere IT-Komponenten, da diese als Bestanteil der IT-Prozesse zu betrachten sind. Relevante Themen sind Überwachung, Datensicherheit und –sicherung, Verfügbarkeit, Datenschutz, Zugangs- und Zugriffsschutz sowie Restart- und Katastrophenfall-Abdeckung.

Teilweise werden für Archiv-Systeme separate Server-Komponenten genutzt (z.B. separate Speichersysteme (NAS-Systeme oder für die jährliche Sicherung nicht wiederbeschreibbare Speichermedien etc.). Diese müssen im Rahmen des allgemeinen Sicherheitskonzepts mit berücksichtigt werden

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Zugriffsschutz auf die Anwender erfolgt über umfangreiches Berechtigungssystem der WDV-Administration mit Freigabe von Modulen sowie spezifischen Funktionen der einzelnen Module. In jeder Berechtigungsstufe kann dem Anwender Rechte in den Stufen Sehen, Bearbeiten, Hinzufügen, Löschen gewährt werden
- ✓ Für jeden Mitarbeiter können spezifische Rechte für unterschiedliche Archiv-Dokumententypen versehen werden, so dass für einen „normalen“ Anwender der Zugriff z.B. auf Personaldaten oder anderweitige Daten, die speziellem Schutz unterliegen nicht möglich ist.
- ✓ Das Löschen von Archiv-Daten ist für Anwender grundsätzlich ausgeschlossen

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Zur Sicherstellung der Datensicherheit und Verfügbarkeit sollten gebäudetechnische Maßnahmen hergestellt werden, so z.B. Aufstellung der Server in einem separaten Rechenzentrum mit Klimaanlage, Alarmanlage, Notstromversorgung sowie besonderer Brandschutzvorrichtungen
- ✓ Zutrittsregelungen zum Rechenzentrum bzw. Serverraum sollten geschaffen werden über welche nur für berechtigte Personen der Zugang gestattet ist, ggf. mit Protokollierung des Zutritts
- ✓ Zur Sicherstellung der Verfügbarkeit können auf Basis definierter Verfügbarkeitsziele / Kenngrößen getroffen – dies betrifft ebenfalls die gesamte Unternehmens-IT
- ✓ Für die Datensicherung muss ein übergreifendes Backup-Konzept für alle IT-Anwendungen erstellt werden. Wesentlicher Bestandteil des Konzepts beschreibt die Verantwortlichkeiten und Prozeduren. D.h.
  - Welche Datenbestände werden wann gesichert
  - Welche Sicherungsverfahren werden verwendet
  - etc.
- ✓ Jede Sicherung muss in regelmäßigen zeitlichen Abständen geprüft werden, ob Backups wieder zurückgeladen werden können (Restore-Test).

- ✓ Schutz der Sicherungskopien vor unberechtigtem Zugriff und gegen Verlust
- ✓ Ggf. Auslagerung der Sicherung in regelmäßigen Zeitabständen an einen externen Ablageort (z.B. Bankschließfach / Treuhänder etc.) oder Lagerung der Backup-Medien in einem externen Rechenzentrum, so dass auch bei gravierenden Zerstörungen der hauseigenen IT durch z.B. Feuer / Wasser Datensicherungen noch verfügbar sind
- ✓ In aktuellen IT-Anwendungen werden die relevanten Daten i.d.R. auf einem Server gespeichert, so dass sich ein Backup für Arbeitsplatzrechner erübrigt; sollten noch alte Systeme zum Einsatz kommen, deren Daten ausschließlich auf lokalen Arbeitsplätzen gespeichert werden, müssen diese in einem Sicherungskonzept ebenfalls berücksichtigt werden
- ✓ Falls erforderlich oder im IT-Konzept vorgesehen teilweise Verwendung spezieller Wechselmedien oder Storage-Subsysteme für ein DMS, für welche ggf. spezielle Backup-Maßnahmen erforderlich sein können.
- ✓ Für den K-Fall (Katastrophe / Totalausfall), Implementierung von Reverssystemen mit hoch verfügbaren Systemauslegungen (z.B. Fail-Over-Cluster ggf. an einem anderen Standort oder in einem externen Rechenzentrum)
- ✓ Spannbreite reicht von Reservesystem für einzelne Komponenten, bis hin zum kompletten Spielgen-Rechenzentren
- ✓ Erstellung eines Notfallplans für Restart und Recovery für den Fall, dass einzelnen Komponenten oder das ganze System ausfällt; einschließlich einer Vorab-Definition der verantwortlichen Rollen und die Prozeduren für einen Restart ggf. in Form einer Arbeitsanweisung.
- ✓ Regelmäßige Recovery-Tests bzw. Wideraufsetzen des gesamten Systems nur aus den Backup Medien
- ✓ Vor Freigabe eines neuen Verfahrens / Prozesses sollte ein geordnetes Test- und Freigabeverfahren definiert und entsprechend durchgeführt werden; bei Änderungen von bestehenden Verfahren, sollten Regeln festgelegt werden, in welchen Fällen Tests durchzuführen sind. Die Ausgestaltung der Tests ist vom jeweiligen Prozess abhängig
- ✓ Für Service- & Supportleistungen von Lieferanten sollten entsprechende Wartungs- und Supportverträge für die Komponenten der Rechenzentrums-Infrastruktur abgeschlossen werden (z.B. Klimaanlage, USV etc.); ebenfalls sollten Verantwortlichkeiten für die Einschaltung des externen Supports festgelegt werden (z.B. Rollen, Eskalationsprozesse etc.)

6.3 Betriebsbedingungen und Wartung

Hersteller von Hard- und Softwarekomponenten definieren für ihre Produkte eine Umgebung, für die die Produkte getestet und freigegeben sind. Für einen sicheren IT-Betrieb ist es erforderlich, dass diese Bedingungen eingehalten werden. Dies gilt auch für die Wartungs- und Updateregelungen.
Dieser Grundsatz gilt für alle IT-Systeme gleichermaßen.

a) Was PRAXIS Ihnen in diesem Zusammenhang anbietet:

- ✓ Zu jeder Freigabeversion der WDV 20xx erhalten Sie einen Newsletter mit den aktuellen Systemvoraussetzungen und Empfehlungen; in Ergänzung hierzu steht Ihnen das „Roadmap für IT-Netzwerke“ zur Verfügung als Unterstützung und Leitfaden für die Konzeption eines IT-Netzwerkes

- ✓ Sie verfügen über einen Software-Wartungsvertrag, und erhalten regelmäßige Updates, in welchem nicht nur Weiterentwicklungen enthalten sind, sondern regelmäßig auch Anpassungen an veränderte gesetzliche Gegebenheiten. Sollten Sie noch keinen Software-Wartungsvertrag abgeschlossen haben, wenden Sie sich bitte an unsere Frau Christa Seyffarth unter christa.seyffarth@praxis-edv.de oder Telefon-Nummer 036258-566-75. Sie wird Ihnen gerne ein Vertragsexemplar zusenden.

- ✓ Über verschiedene Care-Pakete können Sie zusätzliche Service-Leistungen wie z.B. regelmäßige Datenbankwartungen buchen.

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Die Betriebsbedingungen der Hardware müssen eingehalten werden, so z.B. durch Klimatisierung der Räume, Staubfilter, passende Leitungslängen bei Netzwerken. Diese sollten bei Freigabe der Hardware oder bei baulichen Veränderungen geprüft und ggf. angepasst werden

- ✓ Hardware-Wartung erfolgt nach definierten Wartungsplänen gemäß der Hersteller; dies bezieht sich vor allem auf Geräte mit mechanischen Teilen, insbesondere Scanner / Drucker. Server können ebenfalls vorbeugend gewartet werden, werden jedoch oftmals nach einigen Jahren ausgetauscht. Störungen werden bei Bedarf im Rahmen des Hardware-Supports behoben.

- ✓ Die konkrete Ausgestaltung des Wartungs- und Supportkonzepts ist in der Regel individuell je Unternehmen und Größenordnung, sowie bestehender IT-Systemumgebung. Sollte jedoch systemübergreifend für alle IT-Anwendungen erfolgen. Entscheidend ist, dass das Konzept die gewünschte Verfügbarkeit gewährleistet

- ✓ Zur Sicherstellung der Zuverlässigkeit von Hardware sollten Zuständigkeiten und Regeln für den Austausch und Update von Hardware festgelegt werden. Es sollte nur Hardware zum Einsatz kommen, für welche noch Wartung / Support verfügbar ist.

- ✓ Oftmals wird die Nutzungsdauer von Hardware von Beginn an so geplant, dass die Wahrscheinlichkeit von Störungen während der Nutzungsdauer gering ist.

- ✓ Ebenfalls sollten die Betriebsbedingungen für Software eingehalten werden; hierbei sind Freigaben der Hersteller für bestimmte Betriebssysteme, Datenbanken etc. zu beachten. Vor Freigabe bzw. Installation von Software-Komponenten und Updates müssen in jedem Fall ggf. erforderliche Veränderungen der Systemumgebung überprüft werden

- ✓ In aktuellen IT-Anwendungen werden die relevanten Daten i.d.R. auf einem Server gespeichert, so dass sich ein Backup für Arbeitsplatzrechner erübrigt; sollten noch alte Systeme zum Einsatz kommen, deren Daten ausschließlich auf lokalen Arbeitsplätzen gespeichert werden, müssen diese in einem Sicherungskonzept ebenfalls berücksichtigt werden

- ✓ Bezüglich der Installation von Software-Updates und neuen Produktreleases sollten Zuständigkeiten und Regeln definiert werden, ob und wann solche Updates eingespielt werden (Freigabeverfahren). Bei komplexen Anwendungsprozessen wird empfohlen, vor Installation des Updates im Produktivsystem die neue Version in einer Testumgebung vor Freigabe zu überprüfen

- ✓ Protokollierung von Wartungsmaßnahmen, Austausch von Hardware sowie das Einspielen von Updates und neuen Releases

6.4 Problembehebung und Support

Bei Fehlersituationen und Störungen in IT-Systemen müssen inkonsistente Systemzustände und Datenverlust verhindert werden. Die Systeme müssen schnell wieder in einen arbeitsfähigen Zustand gebracht werden – d.h. die Zielsetzung ist, dass die Systeme und Daten möglichst zeitnah und vollständig wieder hergestellt werden

Dieser Grundsatz gilt für alle IT-Systeme gleichermaßen.

a) Was PRAXIS Ihnen in diesem Zusammenhang anbietet:

- ✓ Der PRAXIS Helpdesk kann für unternehmensinterne Kommunikations-Plattform von Ihrem Unternehmen genutzt werden; falls eine Anfrage des Endbenutzers durch Ihren IT-Administrator oder Key-User nicht gelöst werden kann, kann die Meldung an PRAXIS direkt über den Helpdesk weitergeleitet werden

- ✓ Über verschiedene Care-Pakete können Sie zusätzliche Service-Leistungen wie z.B. Hotline-Service / Update-Service sowie regelmäßige Datenbank-wartungen buchen.

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Einrichtung eines unternehmensinternen, technischen IT-Helpdesk für Fachbenutzer. Bei Störungen der technischen Infrastruktur (z.B. PC startet nicht, Netzwerk nicht verfügbar, Passwort abgelaufen, Drucker druckt nicht etc.) müssen für Endbenutzer Ansprechpartner verfügbar sein. Dieser interne, technische IT-Helpdesk kann beraten, kleinere Probleme selbst lösen und ggf. den externen Support einschalten; hierfür können interne IT-Administratoren oder Key-User / Power-User eingesetzt werden

- ✓ Regelwerke und Definition von Verantwortlichkeiten für die Einschaltung des externen Supports (Rollen, Eskalationsprozesse etc.)

6.5 Zugriffs- & Berechtigungssystem

Dokumente und Daten müssen gegen unberechtigte Kenntnisnahme und unberechtigten Zugriff sowie Eingaben, Veränderungen und unberechtigtes Löschen wirksam geschützt werden. Mittels eines Berechtigungssystems muss der unberechtigte Zugriff verhindert werden und somit die Ordnungsmäßigkeit sicherstellen (insbesondere Integrität und Authentizität)

Um dies zu gewährleisten und unterschiedlichen Benutzern oder Benutzergruppen den Zugriff auf bestimmte Daten zu erlauben oder zu verbieten bedarf es eines differenzierten Berechtigungssystems. Insbesondere sind durch dieses System nicht gewollte Veränderungen zu verhindern und administrative Aktionen nur einer begrenzten Benutzeranzahl zur Verfügung zu stellen.

Im Hinblick auf den Datenzugriff der Finanzverwaltung (siehe 8.1 Maschinelle Auswertbarkeit und Datenzugriff) bedarf es – bezogen auf die als steuerrelevant einzustufenden Daten und Dokumente – der Einrichtung einer Betriebsprüfer-Rolle mit Nur-Lesezugriff.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Feines Berechtigungssystem innerhalb der WDV-Administration mit Benutzer- und Benutzergruppen-Rechte-Steuerung; je Modul und Mandant / Wirtschaftsjahr können individuelle Rechte in den Stufen „sehen, bearbeiten, hinzufügen und löschen“ gesetzt werden

- ✓ Freigabesystem von Dokumententypen, auf die der Benutzer zugreifen kann

- ✓ Für den Finanzbeamten kann damit eine spezifizierte „Betriebsprüfer“ Rolle eingerichtet werden, über welche er ausschließlich lesenden Zugriff auf die steuerrelevanten Daten erhält

- ✓ Direkter Zugriff auf die Datenbank ist ausgeschlossen – die Datenbank ist für den unberechtigten Zugriff geschützt

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Erstellung eines übergreifenden Berechtigungskonzepts, ggf. auch für andere IT-Systeme als für das DMS. Das Konzept sollte generelle Regeln enthalten aus denen die Entscheidungen über die Berechtigungen im Einzelfall abgeleitet werden können.

- ✓ Insbesondere Datenschutzes sowie Zugriffsberechtigungen auf personenbezogene Daten sollten sich in diesem Konzept wieder finden. Hier verweisen wir auf die DSGVO, deren Belange in einem Berechtigungskonzept in jedem Fall berücksichtigt werden sollten.

- ✓ Für alle Systeme die im Zusammenhang mit den Vorgaben der GoBD stehen müssen die Benutzer in den jeweiligen Berechtigungssystemen bekannt sein; es empfiehlt sich eine rollenbezogene Benutzerverwaltung *(Hinweis: in der WDV Benutzergruppen*). Die Rollenbeschreibungen mit den entsprechenden Berechtigungen sollten mit den Beschreibungen in den Prozessdefinitionen übereinstimmen. Die Rechtevergabe erfolgt pro Rolle und Zuordnung der Benutzer – hiermit ist ein geringerer administrativer Aufwand verbunden und die Transparenz und Nachvollziehbarkeit wird positiv beeinflusst.

- ✓ Über z.B. das „Active Directory“ lassen sich bereits anwenderübergreifende Benutzerverwaltungen steuern – hier müssen vor allem die Zugriffs-Freigaben auf Daten-Ablageorte (z.B. auf den Archiv-Pfad) für den direkten Zugriff ausgeschlossen werden.

- ✓ Das Berechtigungssystem sollte unternehmens-übergreifend strukturiert und einheitlich abgebildet sein, so dass keine inkonsistenten Rechtevergaben entstehen können.

- ✓ Über Login-Regeln innerhalb des Berechtigungskonzepts sollte auch die sichere Systemanmeldung gesteuert werden, hierzu gehören z.B. Passwort-Regeln, Sperrung bei mehrfach falsch eingegebenem Passwort, Erzwungener Passwortwechsel nach einer bestimmten Zeit; die Regularien für administrative Nutzer sollten hinsichtlich der Passwort-Komplexität restriktiv ausgestaltet werden (im Vergleich zu einem Standard-Nutzer).

- ✓ Berechtigungsstrukturen sollte so strukturiert sein, dass Berechtigungen nach dem sog. „Neet-to-know“ Prinzip vergeben werden – d.h. jede Rolle erhält nur die Rechte, die zur Ausführung der jeweiligen Aufgaben erforderlich sind

- ✓ Sämtliche Berechtigungen sollten ausführlich Dokumentiert sein, sowie Änderungen an den Berechtigungen sind zu protokollieren.

6.6 Mitarbeiter

Die Mitarbeiter, die das IT-System für ihre fachliche Arbeit nutzen oder die für Administration und Betrieb des Systems zuständig sind, müssen über die entsprechenden Qualifikationen und Kenntnisse verfügen.

Es bietet sich an für Mitarbeiter entsprechend Ihres Anforderungsprofils bzw. Aufgabengebietes eine Tätigkeitsbeschreibung zu erstellen, welche auch die zugeordnete Rolle im Unternehmen (Organigramm und daraus resultierend Berechtigungs-Rolle) sowie die erforderlichen Kenntnisse beinhaltet.

Hierauf basierend können gezielt Qualifikationen sowie Weiterbildungsmaßnahmen organisiert und durchgeführt werden.

Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Rollendefintion der Mitarbeiter / Gruppen optimalerweise basierend auf dem Organigramm des Unternehmens – unter Berücksichtigung der mit der Funktion / Rolle verbundenen Rechte an IT-Systemen dies sowohl für das DMS / Archiv, wie auch für andere IT-Systeme
- ✓ Dokumentation von Definierten Aufgaben und Zuständigkeiten der jeweiligen Rollen; dies kann in Form von Arbeitsplatzbeschreibungen erfolgen und für die durchzuführenden Aufgaben können bei Bedarf Arbeitsanweisungen formuliert werden. Dies empfiehlt sich vor allem für komplexe und/oder sicherheitsrelevante Aufgaben. Die erforderlichen Qualifikationen der Mitarbeiter ergeben sich aus ihren Aufgaben
- ✓ Bei der Stellenbesetzung wird auf die Verlässlichkeit und fachliche Eignung der Mitarbeiter geachtet, insbesondere bei administrativen Rollen
- ✓ Jeder Anwender sollte durch Einweisungs- und Schulungsmaßnahmen für sein/ihr Aufgabengebiet qualifiziert werden. Dies kann in Form von Inhouse-Schulungen erfolgen, die z.B. die technische Systembenutzung wie auch fachliche Regeln in der Anwendung beinhalten.
- ✓ Administratoren sollten mit einer speziellen, tiefergehenden Einweisung- bzw. Schulungsmaßnahmen für Administratoren intensiv qualifiziert werden.
- ✓ Hinsichtlich der Nachvollziehbarkeit sollte für alle Mitarbeiter die vorhandene Qualifikation (z.B. Berufsausbildung), sowie zusätzliche Qualifikations-Maßnahmen dokumentiert werden; über Ausbildungspläne können regelmäßige Weiterbildungsmaßnahmen geplant und koordiniert werden.
- ✓ Zur Gewährleistung der Sicherheit und Ordnungsmäßigkeit ist ein angemessenes Problembewusstsein für mögliche Risiken u.a. beim Einsatz eines DMS sicher zu stellen; hierfür sind insbesondere ausreichende Schulungen der Mitarbeiter sowie aussagekräftige Dokumentation der möglichen Risiken von Bedeutung.
- ✓ Diese Dokumentation kann auch in einem Unternehmens-Handbuch oder im Rahmen eines QM-Systems erfolgen und gilt nicht nur für das DMS sondern übergreifend für das Unternehmen mit allen Systemen und Prozessen

7 Erfassung und Verarbeitung im DMS

In diesem Abschnitt werden Prozesse und Themenbereiche dargestellt, die besondere Aspekte bezüglich der Ordnungsmäßigkeitskriterien der GoBD besitzen. Es wird auf die folgenden Themen eingegangen

- ⇨ Scannen von Papierdokumenten
- ⇨ Archivierung von Ausgangsdokumenten
- ⇨ Archivierung von eMails
- ⇨ Archivierung von Rechnungen

7.1 Scannen von Papierdokumenten

Steuerrecht und Handelsrecht gestatten über § 147 Abs. 2 AO, § 257 Abs. 3 HGB im Grundsatz die Aufbewahrung von Unterlagen auf einem Bild- oder anderen Datenträger, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht. Werden Handels- oder Geschäftsbriefe und Buchungsbelege in Papierform empfangen und danach elektronisch erfasst (Scannen), ist das Scanergebnis so aufzubewahren, dass die Wiedergabe mit dem Original bildlich übereinstimmt, wenn es lesbar gemacht wird.

Der Verzicht auf Papierbelege darf die Möglichkeit der Nachvollziehbarkeit und Nachprüfbarkeit nicht beeinträchtigen. Beim Scannen von Papierdokumenten sind verschiedene Anforderungen der GoBD zu beachten (BMF Schreiben Punkt 9.3 Absatz 136 – 141). Darüber hinaus müssen prozessspezifische Besonderheiten (Farberfassung, OCR-Lesung, Rückseiten, Vernichtung) beachtet werden.

Der Prozess muss so gestaltet sein, dass alle Seiten aller Papierdokumente vollständig gescannt werden und bildlich mit dem Original übereinstimmen. Dabei ist dem Betriebsprüfer direkt über das DMS auch die Einsicht der elektronischen Belege unmittelbar am Bildschirm zu gestatten, auch wenn die Belege noch als Papieroriginale verfügbar sind.

Werden gescannte Dokumente per Optical-Character-Recognition-Verfahren (OCR-Verfahren) um Volltextinformationen angereichert (z. B. volltext-recherchierbare PDFs), so sind diese Dateien ebenfalls aufzubewahren. Es ist eine Farbwiedergabe erforderlich, wenn den Farbinformationen eine Beweisfunktion zukommt (z.B. wenn ein negativer Wert „rot“ und ein positiver Wert „schwarz“ dargestellt wird).

Wird das Papierdokument nach dem Scannen in Papierform weiter bearbeitet, ist dieses erneut zu scannen und zum ersten Scanobjekt in Bezug zu setzen. Nach dem Einscannen dürfen Papierdokumente vernichtet werden, soweit sie nicht nach außersteuerlichen oder steuerlichen Vorschriften im Original aufzubewahren sind.

Für die Organisation des Scanprozesses ist zwingend eine Verfahrensdokumentation zu erstellen. Diese sollte insbesondere Ausführungen zum Prozess, zu den personellen sowie den technischen Anforderungen enthalten. Entsprechend sind organisatorische Regelungen erforderlich (Wer darf scannen?; Zu welchem Zeitpunkt wird gescannt?; Was wird gescannt?; Wie erfolgt eine Protokollierung und Qualitätssicherung?; etc.), die in Form von Arbeitsanweisungen vorhanden sein müssen.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Die WDV 2017 mit der integrierten Archivierung erfüllt – wie bereits unter den allgemeinen Anforderungen an DMS-Produkte und Lösungen aufgeführt, die Grundsätze der Ordnungsmäßigkeit auch für gescannte Papierdokumente
- ✓ Bei OCR / Volltexterkennung werden alle Daten aufbewahrt
- ✓ Unterschiedliche Scan-Profile können in der WDV unterschiedliche weiterführende Prozesse automatisiert anstoßen (z.B. PxFlow / Einstellen der Dokumenten in verschiedene Postboxen / Automatischer Scann von Lieferschein-Rückläufern mit der Kundenunterschrift und Zuordnung des Rückläufers als neue Dokumentenversion zum Original-Lieferschein; sonstige Prozesse, die individuell über PxFlow gesteuert werden können) – die erforderliche Dokumentation des Prozesses ist im Rahmen der Verfahrensanweisung durch den Anwender zu dokumentieren
- ✓ Systemtechnische Fehlerbehandlung bei nicht erkannten Barcodes oder Indexen, falls ein Dokument nicht automatisch zugeordnet werden kann falls ggf. der Barcode nicht erkannt wurde (Kaffeefleck o.ä.) – Dokumente werden zur manuellen Nachbearbeitung der Zuordnung in eine vordefinierte Postbox eingestellt

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Zum vollständigen Scann der Dokumente muss entsprechende Hardware eingesetzt werden, welche ggf. die Rückseitenerfassung, eine Doppel-einzugskontrolle beinhaltet sowie die Seiten zur Vollständigkeitsprüfung zählt.
- ✓ Zum Scannen der Papierdokumente sollte mit optimalen Scan-Profilen / Einstellungen gearbeitet werden, damit ausreichend Farbe, DPI und Kontrast zu verwendet wird, um auch schlechte Original-Vorlagen in einer möglichst optimalen Qualität zu scannen; Ggf. kann Bildverbesserungssoftware zum Einsatz kommen, um einer Verbesserung der Lesbarkeit zu erreichen
- ✓ Bei Stapelverarbeitung beim Scannen sichergestellt werden, dass eine korrekte Dokumententrennung erfolgt
- ✓ Doppelterfassungen sollen vermieden werden (organisatorisch)
- ✓ Es muss eine Qualitätssicherung erfolgen, über welche sichergestellt wird, dass die gescannten Dokumente korrekt, vollständig und in bestmöglicher Qualität für die Archivierung gescannt wurden
- ✓ Soweit Farbe in einem Dokument eine Beweisfunktion zukommt, müssen diese Dokumente in Farbe gescannt werden

c) Verfahrensanweisung zum Scan-Prozess

- ✓ Es muss eine vollständige und umfängliche Verfahrensanweisung erstellt werden, welche den vollständigen Prozess beschreibt, diese ist mit entsprechenden Arbeitsanweisungen zu ergänzen:

- ✓ Arbeitsanweisung – Vorbereitung

    - Beim Prozess der Arbeitsvorbereitung für das Scannen geht es im Wesentlichen darum, bei der Vorbereitung trotz Entklammern von gehefteten Dokumenten, Öffnen der Eingangspost und Auflösen von Ordnern, aufgebrachten Post-Ist etc. den richtigen Zusammenhang und die vollständige Erfassung sicherzustellen
    - Die Arbeitsvorbereitung beim Import von gescannten Dateien beinhaltet die Kontrollfunktion, welche sicherstellt, dass die richtigen Dateien in die Übergabeverzeichnisse eingestellt worden sind.

- ✓ Arbeitsanweisung – Scannen

    - Scannen ist ein mehrstufiger Prozess, der in allen Schritten organisatorisch abgesichert sein muss, um die vollständige und richtige Erfassung aller Dokumente zu gewährleisten
    - Dies gilt für das Scannen einzelner Dokumente und für Stapel-Scannen gleichermaßen
    - Es muss eine Festlegung erfolgen, wann welches Scanprofil mit welchen Einstellungen genutzt werden soll
    - Es muss definiert werden, wie der Umgang mit Sonderformaten und geösten / gebundenden Dokumenten erfolgen soll
    - In jedem Fall sind die Bildqualität sowie die korrekte und vollständige Erfassung der Dokumente regelmäßig zu prüfen

- ✓ Arbeitsanweisung – Nachbereitung

    - Die Arbeitsnachbereitung beim Scannen beinhaltet das Aussortieren von Originalen, die in Papierform aufbewahrt oder an Kunden zurückgegeben werden müssen. Die Vernichtung von nicht aufbewahrungspflichtigem oder – würdigem Material, die Vollständigkeitskontrolle der Erfassung etc.
    - Sofern nach dem Scanvorgang aus organisatorischen Gründen eine weitere Vorgangsbearbeitung des Papierbelegs erfolgt, muss nach Abschluss der Bearbeitung der bearbeitete Papierbeleg erneut eingescannt und ein Bezug zum ersten Scanobjekt hergestellt werden (gemeinsamer Index)
    - Die Arbeitsnachbereitung beinhaltet ebenfalls die Kontrolle, ob die temporären Verarbeitungsdateien ordnungsgemäß verarbeiten und anschließend gelöscht worden sind.

- ✓ Arbeitsanweisung – Qualitätssicherung
    - Sofern die bildliche Wiedergabe von originär digitalen Dokumenten im Rahmen der Übernahme relevant ist, ist sicherzustellen, dass die Dokumente bezogen auf die relevanten Dokumenteninhalte unverändert übernommen werden.
    - Bei der Erfassung von gescannten Dokumenten ist es in der Regel notwendig, jede erfasste Seite einer visuellen Qualitätskontrolle zu unterziehen, um die Lesbarkeit und den originalen bildhaften Eindruck sicherstellen zu können.
    - Dies kann ein mehrstufiges Verfahren sein (z. B.: Erster Schritt Erfassen, zweiter Schritt visuelle Kontrolle, dritter Schritt Indizierung).
    - In Abhängigkeit von der Dokumentenart Implementierung von Regelungen für ein 4-Augen-Prinzip bei Stichprobenprüfungen von Dokumenten und Indexdaten

- ✓ Arbeitsanweisung – „frühe Erfassung“
    - Erfolgt bei der frühen Erfassung eine Weiterbearbeitung der Papierbelege nach dem Scannen, sind diese Papierbelege erneut zu scannen und mit den Ursprungsdokumenten zu verknüpfen.

- ✓ Arbeitsanweisung – Aufbewahrung / Vernichtung von Papierbelegen
    - Es bedarf einer klaren und eindeutigen Definition und Regelung, wann und wie welche Papierdokumente nach dem Scannen vernichtet werden.
    - Ebenfalls muss klar definiert werden, welche Papierdokumente im Papier-Original aufbewahrt werden (müssen) und wie und an welcher Stelle diese abgelegt werden (z.B. Pacht-Verträge in einer Vertragsakte / Arbeitsverträge in der Personalakte etc.
    - Bei jedweder Archivierung und Papierablage ist der Mitarbeiter auf die Datenschutzregularien hinzuweisen.
    - Mitarbeiter, die mit besonders schutzwürdigen Daten umgehen, sollten über eine gesonderte Belehrung / Datenschutzvereinbarung auf die Pflichten im Rahmen der DSGVO sensibilisiert werden bzw. auf die (Haftungs-)Risiken belehrt werden.

- ✓ Bei der Aufbewahrung des Originals ist die Authentizität der Dokumente sicherzustellen, dies ist über eine eindeutige Verbindung zwischen dem Original und dem digitalisierten Abbild zu realisieren (z.B. über Barcodes, Archivindexe oder ggf. organisatorisch)

7.2 Archivierung von Ausgangsdokumenten

Soweit es sich um Ausgangsdokumente handelt, wird in § 147 Abs. 2 AO eine inhaltliche Übereinstimmung gefordert. In diesem Fall gelten die Ordnungsmäßigkeitskriterien für die Anwendung, in der die Ursprungsdaten aufbewahrt werden. Eine entsprechende Reproduzierbarkeit verlangt dabei neben den Bewegungsdaten auch den jeweiligen (historischen) Stand der Stammdaten festzuhalten.

Wenn die Daten der Ausgangsdokumente nicht im DMS aufbewahrt werden, sondern bspw. In einer Fakturierungsanwendung, sind keine besonderen Anforderungen an eine DMS-Umgebung zu stellen. Daneben existieren allerdings Archivierungsszenarien, bei welchen die inhaltlichen Informationen eines Ausgangsdokuments in einem DMS aufbewahrt werden, z.B. in Form eines Netto-Images, welches nur aus den formatierten Daten besteht. Diese Daten werden für den Ausdruck dann mit Hintergrund-Layout ergänzt. In diesem Fall muss das DMS die Ordnungsmäßigkeit der Daten sicherstellen. Da die Nutzung historisierter Stammdaten jedoch nicht trivial ist, empfiehlt es sich in der Praxis häufig, die entsprechenden Ausgangsbelege zum Zeitpunkt der Erstellung in einem Bildformat (z. B. PDF/A- oder TIFF-Datei) der Aufbewahrung zuzuführen. Dieses so vorhandene Dokument besitzt dann keine Abhängigkeiten zu anderen Datenbeständen oder Ressourcen-Dateien.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Die in der WDV erstellten (Ausgangs-) Belege werden automatisch in die Archivierung eingebracht; d.h. Angebote, Aufträge, Lieferscheine und Rechnungen sowie Rechnungsausgangsbücher zur Protokollierung der Datenübergabe an die Finanzbuchhaltung werden automatisch archiviert

- ✓ Sämtliche Belege werden mit allen vollständig mit ALLEN inhaltlichen enthaltenen Daten UND Layouts als PDF/A Dokumente ins Archiv eingestellt, so dass auch bei Stammdatenänderungen der jeweilige Original-Beleg beim Abruf aus dem Archiv ausgegeben wird. Ebenso verhält es sich mit Layout-Änderungen (Hintergrund), sofern sich über die Zeit der Briefbogen ändert. Damit ist sichergestellt, dass ein Dokument immer auf Basis der historischen Daten auf dem richtigen Briefbogen ausgegeben wird.

- ✓ Darüber hinaus gehende Dokumente, die in der WDV 2017 erstellt wurden und nicht ins DMS-System bzw. in die Archivierung eingebracht wurden, sind über die WDV 2017 jederzeit reproduzierbar.

- ✓ Ebenfalls können Handels- und Geschäftsbriefe, die z.B. als Word-Dokument erstellt wurden, ebenfalls ins DMS-System eingebracht werden, diese beinhalten den inhaltlichen Umfang, in dem das Dokument erstellt wurde und können zu dem jeweiligen Vorgang in der WDV direkt verknüpft werden

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Bei der Ausgangsarchivierung z.B. von Handels- und Geschäftsbriefen, die mit Word erstellt wurden, sind die aufbewahrungspflichtigen Inhalte, nicht ihre visuelle Gestaltung reproduzierbar sein. D.h. Formatierungsinformationen wie Layout, Zeichensätze, Schriftfarbe sind nicht reproduktionspflichtig.

- ✓ Bildliche Abweichungen zwischen dem ursprünglichen Dokument und der Anzeige bei Reproduktion dürfen eine Prüfung des Sachverhalts nicht unangemessen erschweren (z.B. Zeichenwüste)

- ✓ Hintergrundbilder und andere grafischen Gestaltungselemente bei intern erstellten Dokumenten müssen i.d.R. ebenfalls nicht aufbewahrt oder bei der Reproduktion dargestellt werden.

- ✓ Firmenlogos sind ebenfalls häufig nur Dekoration und können dann ignoriert werden, wenn bei der Reproduktion sichergestellt ist, dass der Handels- oder Geschäftsbrief der zum Zeitpunkt des Versands verantwortlichen natürlichen oder juristischen Person sicher zugeordnet werden kann (korrekte Zuordnung zum Steuerpflichtigen) und keine steuerrelevanten Informationen verloren gehen

- ✓ Die Wiedergabe muss wortgetreu sein, eine Zusammenfassung des wesentlichen Inhalts ist nicht zulässig.

- ✓ Wenn im Original der ausgehenden Handels- und Geschäftsbriefe Allgemeine Geschäftsbedingungen oder andere relevanten Texte mitgeliefert werden, sind diese ebenfalls zu dokumentieren. Gegebenenfalls genügt ein Verweis und sie müssen jederzeit verfügbar sein

- ✓ Zu Ihrer Sicherheit empfehlen wir, auch Handels- und Geschäftsbriefe immer vollständig, wie diese versendet wurden ins WDV-Archiv einzubringen. So werden mögliche Auslegungen bereits im Vorfeld vermieden.

- ✓ Sofern im Rahmen des Ausgangsprozesses zusätzliche steuerrelevante Daten (z.B. ZUGFeRD- oder EDI-Daten) entstehen, fallen diese nicht unter die Festlegung von Ausgangsdokumenten. Hierbei handelt es sich um steuerrelevante Daten, die ebenfalls aufbewahrt werden müssen (siehe Archivierung von Rechnungen)

7.3 Archivierung von eMails / 10 Merksätze

E-Mails mit der Funktion eines Handels- oder Geschäftsbriefs oder eines Buchungsbelegs sind entsprechend den GoBD in elektronischer Form aufbewahrungspflichtig. E-Mails werden explizit als originär digitales Dokument eingestuft und müssen entsprechend im Originalformat vorgehalten werden.

Werden steuerrelevante E-Mails in einer DMS-Umgebung aufbewahrt, müssen die allgemeinen Ordnungsmäßigkeitsanforderungen beachtet werden. Hier gibt es Besonderheiten, da E-Mails aus mehreren Komponenten bestehen können und maschinell auswertbar oder zumindest recherchierbar vorzuhalten sind.

Sonderfall: Dient eine E-Mail nur als »Transportmittel«, z. B. für eine angehängte elektronische Rechnung, und enthält darüber hinaus keine weitergehenden aufbewahrungspflichtigen Informationen, so ist diese nicht aufbewahrungspflichtig (wie der Briefumschlag bei Papierdokumenten).

Wichtiger Hinweis:

Die hier dargestellten Ausführungen behandeln E-Mails isoliert unter steuerrechtlichen bzw. handelsrechtlichen Aspekten. E-Mails und ihre Archivierung unterliegen dabei stets weiteren gesetzlichen Regelungen, wie insbesondere Vorschriften aus dem Zivilrecht, Arbeitsrecht oder Datenschutzrecht, dazu kommen häufig innerbetriebliche Regelungen. In der Praxis ist eine einzelfallbezogene Auflösung der dadurch generierten Zielkonflikte geboten.

In Ergänzung an dieser Stelle die 10 Merksätze für die eMail Archivierung :

1.) E-Mails sind aufbewahrungspflichtig
E-Mails mit der Funktion eines Geschäftsbriefs oder eines Buchungsbelegs müssen aufbewahrt werden.

2.) E-Mails sind elektronisch aufzubewahren
Ausdrucke auf Papier reichen nicht aus.

3.) Dateianhänge sind im Original aufzubewahren
Steuerrelevante E-Mail Dateianhänge müssen im Originalformat aufbewahrt werden. Verschlüsselte E-Mails müssen auch unverschlüsselt gespeichert werden

4.) E-Mail als Transportmittel
Dient eine E-Mail als reines Transportmittel für eine andere elektronische Datei, zum Beispiel eine Rechnung, muss sie nicht aufbewahrt werden. Die isolierte Speicherung der transportierten Datei reicht aus.

5.) E-Mails sind zu indexieren
Von besonderer Bedeutung ist das Kriterium der Ordnung. Danach müssen E-Mails mittels einer Indexstruktur identifizierbar und klassifizierbar sein. Insbesondere muss eine eindeutige Zuordnung zum jeweiligen Geschäftsvorfall oder Buchungsbeleg hergestellt werden.

6.) E-Mails sind unverändert zu archivieren
Die Aufbewahrung von geschäftlicher E-Mail-Korrespondenz innerhalb des

Mailsystems oder des Dateisystems ohne zusätzliche Sicherungsmaßnahmen reicht nicht aus, um die Anforderungen an die Unveränderbarkeit zu erfüllen.

7.) Die Konvertierung von E-Mails unterliegt spezifischen Vorgaben
Bei der Konvertierung einer volltextrecherchierbaren E-Mail in eine anderes Format müssen die Recherchemöglichkeiten erhalten bleiben.

8.) Der Umgang mit E-Mails ist zu dokumentieren
Die Prozesse für den Empfang und Versand von aufbewahrungspflichtigen bzw. steuerlich relevanten E-Mails müssen dokumentiert werden.

9.) E-Mails unterliegen dem Recht auf Datenzugriff
Betriebsprüfer dürfen laut GoBD E-Mails mit einer Volltextsuche durchsuchen und maschinell auswerten. Daher sollten E-Mails mit steuerlicher Relevanz getrennt von anderer Korrespondenz aufbewahrt werden.

10.) Rechnungen als E-Mails sind zulässig
Seit der Änderung durch das Steuervereinfachungsgesetz 2011 ist es möglich, dass E-Mails ohne weitere Voraussetzungen als elektronische Rechnungen fungieren und beim Empfänger zum Vorsteuerabzug berechtigen.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Es werden nicht automatisch alle eMails in die WDV-Archivierung eingebracht, sondern es muss ein Regelwerk definiert werden, welche eMails mit steuerrelevantem Inhalt in das WDV-Archiv übernommen werden.
- ✓ Sofern ein eMail in die WDV-Archivierung eingebracht wird, wird das Dokument mit einem Index versehen und durch den Anwender beschlagwortet und kann dem Geschäftsvorfall zugeordnet werden (z.B. durch Zuordnung einer Rechnungs-Nummer, auf welche sich das eMail bezieht) – hiermit sind die Grundsätze der Ordnung lt. GoBD gewährleistet
- ✓ Sowie ein eMail in die Archivierung eingebracht ist, bestehen die Grundsätze der Nachvollziehbarkeit und Nachprüfbarkeit, d.h. Ändernde Aktionen an steuerrelevanten eMails sind nachvollziehbar und es erfolgt eine Versionierung.
- ✓ Beim Rechnungsversand per eMail wird nur der Anhang (PDF/A oder PDF/A3 mit ZUGFeRD) automatisch archiviert. Das Belgeitmail als „Briefumschlag“ geht nicht in die Archivierung ein.
- ✓ Die WDV Archivierung bietet für Office-Programme (Word, Excel, PowerPoint, Outlook) entsprechende Add-ins, über welche die Dokumente per Mausklick im originären Format ins Archiv eingefügt werden können.
- ✓ Ebenfalls ist eine Drag & Drop Funktionalität und Volltext-Archivierung enthalten

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Es muss eine Verfahrensanweisung erstellt werden, in welcher der Umgang und die Aufbewahrung von steuerrelevanten eMails geregelt ist. Diese muss im speziellen beinhalten:
  - Festlegung, in welchen Fällen eMails als eMail Objekte (inkl. Anhängen) ins Archiv eingefügt werden und wann und wie die eMails oder Anhänge anderen fachlichen Kategorisierungen zugeordnet werden (Beispiel: das Mail wird archiviert und der Dokumentenart „Korrespondenz“ zugeordnet – der Anhang jedoch soll mit der Dokumentenart „Verträge“ archiviert werden
  - Definition von Mails mit „steuerrelevantem Inhalt“ so dass auch ein Anwender, der diese Bewertung nicht vornehmen kann, ein Regelwerk zur Verfügung hat, welche eMails ins Archiv eingefügt werden müssen, und welche nicht
  - Festlegung welche weiteren Mails, die Sie in Ihr WDV Archivsystem übernehmen möchten, auch wenn diese über keinen steuerrelevanten Tatbestand verfügen.
  - Definition und Vorgabe der Indizierung bzw. Beschlagwortung für die jeweiligen eMails, Zuordnung der Dokumentenart, Verknüpfung zur Kunden- bzw. Baustellenakte etc.
  - Aus der Verfahrensanweisung müssen alle Regularien hervorgehen um die die Vollständigkeit der eMail-Archivierung sicher zu stellen; ggf. ist diese um entsprechende Arbeitsanweisungen zu ergänzen.

- ✓ In der Verfahrensanweisung müssen ändernde Aktionen dokumentiert werden (z.B. Systemeinstellungen oder Stammdaten)

- ✓ Reine SPAM-Mails / Werbemails sind nicht steuerrelevant und unterliegen nicht der Anforderung an Vollständigkeit

- ✓ Um die Richtigkeit nach den Anforderungen der GoBD zu erfüllen, müssen eMails inhaltlich gleich aufbewahrt werden, wie diese erzeugt wurden, da sich das technische „Originalformat“ nach der Anwendung richtet, in der die eMail angezeigt wird; das Ausdrucken oder die PDF-Konvertierung von eMails erfüllt nicht die Anforderungen an die inhaltlich gleiche Aufbewahrung (originär elektronisch)

- ✓ Verschlüsselte eMails müssen auch entschlüsselt aufbewahrt werden

7.4 Archivierung von Rechnungen

Elektronische bzw. digitalisierte (gescannte) Rechnungen unterliegen insbesondere den Anforderungen des Umsatzsteuergesetzes sowie der GoBD. Sie sind nach § 14b UStG grundsätzlich zehn Jahre aufzubewahren.

Wichtiger Hinweis:

Bezüglich der umsatzsteuerlichen Anforderungen ist in Ergänzung zu diesen Ausführungen das BMF-Schreiben vom 2. Juli 2012 (Umsatzsteuer; Vereinfachung der elektronischen Rechnungsstellung zum 1. Juli 2011 durch das Steuervereinfachungsgesetz 2011, BMF vom 2. Juli 2012 - IV D 2 - S 7287-a/09/10004 :003, BStBl. I 2012, S. 726) zu berücksichtigen. Darin finden sich insbesondere Ausführungen zur vereinfachten Rechtslage in Bezug auf den elektronischen Rechnungsaustausch.

Siehe auch:

- ⇨ Kapitel 5 : Allgemeine Anforderungen an DMS-Produkte und Lösungen für die grundsätzlichen Anforderungen an die Aufbewahrung von Rechnungen
- ⇨ Kapitel 7.1 Scannen von Papierdokumenten für das Scannen von Eingangsrechnungen
- ⇨ Kapitel 7.2 Archivierung von Ausgangsdokumenten für die Aufbewahrung von Ausgangsrechnungen
- ⇨ Kapitel 7.3 Archivierung von E-Mails für Rechnungen, die per E-Mail empfangen oder versendet wurden
- ⇨ Kapitel 8.1 Maschinelle Auswertbarkeit und Datenzugriff für die Sicherstellung des Datenzugriffs auf Rechnungen und Rechnungsdaten

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Elektronisch versendete Rechnungen werden ohne den „Briefumschlag“ automatisch archiviert – wahlweise als PDF/A oder PDF/A3 mit ZUGFeRD
- ✓ Es ist sichergestellt, dass die Reproduzierbarkeit von Ausgangsrechnungen auf historische Stammdaten zurückgreift bzw. die Daten / Layouts im Archiv Dokument gespeichert sind; sämtliche Änderungen werden in neuen Dokumentenversionen geführt und protokolliert – es ist jederzeit das Ursprungs-Dokument reproduzierbar
- ✓ Bei frührerer Rechnungserfassung (Scan-Prozess) wird das Dokument ab dem ersten Scann archiviert und ab diesem Zeitpunkt Änderungen durch Versionierung geführt und protokolliert
- ✓ OCR –Daten werden ebenfalls aufbewahrt
- ✓ Die Einrichtung und Dokumentation einer Rechnungseingangsprüfung (Innerbetriebliches Kontrollverfahren mit Prüfpfand) kann mittels dem Zusatzmodul PxFlow und einer gemeinsamen Prozessdefinition eingeführt werden. Ansonsten muss eine Verfahrensanweisung zur Rechnungseingangsprüfung erstellt werden, um mindestens und insbesondere die Prüfung der Pflichtangaben nach § 14 Abs. 4 UstG sicherzustellen.

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Es sollte eine Prozessbeschreibung mit einer Verfahrensanweisung ins Betriebs- oder Unternehmenshandbuch aufgenommen werden, in welcher die beiden Prozesse zur Rechnungsarchivierung dokumentiert sind; speziell die Prozesse und Systemeinrichtungen zum
  - Elektronischen Versand von Ausgangrechnungen
  - Prozess für die Eingangsrechnungsprüfung bzw. Dokumentation zur Prozessabbildung des Workflows im PxFlow

8 Besondere Anforderungen aus steuerlicher Sicht

8.1 Maschinelle Auswertbarkeit und Datenzugriff

Grundsatz GoBD

Sind die nach § 147 Abs. 1 AO aufbewahrungspflichtigen Unterlagen mit Hilfe eines Datenverarbeitungssystems erstellt worden, hat die Finanzverwaltung im Rahmen einer Außenprüfung das Recht, Einsicht in die gespeicherten Daten zu nehmen und das IT-System des Unternehmens zur Prüfung dieser Unterlagen zu nutzen (Unmittelbarer Datenzugriff oder »Z1-Zugriff«). Sie kann im Rahmen einer Außenprüfung auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet (Mittelbarer Datenzugriff oder »Z2-Zugriff«) oder ihr gespeicherte Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden (Datenträgerüberlassung oder »Z3-Zugriff«). Diese Anforderungen gelten im Grundsatz auch für eine DMS-Umgebung.

Für DMS-Umgebungen sind die Themen maschineller Auswertbarkeit und Datenzugriff unter mehreren Aspekten zu betrachten:

Formatkonvertierung

Nach den GoBD sind bei einer Umwandlung (Konvertierung) aufbewahrungspflichtiger Unterlagen in ein Inhouse-Format beide Versionen zu archivieren, unter demselben Index zu verwalten und die konvertierte Version ist als solche zu kennzeichnen. Auch nach einer Konvertierung in ein Inhouse-Format, bei dem das Ergebnis der Umwandlung inhaltlich identisch (verlustfrei) und für die maschinelle Auswertbarkeit verfügbar ist, ist die ursprünglich in das Unternehmen eingegangene Datei in der Originalversion aufzubewahren und darf damit nicht gelöscht werden.
Nicht aufbewahrungspflichtig hingegen sind die während der maschinellen Verarbeitung durch das Buchführungssystem erzeugten Dateien, sofern diese ausschließlich einer temporären Zwischenspeicherung von Verarbeitungsergebnissen dienen und deren Inhalte im Laufe des weiteren Verarbeitungsprozesses vollständig Eingang finden (z. B.: Import-Formate von DMS-Herstellern, die nur dem automatisierten Import dienen). Damit ist eine Umwandlung in ein alternatives Datenformat soweit zulässig, als hierdurch die maschinelle Auswertbarkeit weder eingeschränkt wird noch inhaltliche Veränderungen vorgenommen werden.

Bereitstellung von Stammdaten und Systemeinstellungen

Die GoBD fordern, dass im Rahmen der Datenträgerüberlassung der Finanzbehörde mit den gespeicherten Unterlagen und Aufzeichnungen alle zur Auswertung der Daten notwendigen (Struktur-)Informationen in maschinell auswertbarer Form zur Verfügung gestellt werden. Insoweit sind neben den Daten in Form von Datensätzen und den elektronischen Dokumenten auch alle zur maschinellen Auswertung der Daten im Rahmen des Datenzugriffs notwendigen Strukturinformationen in maschinell auswertbarer Form aufzubewahren.
Damit einher geht die Forderung nach einer vollständigen Beschreibung der Dateiherkunft, der Dateistruktur, der Datenfelder, der verwendeten Zeichensatztabellen sowie der internen und externen Verknüpfungen des zugrunde liegenden IT-Systems.

Das häufig in der Praxis vorhandene Problem der Nachvollziehbarkeit von Stammdaten (z. B.: Datensatzbeschreibungen, Abkürzungs- oder Schlüsselverzeichnisse, Organisationspläne, Umsatzsteuerschlüssel, Währungseinheit, Kontoeigenschaften) sowie von technischen Systemeinstellungen wird konkret adressiert. Um mehrdeutige Verknüpfungen zu verhindern, müssen diese mit Gültigkeitszeiträumen historisiert werden. Die Änderungshistorie darf nachträglich nicht veränderbar sein. Dies betrifft alle steuerrelevanten Systeme und somit auch eine DMS-Umgebung.

Auslagerung von steuerrelevanten Daten in ein DMS

Siehe hierzu Kapitel 5.2 Auslagerung und Migration.

Zugriff auf ein DMS durch den Betriebsprüfer

Die GoBD halten in Bezug auf die Interpretation der maschinellen Auswertbarkeit für Zwecke des Datenzugriffs eine neue oder zumindest modifizierte Sichtweise bereit. Während bereits bislang eine maschinelle Auswertbarkeit bei Daten, Datensätzen, elektronischen Dokumenten und elektronischen Unterlagen gegeben war, die mathematisch-technische Auswertungen ermöglichen, soll dies nun auch der Fall sein, wenn bloß die Möglichkeit einer Volltextsuche besteht. Mittels »Volltextsuche« ergibt sich für die Finanzverwaltung die Möglichkeit einer unspezifizierten dateiübergreifenden Auswertung.

Über frei wählbare Stichworte können jegliche Textdokumente wie E-Mails, Briefe, Buchungstexte oder Reisekostenabrechnungen durchsucht werden. Man muss also in der Praxis davon ausgehen, dass der Prüfer auch die vorhandenen Auswertungsmöglichkeiten eines DMS nutzt. Insoweit sollte hierfür ein entsprechendes Berechtigungsprofil vorhanden sein.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Formatkonvertierungen in ein Inhouse-Format sind in der WDV 2017 nicht vorhanden, weshalb immer nur das originäre Dokument in der Archivierung enthalten ist – die ursprünglich in das Unternehmen eingegangene Datei wird immer in der Originalversion aufbewahrt und wird nicht gelöscht

- ✓ Eine Datenträgerüberlassung der Archiv-Daten nach Z2 oder Z3 war bisher von keinem Betriebsprüfer gefordert; sofern dies der Fall sein sollte, wenden Sie sich bitte mit der Bereitstellungsaufforderung des Betriebsprüfers an unsere Service-Team

- ✓ Für den Datenzugriff nach Z1 können Sie in der WDV ein entsprechendes Berechtigungsprofil definieren, und dem Betriebsprüfer damit für den Prüfungszeitraum (Mandanten bzw. Wirtschaftsjahre sowie Firmen und steuerrelevante Dokumentenarten lesenden Zugriff gewähren. Wir beraten Sie gerne, wie Sie Ihr Archivsystem aufbauen, so dass der Betriebsprüfer genau die Daten bereit gestellt bekommt, die für die Betriebsprüfung relevant sind

8.2 Auslagerung und Migration

Nach den GoBD darf im Fall eines Systemwechsels, einer Systemänderung oder einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem von einer Aufbewahrung bislang verwendeter Hard- und Software nur dann abgesehen werden, wenn eine maschinelle Auswertbarkeit der Daten nebst Stammdaten und Verknüpfungen durch das neue oder ein anderes System gewährleistet ist. Ein Systemwechsel oder eine Auslagerung von Daten aus der Produktivumgebung ist nur zulässig, wenn quantitativ und qualitativ weiterhin die gleichen Auswertungsmöglichkeiten ermöglicht werden.

Bei der Migration von DMS-Umgebungen können die Anforderungen an die Beibehaltung der Auswertungsmöglichkeiten einfacher erfüllt werden als bei der Migration einer ERP-Umgebung oder der Auslagerung von Daten aus einer ERP-Umgebung in ein DMS.
Ein DMS verfügt in der Regel über beschränkte Auswertungsmöglichkeiten. Diese beschränken sich i. d. R. auf indexbasierte Such- und Sortierfunktionen sowie die Möglichkeit einer Volltextsuche, ggf. sind Suchreports vorhanden.
Der Fokus bei DMS-Migrationen liegt auf dem Erhalt der Formate (wenn originär digital).
Ansonsten müssen im Rahmen von Systemumstellungen die bildliche oder inhaltliche Gleichheit sichergestellt werden.

Bei der Auslagerung von Daten aus der ERP-Umgebung in eine DMS-Umgebung liegen die Anforderungen an Beibehaltung der Auswertungsmöglichkeiten deutlich höher, da eine ERP-Umgebung über einen Funktionsumfang verfügt, die nicht ohne weiteres durch ein DMS abgedeckt werden kann.

Migrationen von Fremdsystemen in die WDV sowie (falls erforderlich) von der WDV in ein Fremdsystem sind grundsätzlich individuelle Projekte, bei welchen die Anforderungen der GoBD berücksichtigt werden.

8.3 Outsourcing / Auslagerung von DMS-Funktionen

Anforderungen an das Outsourcing sind nur indirekt in den GoBD enthalten. Für die Ordnungsmäßigkeit elektronischer Bücher und sonst erforderlicher elektronischer Aufzeichnungen, einschließlich der eingesetzten Verfahren, ist allein der Steuerpflichtige verantwortlich. Dies gilt auch bei einer teilweisen oder vollständigen organisatorischen und technischen Auslagerung von Buchführungs- und Aufzeichnungsaufgaben an Dritte (z. B. Steuerberater oder Rechenzentrum).

Wichtiger Hinweis:

Soweit rechnungslegungsrelevante Dienstleistungen ausgelagert werden, ist dem Entwurf einer IDW-Stellungnahme zur Rechnungslegung »Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing« (IDW ERS FAIT 5) Beachtung zu schenken.

Hier wird korrespondierend zu den GoBD ausgeführt, dass die Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen auch dann bei den gesetzlichen Vertretern des auslagernden Unternehmens verbleibt, wenn im Rahmen eines Outsourcings die Speicherung und Verarbeitung von rechnungslegungsrelevanten Daten von einem damit beauftragten Dienstleistungsunternehmen wahrgenommen wird.

Besonderheiten aus steuerlicher Sicht gilt es bei einer Auslagerung ins Ausland zu beachten. Gemäß § 146 Abs. 2 S. 1 AO sind Bücher und sonstige erforderliche Aufzeichnungen im Inland zu führen und aufzubewahren. Elektronische Bücher, Aufzeichnungen und Rechnungen dürfen jedoch nach § 146 Abs. 2a AO auch ins Ausland verlagert werden. Der Unternehmer kann dazu beim zuständigen Finanzamt einen schriftlichen Antrag stellen. Dabei muss jedoch insbesondere sichergestellt sein, dass die GoB (einschließlich der GoBD) in vollem Umfang eingehalten werden.
Die Genehmigung ist insbesondere daran geknüpft, dass die Besteuerung im Inland nicht beeinträchtigt wird. Für Rechnungen existiert eine Sonderregelung (§ 14b UStG). Für umsatzsteuerliche Zwecke enthält § 14b UStG Sonderregelungen für die Aufbewahrung von Rechnungen, die die allgemeinen Aufbewahrungspflichten in der AO zum Teil verdrängen. Demnach sind Rechnungen, die ein inländischer Unternehmer ausgestellt bzw. empfangen hat, grundsätzlich im Inland aufzubewahren.

Eine elektronische Aufbewahrung dieser Rechnungen insbesondere im übrigen Gemeinschaftsgebiet setzt voraus, dass eine vollständige Fernabfrage (Online-Zugriff) der betreffenden Daten und deren Herunterladen und Verwendung gewährleistet ist.

Dabei hat der Unternehmer dem Finanzamt den jeweiligen Aufbewahrungsort mitzuteilen.
Ein Antrag des Unternehmers nach § 146 Abs. 2a AO und dessen Bewilligung durch das Finanzamt sind insoweit nicht erforderlich.

a) Wie die WDV 2017 diesen Grundsatz unterstützt:

- ✓ Sofern Sie sich für die Nutzung der WDV Archivierung in der Cloud entscheiden, oder die Archivierung ins PRAXIS Rechenzentrum auslagern möchten, versichern wir bereits an dieser Stelle, dass die Daten ausschließlich in gesicherten Rechenzentren der Telekom in Deutschland liegen.
- ✓ Der Zugriff auf die WDV-Archivierung erfolgt über einen Remote-Zugang, mit welchem Sie über die gleichen, vollen Zugriffsrechte auf die Archivierung verfügen, wie wenn der Server in Ihrem eigenen Server-Raum oder in Ihrem eigenen Rechenzentrum steht
- ✓ Die Nutzungsbedingungen / Vereinbarungen für die WDV Nutzung in der Cloud (Rechenzentrum) werden gesondert vertraglich vereinbart

b) Was muss geregelt, gewährleistet und dokumentiert sein

- ✓ Vertragliche Vereinbarung für die Nutzung der WDV Archivierung in der Cloud wird gesondert getroffen
- ✓ Hier sind die entsprechenden Zugriffs- und Kontrollrechte sowie die Verfügbarkeit geregelt
- ✓ Die Verfahrensdokumentation für Ihre DMS-Prozesse ist analog zu erstellen
- ✓ Sonstige Vereinbarungen / Definition der Rahmenbedingungen / Dokumentationspflichten des Cloud-Service-Anbieters sowie Service-Level-Agreement und Störungsbehandlung sind ebenfalls separat zu vereinbaren

9 Verfahrensdokumentation / IKS

9.1 Erstellung und Umgang mit der Verfahrensdokumentation

Ein sehr wichtiger Punkt der geltenden GoBD ist die Verfahrensdokumentation. Alle steuerpflichtigen Unternehmen müssen in der Verfahrensdokumentation genau beschreiben, wie Belege und Dokumente erfasst, empfangen, digitalisiert, verarbeitet, ausgegeben und aufbewahrt werden. Die Verfahrensdokumentation soll den kompletten organisatorischen und technischen Prozess der digitalen Archivierung innerhalb eines Unternehmens darstellen.

Die Pflicht zur Erstellung einer Verfahrensdokumentation gilt grundsätzlich, unabhängig von der Größe oder Komplexität des Unternehmens.

„Die Verfahrensdokumentation beschreibt den organisatorisch und technisch gewollten Prozess, zum Beispiel bei elektronischen Dokumenten von der Entstehung der Informationen über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit der Absicherung gegen Verlust und Verfälschung und der Reproduktion.“

Im optimalen Fall erfolgt die Verfahrensdokumentation in Form eines Datenfluss-Diagramms in welchem die relevanten Geschäftsprozesse abgebildet werden:

Beispiel:

- Wie erfolgt der Prozess / das Verfahren der elektronischen Erfassung von Papierdokumenten – also die Überführung in ein elektronisches Dokument (Scan-Vorgang). Dieser Prozess muss klar definiert und in der Verfahrensdokumentation beschrieben werden.

- Resultierend muss aus der Verfahrensdokumentation erkennbar sein, wie die elektronischen Belege erfasst, verarbeitet, ausgegeben und aufbewahrt werden.

- Ebenfalls Bestandteile der Verfahrensdokumentation sind die Beschreibung des Internen Kontrollsystems (IKS) und der Vorgehensweise zur Datensicherung (Datensicherungsplan)!!!!!

- Ggf. bestehende automatische Buchungsvorgänge müssen nachvollziehbar sein.

- Die Unveränderbarkeit und Pflege der Verfahrensdokumentation ist sicher zu stellen; Es ist auf eine korrekte Versionierung/Historisierung der Dokumentation zu achten.
  Dazu sollte es Regeln geben, bei welchen Änderungen eine Anpassung der Verfahrensdokumentation erforderlich ist und wann nur referenzierte Dokumente fortgeschrieben werden.

- Es ist permanente Aktualisierung der Änderungshistorie ist zu gewährleisten. Für jeden Zeitpunkt in der Vergangenheit sollte das damals gültige Soll-Verfahren aus der Dokumentation einfach ersichtlich sein (insbesondere soweit damals Unterlagen betroffen waren, die aktuell noch aufbewahrungspflichtig sind).

- Wenn eine Änderung nur geringe Auswirkung auf die Ordnungsmäßigkeit hat (z. B.: Vorhandener Benutzer bekommt ein Recht, Annotationen anzufügen), können solche Änderungen auch zeitversetzt (z. B.: Prüfung der Dokumentation am Geschäftsjahresende) erfolgen.

- Um die Unveränderbarkeit der Dokumentation sicherzustellen, kann die Ablage und Verwaltung der Dokumente der Verfahrensdokumentation im DMS erfolgen oder durch einen Ausdruck erreicht werden.

- Die Verfahrensdokumentation gehört zu den Arbeitsanweisungen und sonstigen Organisationsunterlagen i. S. d. § 257 Abs. 1 HGB bzw. § 147 Abs. 1 AO und ist über die gesetzliche Aufbewahrungsfrist von 10 Jahren aufzubewahren. Dies schließt nicht nur den aktuellsten Stand ein, sondern auch alle vorangegangenen Versionen innerhalb des Aufbewahrungszeitraums.
  Die Aufbewahrungsfrist für die Verfahrensdokumentation läuft nicht ab, soweit und solange die Aufbewahrungsfrist für die Unterlagen noch nicht abgelaufen ist, zu deren Verständnis sie erforderlich ist.

- Vorhandene Dokumentationen, auf die verwiesen werden könnte, sind typischerweise: Fachkonzepte, IT-Konzepte, Arbeitsanweisungen, Organisationshandbücher etc.
  Einfache Verlinkungsmöglichkeiten zum Verweis auf vorhandene Beschreibungen sind einzurichten.

- Zuständigkeiten für die Erstellung und Pflege sind zu regeln

Kurze Checkliste zur Verfahrensdokumentation

- ✓ Sind alle relevanten Prozesse und Tätigkeiten durch Verfahrens- und Arbeitsanweisungen dokumentiert – sind diese ev. Bestandteil eines ISO-QM-Handbuchs bereits vorhanden und müssen ev. nur aktualisiert werden?

- ✓ Sind alle relevanten automatischen Bearbeitungsschritte dokumentiert? Hier ist die Dokumentation in Form eines Datenflussdiagramms / Prozessdiagramms zu empfehlen.

- ✓ Liegen ggf. im Rahmen des ISO-QM-Handbuchs aktuelle interne Verfahrensübersichten bzw. ein Verfahrensverzeichnis vor? Werden diese bei Veränderungen zeitnah gepflegt?

- ✓ Liegt eine Anwenderdokumentation und technische Systemdokumentation für sämtliche IT-Systeme im Unternehmen (Benutzerhandbuch, Administrationshandbuch usw.) vor?

- ✓ Wurden die gelieferten Dokumentationen ggf. durch die Darstellung von unternehmens-spezifischen / individuellen Anpassungen ergänzt?

9.2 Inhalte einer Verfahrensdokumentation

Aus der Verfahrensdokumentation muss ersichtlich sein, wie die elektronischen Belege erfasst, empfangen, verarbeitet, ausgegeben und aufbewahrt werden. Die konkrete Ausgestaltung dieser Verfahrensdokumentation ist abhängig von der Komplexität und Vielfalt der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten IT-Systems. Der Umfang der im Einzelfall erforderlichen Dokumentation wird dadurch bestimmt, was zum Verständnis des IT-Verfahrens, der Bücher und Aufzeichnungen sowie der aufbewahrten Unterlagen notwendig ist.

Über die formale Gestaltung und technische Ausführung kann der Buchführungspflichtige individuell entscheiden. Eine konkrete Definition der Inhalte einer Verfahrensdokumentation wird auch in den GoBD nicht gegeben. Es gibt nur den Hinweis, dass eine Verfahrensdokumentation in der Regel aus einer allgemeinen Beschreibung, einer Anwenderdokumentation, einer technischen Systemdokumentation und einer Betriebsdokumentation besteht. Dabei kann die Verfahrensdokumentation aus mehreren Dokumenten bestehen oder auf andere Dokumente verweisen, beispielsweise auf die Anwenderdokumentation, auf Testdokumentationen oder grundsätzliche Steuerungs- und Kontrollkonzepte (IT-Risikomanagement und allgemeines Sicherheitskonzept, Bedrohungen und Maßnahmen, IT-Strategie, IT-Sicherheitsrichtlinie etc.). Die Verfahrensdokumentation hat dabei stets der in der Praxis eingesetzten Version des IT-Systems zu entsprechen und ist über die Dauer der Aufbewahrungsfrist in der jeweils gültigen Fassung (historisiert) aufzubewahren.

Die DMS-Verfahrensdokumentation beschreibt den organisatorisch und technisch gewollten Prozess bei Dokumenten, von der Entstehung über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, der Absicherung gegen Verlust und Verfälschung und der Reproduktion. Ausgehend von diesen Inhalten können sich durchaus Unterschiede im inhaltlichen Aufbau ergeben, bspw. durch:

- ✓ Organisationsdurchdringung, Anzahl der die Lösung einsetzenden Bereiche und Abteilungen.
- ✓ Anzahl Produkte, Module von unterschiedlichen Herstellern.
- ✓ Umfang an unterschiedlichen Prozessen, bspw. Scannen, Druckdaten-Archivierung, E-Mail-Archivierung, EDI-Verarbeitung, Rechnungsfreigabe, Kreditorenakte etc.
- ✓ Einsatz von externen Dienstleistern, bspw. für IT-Betrieb oder Scandienstleistung.

Muster / Inhalt einer Verfahrensdokumentation

1.) Beschreibung der steuerrelevanten Dokumente
Beinhaltet die Zusammenstellung der Dokumentenarten, die Steuerrelevanz besitzen

2.) Beschreibung der steuerrelevanten Daten
Beinhaltet die Zusammenstellung der Datenbestände, die Steuerrelevanz besitzen

3.) Prüfung auf weitere Rechtsgrundlagen
Beinhaltet die Prüfung ob neben den steuerlichen Anforderungen an die Aufbewahrung weitere Rechtsgrundlagen relevant sind

4.) Kapitel: Aufbau- und Ablauforganisation
beinhaltet z.B.

- Darstellung des Unternehmens bzw. der Organisation sowie der organisationsspezifischen Schwerpunkte.
- Beschreibung des genauen Standorts des Systems.
- Verständliche Darstellung der Aufbauorganisation sowohl in Text-Form als auch grafisch.

5.) Kapitel: Sachlogische Lösung
beinhaltet z.B.

- Beschreibung der Rahmendaten und Aufgabenstellungen (Ziele) des DMS.
- Organisationsbeschreibung der betroffenen Bereiche.

- Gesamtauflistung aller durch die Systemlösung einzuhaltenden Richtlinien wie Gesetze, Verordnungen, Auflagen und Vereinbarungen.
- Beschreibung der Strukturen für Schlüsselverzeichnisse, Aktenplan, Dokumentenklassen, Aufbewahrungsfristen, Vernichtungsregelungen

6.) Kapitel: IT-Infrastruktur

Beinhaltet z.B.

- Übersichtliche Systemdarstellung mit allen Komponenten inkl. der Darstellung von Beziehungen zu vorgelagerten Systemen.
- Beschreibung der Softwarekomponenten (z. B. Standardsoftware, Individualsoftware, Systemkonfiguration, Anwenderoberflächen, Schnittstellen, Infrastrukturkomponenten).
- Beschreibung der technischen Hardwarekomponenten (z. B. Speichersysteme und Datenträger, Erfassungssysteme, Server etc.) soweit zum Verständnis der Lösung erforderlich.
- Beschreibung des Datenbankmodells.
- Dokumentation der Systemkonfiguration: Übersicht über die eingesetzten Programme, Parameter-Einstellungen je Programm.
- Beschreibung der Vorgehensweise der Datensicherung.
- Beschreibung der technischen Verarbeitungsregeln (z. B. Datenflüsse, Protokollierungen, Ablaufpläne etc.).
- Darstellungen zur Datensicherheit und Datenintegrität (Transaktions- und Konsistenzsicherung, Protokollierung, Ausfallsicherheit).
- Sicherstellung von Zugangs- und Zugriffsschutz (Benutzerverwaltung, Berechtigungskonzept).
- Sicherstellung des technischen Betriebs (Betriebsvoraussetzungen, Betriebsbedingungen).

7.) Kapitel: Prozesse allgemein

Beinhaltet z.B.

- Es muss ersichtlich sein, wie die Belege erfasst, empfangen, verarbeitet, ausgegeben und aufbewahrt werden.
- Weitere Dokumentationen zum Löschen von Dokumenten, Ändern von Dokumenten sowie fach- und systemadministrativen Prozessen.

8.) Kapitel: Erfassungsprozesse

Beinhaltet z.B.

- Digitalisierung (Scannen).
- Übernahme von originär digitalen Dokumenten (Dateien, E-Mails).
- Automatisierte Übernahme von digitalen Massendaten (COLD, Import, EDI).
- Indizierung.
- Archivierung.

9.) Kapitel: Bearbeitungsprozesse

Beinhaltet z.B.

- Ändern von Objekten.
- Änderung der Indexstrukturen.
- Weiterleiten.
- Genehmigen.
- Speichern/Versionierung

10.) Kapitel: Recherche und Reproduktionsprozesse

Beinhaltet z.B.

- Zugriff über Client.
- Anwendungsintegration.
- Anzeige, Ausdruck
- Datenzugriff gemäß GoBD.

11.) Kapitel: Internes Kontrollsystem

Beinhaltet z.B.

- Beschreibung des IKS.
- Zeitnahe Aktualisierung der Verfahrensdokumentation bei Systemänderungen.
- Auflistung der automatischen und manuellen Kontrollfunktionen in der Verfahrensdokumentation.

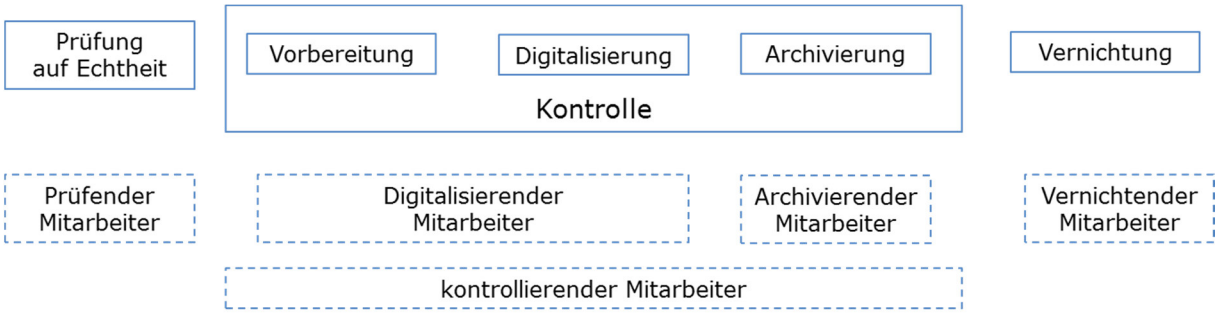
12.) Kapitel: sonstige relevante Dokumentationen und Inhalte

Beinhaltet z.B.

- Darstellung der vorhandenen Mitarbeiterqualifikation (Rollen, erforderliche Kenntnisse, durchgeführte Qualifizierungsmaßnahmen), Kompetenzen und Verantwortlichkeiten für den Betrieb.
- Organisationsanweisungen für die fachlichen Prozesse/Arbeitsanweisungen für den Standardbetrieb (z. B.: Scannen, Indizierung, Datensicherung, Umgang mit Datenträgern) und für Notfallszenarien (Restart, Recovery, K-Fall).
- Darstellung der Langfristverfügbarkeit (Migrationsmöglichkeiten, Bedingungen für die Migration).
- Vorgehensweise bei Test und Abnahme inkl. des eingesetzten Change-Management-Verfahrens.
- Darstellung der Wartungsregelungen (Verantwortlichkeiten, Eskalationswege, präventive Wartung, Störungsbehebung, Dokumentation).
- Verfahren zur Sicherstellung der Programmidentität (Identität von technischer Umgebung zur Dokumentation).

Beispiel-Auszug einer Beschreibung mit grafischer Abbildung

Um die Einhaltung der vorgegebenen Verfahren zu gewährleisten, werden regelmäßige Kontrollen durchgeführt. Diese orientieren sich an den tatsächlich aufgrund der organisatorischen Rahmenbedingungen zweckmäßigen und etablierten Aufgaben- und Funktionstrennungen, wobei von einzelnen funktionalen Verfahrensschritten ausgegangen wird.



10 Wesentliche Quellen- und Literaturverzeichnis

BMF-Schreiben vom 14.11.2017
Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.html

bitkom GoBD – Checkliste für Dokumentenmanagement-Systeme

https://www.bitkom.org/Bitkom/Publikationen/GoBD-Checkliste-fuer-Dokumentenshymanagement-Systeme.html

bitkom 10 Merksätze zur Archivierung von eMails im Unternehmen

https://www.bitkom.org/Presse/Presseinformation/Zehn-Merksaetze-zur-Archivierung-von-E-Mails-in-Unternehmen.html

PRAXIS

EDV-Betriebswirtschaft- und
Software- Entwicklung AG

Lange Straße 35
D 99869 Pferdingsleben / Gotha

Tel +49 (0) 36258 - 566-0
Fax +49 (0) 36258 - 566-40
Service Hotline +49 (0) 36258-566-101

Info@praxis-edv.de
www.praxis-edv.de

PRAXIS Academy

Lange Straße 40
D 99869 Pferdingsleben / Gotha

Tel +49 (0) 36258 - 566-0
Fax +49 (0) 36258 - 566-40
Service Hotline +49 (0) 36258-566-101

Info@praxis-edv.de
www.praxis-academy.de

Wir machen Erfolg messbar!

Ihr Uwe Wirth
Vorstand der PRAXIS AG

für den Mittelstand eG
10 Partner
10 Standorte
5 Schulungsstandorte
über 100 Experten
über 3000 Kunden

Tel. 0800-2020209
www.mybsm.eu
www.mittelstand-software.de

Microsoft Certified Database Administrator · Microsoft Certified Solution Developer · Microsoft Certified Professional · Microsoft Gold Certified Partner · Microsoft Certified Technology Specialist · SAP BusinessObjects OEM - Partner · Citrix Silber Partner

DATEV System-Partner · BVMW · TÜV PROFI CERT ISO 9001 73 100 503 · Herstellererteichung für Waage PWW/T nach LMET-66-01-0118/Q · PTB Waage PWW/T D01-09-012 · ITIL - Qualifizierung · TÜV PROFI CERT Integrierte Archivierung Reg.-Nr.: 70 900 503

Certified MESONIC SolutionPartner ERP · Certified MESONIC SolutionPartner HR · Certified MESONIC Competence Center · Certified MESONIC Development Consultant · Certified MESONIC SalesPartner

Henry Ford

Zusammenkommen ist ein Beginn,
Zusammenbleiben ein Fortschritt,
Zusammenarbeiten ein Erfolg.

EDV-Betriebswirtschaft- und Software-Entwicklung AG

Lange Straße 35
D 99869 Pferdingsleben (Thüringen)

Ansprechpartner:
Beate Volkmann, Geschäftsleitung

Tel.: +49 (0) 36258 566 0
Fax: +49 (0) 36258 566 40

info@praxis-edv.de

www.praxis-edv.de || www.wdv20xx.org

Branchen-Software (Schweiz)

Tel.: +49 (0) 36258 566 0
Fax: +49 (0) 36258 566 40

info@praxis-edv.de

www.praxis-branchen-software.ch

PRAXIS BAYERN

Freisinger Str. 28a
D 85764 Oberschleißheim

Ansprechpartner:
Dennis Richter, Geschäftsführer

Tel.: +49 (0) 89 21 59 64 03
Fax: +49 (0) 89 23 96 22 28

info@praxis-edv.bayern

www.praxis-edv.bayern

1989 Firmengründung

1997 Beginn WDV-Entwicklung

Seit **1997** entwickeln wir Software zur Abbildung der Prozessstrukturen für Unternehmen der Baustoffzulieferindustrie.

2013 Gründung Vertretung CH, BW

2014 Gründung Vertretung BY, A

2016 Vollständige Prozessintegration

Über **2500** WDV-Anwender in Zentrale und Verwaltung.
Über **1000** Anwender der WDV-Lieferschein-Erfassung an der Waage.
WDV in über **350** Firmen im Einsatz.
Abwicklung von jährlich mehr als **15 Millionen** Tonnen Material über WDV.
Software-Module in Französisch, Holländisch, Polnisch, Tschechisch und Englisch.
Abdecken aller Prozesse eines modernen Unternehmen der Baustoffzulieferindustrie.
Sichere und verschlüsselte Vernetzung aller Datenverbindungen über Bau-ELSE Cloud.

PRAXIS ist langjähriges Mitglied in diesen Fachverbänden