GoBD-Checkliste

für Dokumentenmanagement-Systeme

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Frank Früh | Bitkom e. V.
Bereichsleiter Bereichsleiter ECM
Tel.: 030 27576-201 | f.frueh@bitkom.org

Verantwortliches Bitkom-Gremium

Arbeitskreis ECM Compliance

GoBD-Checkliste

für Dokumentenmanagement-Systeme

Autoreninformationen

- Thorsten Brand, Zöller & Partner GmbH
- Stefan Groß, PSP Peters Schönberger GmbH
  Wirtschaftsprüfungs- und Steuerberatungsgesellschaft
- Wolfgang Heinrich, Easy Software AG

Disclaimer

Die vorliegende Checkliste gibt die persönliche Meinung der Autoren zur derzeitigen Rechtslage wieder und enthält lediglich einen Überblick über einzelne Themenkomplexe. Spezielle Umstände einzelner Fallkonstellationen wurden nicht berücksichtigt; diese können durchaus zu abweichenden Betrachtungsweisen und/oder Ergebnissen führen. Die Checkliste kann daher keine rechtliche oder steuerliche Beratung ersetzen; bitte holen Sie eine auf Ihre Umstände zugeschnittene, weitere Entwicklungen berücksichtigende Empfehlung Ihres Steuerberaters oder Wirtschaftsprüfers ein, bevor Sie Entscheidungen über die in diesem Leitfaden besprochenen Themen treffen. Die Finanzverwaltung und/oder Gerichte können abweichende Auffassungen zu den hier behandelten Themen haben oder entwickeln.

Inhaltsverzeichnis

Abkürzungsverzeichnis 5

1 Einleitung 8
1.1 Zielsetzung dieser Checkliste 8
1.2 Die GoBD 8
1.3 Relevanz der GoBD für ein DMS 9
1.4 Weitere relevante Vorschriften für die elektronische Aufbewahrung 10
1.5 Aufbau und Verwendung der Checkliste 11

2 Allgemeine Anforderungen an DMS-Produkte und Lösungen 17
2.1 Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit 18
2.2 Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung 20
2.2.1 Vollständigkeit 20
2.2.2 Richtigkeit 22
2.2.3 Zeitgerechte Buchungen und Aufzeichnungen 24
2.2.4 Ordnung 26
2.2.5 Unveränderbarkeit 28

3 Anforderungen an einen ordnungsmäßigen IT-Betrieb 32
3.1 Generelle Anforderungen 32
3.2 IT-Infrastruktur und Rechenzentrumsbetrieb 34
3.3 Betriebsbedingungen und Wartung 36
3.4 Problembehebung und Support 38
3.5 Berechtigungssystem 40
3.6 Mitarbeiter 42

4 Erfassungs- und Verarbeitungsprozesse im DMS 47
4.1 Scannen von Papierdokumenten 47
4.2 Archivierung von Ausgangsdokumenten 50
4.3 Archivierung von E-Mails 52
4.4 Archivierung von Rechnungen 54

5 Besondere Anforderung aus steuerlicher Sicht 59
5.1 Maschinelle Auswertbarkeit und Datenzugriff 59
5.2 Auslagerung und Migration 62
5.3 Outsourcing/Auslagerung von DMS-Funktionen 64

6 Verfahrensdokumentation 68
6.1 Erstellung und Umgang mit der Verfahrensdokumentation 68
6.2 Inhalte einer Verfahrensdokumentation 70

7 Glossar 73

8 Die Autoren 79

Abkürzungsverzeichnis

Abkürzung	Definition
AO	Abgabenordnung
BMF	Bundesministerium der Finanzen
COLD	Computer Output on Laserdisk
DMS	Dokumentenmanagement-System
DPI	Dots per Inch
ECM	Enterprise Content Management
EDI	Electronic Data Interchange
ERP	Enterprise Resource Planning
EStG	Einkommensteuergesetz
FeRD	Forum elektronische Rechnung Deutschland
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GoBIT	Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz
HGB	Handelsgesetzbuch
IDW	Institut der Wirtschaftsprüfer
IKS	Internes Kontrollsystem
OCR	Optical Character Recognititon
PDF	Portable Document Format
RPO	Recovery Point Objective
RTO	Recovery Time Objective
Rz.	Randziffer
TIFF	Tagged Image File Format
UStG	Umsatzsteuergesetz
XML	eXtensible Markup Language
ZUGFeRD	Zentraler User Guide des Forums elektronische Rechnung Deutschland

1 Einleitung

1 Einleitung

1.1 Zielsetzung dieser Checkliste

Mit einem Dokumentenmanagement-System (DMS [1]) lassen sich originär elektronische sowie digitalisierte Dokumente verwalten. Eine DMS-Anwendung dient der Organisation und Koordination der Erstellung, Überarbeitung, Überwachung und Verteilung sowie der geordneten Aufbewahrung von Dokumenten und Informationen unterschiedlichster Art über ihren gesamten Lebenszyklus bzw. ihre vorgegebene Aufbewahrungsfrist im Unternehmen. Neben der Aufbewahrung für rein betriebliche Belange ist eine Vielzahl von Dokumenten aufgrund gesetzlicher Pflichten aufzubewahren. Dabei handelt es sich häufig um sogenannte steuerrelevante Dokumente oder Daten, die insbesondere zum Zwecke der Betriebsprüfung vorgehalten werden müssen.

Die Vorgaben für die Aufbewahrung und Verfügbarmachung sind in gesetzlichen Grundlagen (AO, HGB, UStG) sowie insbesondere in den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) niedergelegt, welche spezielle Anforderungen an IT-gestützte Prozesse aus Sicht der Finanzverwaltung erheben.

Ausgehend von den Anforderungen der GoBD stellt die vorliegende Checkliste die sich daraus konkret ergebenden Anforderungen für ein DMS dar und gibt diverse Hilfestellungen, was es bei der Umsetzung innerhalb der Unternehmens-IT konkret zu beachten gilt. Die Checkliste richtet sich sowohl an die Hersteller von DMS-Anwendungen, als auch an Systemintegratoren sowie Anwender der entsprechenden Lösungen.

1.2 Die GoBD

Mit Schreiben vom 14. November 2014, den »Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen inelektronischer Form sowie zum Datenzugriff (GoBD)«, hat das BMF dargelegt, welche Vorgaben aus Sicht der Finanzverwaltung an IT-gestützte Prozesse zu stellen sind.[2] Die GoBD treten an die Stelle der GoBS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme)[3] sowie der GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)[4]. Damit kommt das BMF letztlich auch den Forderungen der Wirtschaft nach einer dringend erforderlichen Modernisierung der genannten

1 Die Begriffe DMS und ECM werden hier gleichbedeutend entsprechend der obigen Definition behandelt. Im Folgenden wird nur der Begriff DMS genutzt. Siehe auch Glossar.

2 BMF-Schreiben vom 14. November 2014 – IV A 4 – S 0316/13/10003, BStBl. I 2014, S. 1450.

3 BMF-Schreiben vom 7. November 1995 – IV A 8 - S 0316 - 52/95, BStBl. I 1995, S. 738.

4 BMF-Schreiben vom 16 Juli 2001 – IV S 2 – S 0316 - 36/01, BStBl. I 2001, S. 415.

Vorgaben nach und bringt ergänzend in der Zwischenzeit stattgefundene Entwicklungen[5] mit ein.

Die GoBD sind für Veranlagungszeiträume anzuwenden, die nach dem 31. Dezember 2014 beginnen und betreffen grundsätzlich alle Steuerpflichtigen mit Gewinneinkünften i. S. d. § 5 EStG, § 4 Abs. 1 EStG sowie auch nicht buchführungspflichtige Unternehmen, wie insbesondere Einnahmen-Überschuss-Rechner[6], soweit diese ihre unternehmerischen Prozesse IT-gestützt abbilden und ihren Buchführungs- und Aufbewahrungspflichten in elektronischer Form nachkommen.[7] Im Ergebnis dürfte damit die gesamte deutsche Unternehmenslandschaft betroffen sein.

1.3 Relevanz der GoBD für ein DMS

Auf der Grundlage von § 147 Abs. 2 AO können – abgesehen von bestimmten Ausnahmen – Unterlagen auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht. Die in den GoBD definierten Grundsätze, wie Unveränderbarkeit, Ordnung, Vollständigkeit oder Nachvollziehbarkeit müssen dabei auch von einem DMS erfüllt werden. Dabei muss sichergestellt sein, dass die Wiedergabe bzw. die Daten mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. Dazu ist weiter sicherzustellen, dass aufbewahrungspflichtige Unterlagen während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können.

Sind aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen im Unternehmen entstanden oder dort eingegangen, sind sie entsprechend den GoBD auch in dieser Form aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden. Sie dürfen daher nicht mehr ausschließlich in ausgedruckter Form aufbewahrt werden und müssen für die Dauer der Aufbewahrungsfrist unveränderbar erhalten bleiben.

Die Ablage von Daten und elektronischen Dokumenten in einem üblichen Dateisystem erfüllt – so die GoBD – die Anforderungen der Unveränderbarkeit regelmäßig nicht, soweit nicht zusätzliche Maßnahmen ergriffen werden, die eine Unveränderbarkeit gewährleisten. An dieser Stelle tritt die Notwendigkeit eines DMS deutlich zu Tage. Zugleich muss sich – bei Einsatz eines DMS – dieses an den Vorgaben der GoBD messen lassen. Dies betrifft insbesondere die Vorgaben an

5 Im Rahmen der GDPdU insbesondere Inhalte aus dem sog. Fragen- und Antwortenkatalog zum Datenzugriffsrecht der Finanzverwaltung, Stand: 22. Januar 2009, online abrufbar unter: http://www.elektronische-steuerpruefung.de/bmf/bmf-faqs-2009.pdf

6 Steuerpflichtige, die ihren Gewinn nach den Vorschriften des § 4 Abs. 3 EStG ermitteln.

7 Nach § 146 Abs. 6 AO gelten die Ordnungsvorschriften auch dann, wenn der Unternehmer elektronische Bücher und Aufzeichnungen führt, ohne dazu verpflichtet zu sein.

die Aufbewahrung und Bereitstellung (insbesondere für den Datenzugriff der Finanzverwaltung) entsprechender Dokumente und Datenbestände.

1.4 Weitere relevante Vorschriften für die elektronische Aufbewahrung

Auf Basis der wesentlichen Anforderungen der GoBD gibt diese Checkliste Empfehlungen, die eine Umsetzung in der Unternehmenspraxis unterstützen sollen. Diese können und sollen aufgrund der in den Unternehmen durchaus vorherrschenden Diversifikation nur eine Orientierungshilfe darstellen.

Zur ganzheitlichen Darstellung aller Anforderungen an die elektronische Aufbewahrung in einem DMS sollten insbesondere folgende Ausarbeitungen in die Betrachtung einbezogen werden:

- IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie
- IDW PS 880: Die Prüfung von Softwareprodukten
- IDW PS 951: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen
- IDW PS 980: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen
- IDW RS FAIT 3: Grundsätze ordnungsmäßiger Buchführung beim Einsatz
- elektronischer Archivierungsverfahren
- IDW ERS FAIT 5: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing
- BMF: Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung, Stand: 22. Januar 2009
- BMF-Schreiben: Vereinfachung der elektronischen Rechnungsstellung zum 1. Juli 2011 durch das Steuervereinfachungsgesetz 2011[8]
- GoBIT: Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz (Entwurf mit Stand: 13. Oktober 2012)[9]

8 BMF-Schreiben vom 2. Juli 2012 - IV D 2 - S 7287-a/09/10004 :003, BStBl. I 2012, S. 726, online abrufbar unter: http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2012-07-02-Vereinfachung-der-elektronischen-Rechnungsstellung.html

9 Die GoBIT waren ein Arbeitsvorhaben der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV). Nach Erscheinen der GoBD wurde die Arbeit an den GoBIT nicht weitergeführt. Der letzte veröffentlichte Entwurf enthält allerdings viele wertvolle Aussagen, die zur Umsetzung der GoBD hilfreich sein können. GoBIT (Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz) mit Stand: 13. Oktober 2012, unter: http://www.awv-net.de/cms/Fachinformationen/GoBIT/_AktuellerEntwurfderGoBIT,cat267.html

1.5 Aufbau und Verwendung der Checkliste

Während die GoBD dezidiert ausführen, welche Anforderungen an IT-gestützte Prozesse zu stellen sind, treffen sie keine Aussage, auf welche Weise das Unternehmen diese erfüllen kann. Der Grund hierfür liegt in der Technikneutralität, die es dem Unternehmen überlässt, die aus seiner Sicht (technisch und betriebswirtschaftlich) sinnvollste Lösung zu implementieren. So konstatieren die GoBD richtigerweise, dass technische Vorgaben und Standards angesichts der geringen IT-Halbwertszeiten sowie der sehr großen Unterschiede im organisatorischen Umfeld der verschiedenen Unternehmen nicht festgeschrieben werden können.

Es wird daher durchaus Fallkonstellationen geben, bei welchen nicht ausschließlich nach den GoBD entschieden werden kann, ob ein bestimmter Sachverhalt den Ordnungsmäßigkeitskriterien entspricht oder nicht. In solchen Situationen ist dann über einen Analogieschluss festzustellen, ob die Ordnungsvorschriften eingehalten wurden. Dabei lassen die GoBD auch explizit Vergleiche mit der herkömmlichen »Papierwelt« zu. So kann z. B. beurteilt werden, ob ein elektronischer Zugriffsschutz die gleiche Sicherheit bietet wie die Aufbewahrung von Papierdokumenten in einem verschlossenen Schrank.

Ausgehend von diesem Grundverständnis soll die Checkliste zunächst aufzeigen, WAS (Anforderungen, Ziele) gefordert ist, um darauf aufbauend Hilfestellung zu geben, WIE dies in der Unternehmenspraxis erreicht werden kann (i. A. beispielhafte Lösungen OHNE den Anspruch auf Vollständigkeit). Auf diese Weise werden einerseits geeignete Maßnahmen für eine GoBD-konforme Implementierung definiert, andererseits lassen sich Prüfkriterien zur Beurteilung entsprechender Systeme und Installationen ableiten.

Die Checkliste führt von den grundsätzlichen Anforderungen zu den Anforderungen für den IT-Betrieb im Allgemeinen. Dann wird auf die Besonderheiten einer DMS-Umgebung eingegangen. Abschließend werden die Anforderungen an eine DMS-Verfahrensdokumentation dargestellt.

Die Checkliste besitzt im Einzelnen den folgenden Aufbau:

Kapitel	Inhalte
Allgemeine Anforderungen an DMS-Produkte und Lösungen	Grundsätze der GoBD, wie Nachvollziehbarkeit, Vollständigkeit, Richtigkeit, Ordnung oder Unveränderbarkeit werden dargestellt und deren Umsetzungsmöglichkeiten für ein DMS erläutert.
Anforderungen an einen ordnungsmäßigen IT-Betrieb	Allgemeine Anforderungen an den IT-Betrieb werden unabhängig vom Einsatz einer DMS-Umgebung betrachtet.
Erfassungs- und Verarbeitungsprozesse im DMS	Besonderheiten von einzelnen DMS-Prozessen, wie z. B. Scanning, E-Mail-Archivierung, Verarbeitung von elektronischen Rechnungen, werden aufgezeigt.
Besonderheiten aus steuerlicher Sicht	Auf besondere Anforderungen, die sich aus steuerlicher Sicht ergeben, aber nicht direkt im Zusammenhang mit der Aufbewahrung von Dokumenten stehen, wird Bezug genommen. Betroffen sind Anforderungen an die maschinelle Auswertbarkeit, das Outsourcing eines DMS sowie Systemabschaltungen/Migrationen.
Verfahrensdokumentation	Es werden Hinweise zum Aufbau (Gliederung) und zu den Inhalten einer DMS-Verfahrensdokumentation gegeben.

2 Allgemeine Anforderungen an DMS-Produkte und Lösungen

2 Allgemeine Anforderungen an DMS-Produkte und Lösungen

Die GoBD formulieren in Kapitel 3 Allgemeine Anforderungen für den Einsatz steuerrelevanter IT-Systeme:

- Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit (siehe GoBD-Kapitel 3.1),
- Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung (siehe GoBD-Kapitel 3.2), mit den Einzelthemen
  - Vollständigkeit (siehe GoBD-Kapitel 3.2.1),
  - Richtigkeit (siehe GoBD-Kapitel 3.2.2),
  - Zeitgerechte Buchungen und Aufzeichnungen (siehe GoBD-Kapitel 3.2.3),
  - Ordnung (siehe GoBD-Kapitel 3.2.4),
  - Unveränderbarkeit (siehe GoBD-Kapitel 3.2.5).

Diese Grundsätze sollen sicherstellen, dass die Geschäftsvorfälle in der Buchhaltung vollständig und korrekt abgebildet werden, sodass die Prüfbarkeit über die Dauer der gesetzlichen Aufbewahrungsfristen gewährleistet ist. Die Grundsätze beziehen sich insbesondere auf die Kernsysteme der Buchhaltung wie z. B. ERP-Systeme, Lohnbuchhaltung oder Anlagenbuchhaltung. Auch ist ein DMS als Neben- oder Hilfssystem von entsprechender Relevanz. Es enthält erfasste Daten und Belege (z. B. durch Scannen von Papierunterlagen) und übernimmt die längerfristige Speicherung (Aufbewahrung) von Daten und Dokumenten. Dabei ist sicherzustellen, dass die Unterlagen (inkl. der Stamm- und Indexdaten) vollständig und fehlerfrei erfasst werden und während der Aufbewahrung keine Daten oder Dokumente verloren gehen oder verfälscht werden.

Nachfolgend werden zunächst die wesentlichen generellen Anforderungen an ein DMS aufgeführt. Darauf aufbauend soll anhand von ausgewählten typischen Lösungen und Beispielen aufgezeigt werden, wie sich diese Anforderungen in die Praxis umsetzen lassen. Spezielle Anforderungen an bestimmte DMS-Prozesse werden in Kapitel 4 Erfassungs- und Verarbeitungsprozesse im DMS behandelt.

Anmerkung

Manche aktuellen DMS-Produkte verfügen über umfangreiche Anpassungsmöglichkeiten. Damit können beim einzelnen Anwender im DMS sehr »buchungsnahe« Funktionen realisiert werden, die über die oben genannte typische Rolle eines DMS weit hinausgehen. Soweit derartige Zusatzfunktionen implementiert sind, bedürfen diese stets einer gesonderten – auf den Einzelfall bezogenen – Beurteilung, die nicht Gegenstand dieser Checkliste ist.

2.1 Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit

a) Grundsatz GoBD

Die Verarbeitung der einzelnen Geschäftsvorfälle sowie das dabei angewandte Buchführungs- oder Aufzeichnungsverfahren müssen nachvollziehbar sein (GoBD-Kapitel 3.1; Rz. 30–35). Insbesondere sollen die Aufzeichnungen eine progressive und retrograde Prüfbarkeit ermöglichen. Außerdem soll einem sachverständigen Dritten (u. a. Betriebsprüfer) in angemessener Zeit ein Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens ermöglicht werden. Hierfür ist in der Regel eine sogenannte Verfahrensdokumentation erforderlich.

Eine lückenlose Verfolgung der Geschäftsvorfälle von der Entstehung bis zur Abwicklung muss für die gesamte Dauer der Aufbewahrungsfrist möglich sein.

b) Kontrollziel

Sicherstellung der retrograden und progressiven Prüfbarkeit von Buchführungs- und Aufzeichnungsverfahren sowie der dazugehörigen Daten und Dokumente.

c) Auswirkungen auf ein DMS

Die rechnungslegungsrelevanten DMS-Prozesse müssen durch eine geeignete Dokumentation nachvollziehbar sein (vgl. Kapitel 6 Verfahrensdokumentation). Die Anforderungen an die Nachvollziehbarkeit, die über die Verfahrensdokumentation abgedeckt werden, sind dort beschrieben.

Protokollfunktionen im DMS dienen einerseits dazu, den ordnungsmäßigen Betrieb nachzuweisen, d. h. man kann anhand der Systemprotokolle verifizieren, dass das DMS tatsächlich so, wie in der Verfahrensdokumentation beschrieben, betrieben wurde. Zum anderen können durch Protokolle auch einzelne Geschäftsvorfälle im Detail nachvollzogen werden (z. B.: Wann wurde ein bestimmtes Dokument erfasst oder archiviert?).

Bei der Protokollierung muss ggf. der Zielkonflikt mit den Belangen des Datenschutzes aufgelöst werden. Dabei ist auch zu berücksichtigen, welche Informationen bereits in anderen rechnungslegungsrelevanten IT-Systemen protokolliert werden.

Die Protokolle selbst sind gegen unberechtigten Zugriff zu schützen und über die gesamte Aufbewahrungsfrist gegen Verlust und Verfälschung zu sichern. Hier bietet es sich meist an, die Archivkomponente des DMS zur Speicherung der Protokolle zu verwenden. Auch die Dokumente der Verfahrensdokumentation selbst sollten im elektronischen Archiv gespeichert werden.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(1)	Nachvollziehbarkeit bei der Erfassung von Dokumenten	▪ Protokollierung der Erfassungsaktionen (Import, Scan, Indizierung, Qualitätssicherung) mit Datum/Uhrzeit und ggf. der beteiligten Personen.
(2)	Nachvollziehbarkeit von Änderungen an Dokumenten	▪ Protokollierung der zu ändernden Aktionen mit Datum/Uhrzeit und ggf. der beteiligten Personen. ▪ Eine Änderung erzeugt eine neue Version des Dokuments, sodass frühere Inhalte nachvollziehbar bleiben.
(3)	Nachvollziehbarkeit von administrativen Änderungen	▪ Protokollierung der Änderungen an Systemeinstellungen, auch bei direkten Datenbankzugriffen (seitens der Datenbankadministratoren).
(4)	Übereinstimmung des Echtbetriebs mit der Verfahrensdokumentation	▪ Implementierung von Regelungen zu Sichtung und Auswertung der Protokolle, u. a. zur schnellen Behebung technischer Fehler und zur Behandlung von sicherheitsrelevanten Vorfällen. ▪ Protokollierung von administrativen Einstellungen im DMS (Berechtigungseinstellungen, Indexregeln, Fristenänderungen etc.). ▪ Protokollierung von Fehlersituationen.
(5)	Nachvollziehbarkeit während der gesamten Aufbewahrungsfrist	▪ Verlust- und fälschungssichere Aufbewahrung der Protokolle entsprechend der gesetzlich vorgeschriebenen Aufbewahrungsfrist der Dokumente (im DMS sowie in anderen Systemen).
(6)	Nachvollziehbarkeit des gesamten DMS-Verfahrens	▪ Erstellung einer Verfahrensdokumentation für das DMS ▪ (vgl. Kapitel 6 Verfahrensdokumentation).
(7)	Kein Informationsverlust bei Konvertierungen	▪ Im Fall von Datenkonvertierungen und/oder Datenkompression werden geeignete Datenformate und Verfahren gewählt, sodass die Lesbarkeit der Dokumente sowie die maschinelle Lesbarkeit von Daten erhalten bleiben. ▪ Originär elektronische Dokumente müssen (zusätzlich) im Originalformat aufbewahrt werden. ▪ Siehe auch Kapitel 5 Besondere Anforderung aus steuerlicher Sicht.

2.2 Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung

2.2.1 Vollständigkeit

a) Grundsatz GoBD

Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen (GoBD-Kapitel 3.1; Rz. 36). Dies erfordert eine vollzählige und lückenlose Erfassung sämtlicher Sachverhalte. Die geforderte Vollständigkeit lässt sich grundsätzlich durch eine Kombination technischer und organisatorischer Kontrollen (Kontrollumfeld) realisieren.

b) Kontrollziel

Sicherstellung der Vollständigkeit der innerhalb eines DMS aufgezeichneten Geschäftsvorfälle.

c) Auswirkungen auf ein DMS

Bezogen auf ein DMS betrifft der Grundsatz der Vollständigkeit die lückenlose Erfassung aller rechnungslegungsrelevanten Dokumente und Daten. Jedes aufbewahrungspflichtige Dokument ist grundsätzlich einzeln und mit allen Bestandteilen zu erfassen. Dieser Grundsatz ist vor allem dann relevant, wenn das DMS die Vorgänge erstmalig erfasst. 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.

Vollständigkeit ist auch im Hinblick auf die Aufbewahrung von steuerrelevanten Daten von Relevanz, da alle vorliegenden steuerlichen Informationen vollständig und maschinell auswertbar – insbesondere auch ohne Verdichtung – zur Verfügung gestellt werden müssen.

Auch die Wahl des Archivierungsformates von Dokumenten kann indirekt die Vollständigkeit betreffen. Können aufgrund von nicht mehr anzeigbaren bzw. aufrufbaren Formaten Dokumente – insbesondere Buchungsbelege – nicht mehr angezeigt werden, gilt eine Buchführung als nicht mehr vollständig. Auf der anderen Seite ist zu beachten, dass gerade Ausgangsbelege nicht durchweg über die Dauer der Aufbewahrungsfrist reproduzierbar bleiben, insbesondere dann, wenn sich Stammdaten ändern und die Versionsstände keiner Historisierung unterliegen.

Spezielle Aspekte beim Scannen (bspw. Vermeidung von Doppelerfassung) und bei der Archivierung von E-Mails sind an anderer Stelle beschrieben (siehe Unterkapitel in Kapitel 4 Erfassungs- und Verarbeitungsprozesse im DMS).

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(8)	Vollständige Erfassung der Dokumente	▪ Betrifft insbesondere die Systemschnittstelle eines DMS. Alle Daten und Dokumente, die für eine Archivierung angeliefert werden, müssen auch verarbeitet werden. Fehler, die die Vollständigkeit betreffen, müssen nachvollziehbar sein. ▪ Neben technischen Systemprotokollen und Überwachungswerkzeugen können organisatorische Regelungen hilfreich sein (z. B.: Regelmäßige Prüfung, ob eine Anlieferung komplett verarbeitet wurde). ▪ Regeln für die manuelle Erfassung sind zu beachten (z. B. Manuelle Archivierung einzelner Dateien). ▪ Es ist sicherzustellen, dass logisch zusammengehörige Dateien komplett erfasst werden (z. B.: Netto-Daten und Hintergrund-Layout). ▪ In Bezug auf Maßnahmen beim Scannen und bei der E-Mail-Erfassung, siehe Kapitel 4 Erfassungs- und Verarbeitungsprozesse im DMS.
(9)	Vollständigkeit und Korrektheit von Daten, die von anderen Daten abhängen	▪ Anforderung ist durch historisierte (versionierte) Speicherung bei Änderung der Stammdaten zu gewährleisten. Damit lässt sich insbesondere sicherstellen, dass ein Dokument auf Basis der historischen Stammdaten rekonstruiert werden kann (z. B.: Rechnung an Kunden, dessen Adresse später in den Stammdaten geändert wurde).
(10)	Vollständigkeit und Korrektheit von Daten, die von Konfigurationsdaten abhängen	▪ Anforderung ist durch historisierte (versionierte) Speicherung von bestimmten Konfigurationsdaten des Systems zu gewährleisten. ▪ Bsp.: Zu einer Rechnung werden nur die (Netto-)Inhaltsdaten archiviert. Der (stets gleiche) Briefkopf wird bei der Dokumentanzeige (bzw. beim Drucken) dynamisch eingeblendet. Die versionierte Speicherung des Briefkopfs ermöglicht, auch nach späteren Änderungen im Briefkopf, stets die richtige Version anzuzeigen. ▪ Alternatives Vorgehen: Dokumente sollen später nicht mittels der Stammdaten und/oder Briefköpfe neu erzeugt (reproduziert) werden. Bereits bei ihrer Entstehung werden sie (basierend auf den dann gültigen Stamm- und Bilddaten) als Kopie im Archiv abgelegt. Die Dokumente können somit jederzeit ohne Zugriff auf andere Daten im DMS recherchiert werden.
(11)	Vollständige und lückenlose Übernahme von Dokumenten aus Fremdsystemen	▪ Durch manuelle oder automatische Prüfung/Abgleich von Protokollen sicherzustellen (z. B.: System A hat lt. Protokoll 1.000 Dokumente exportiert; somit muss auch das DMS 1.000 Dokumente importiert haben). ▪ Durch alternative Abgleiche mit externen Systemen zu gewährleisten (z. B.: Identifikation gescannter Barcode-Belege, die keiner Buchung im ERP zugeordnet werden können). ▪ Transaktionskontrolle bei Datenübernahme implementieren. Im Fehlerfall »weiß« das DMS damit, welche Dokumente nicht angekommen sind und daher erneut importiert werden müssen. ▪ Nutzung von DMS-Funktionen (Auswertung von Trefferlisten, Reports, Skripts) um zu kontrollieren, ob die Inhalte bestimmter Indexfelder eines Datenbestands lückenlos sind (z. B.: Lückenanalyse auf Basis von Belegnummern).
(12)	Vollständige und lückenlose Erfassung	▪ Implementierung eines übergreifenden Konzepts im Rahmen des Internen Kontrollsystems (IKS) zur Sicherstellung der vollständigen und lückenlosen Erfassung. Von den hier genannten (und anderen) organisatorischen und/oder technischen Maßnahmen müssen die geeigneten ausgewählt und passend kombiniert werden. ▪ Durchführung technischer und/oder organisatorischer Plausibilitätskontrollen bei Eingabe oder Übernahme von Daten. ▪ Zählen von Belegen und Abgleich mit den Verarbeitungsdaten. ▪ Feste Import-/Stapelgröße definieren (z. B.: Im Stapel von 100 Dokumenten).
(13)	Vermeidung doppelter Erfassung	▪ Implementierung automatischer Funktionen, welche die Doppelerfassung verhindern (z. B.: Durch die Definition des Indexfeldes »Rechnungsnummer« als »unique« im DMS wird darauf hingewiesen, dass mehrere Dokumente mit der gleichen Rechnungsnummer erfasst wurden, bspw. bei gescannter und kommentierter gescannter Eingangsrechnung). ▪ Implementierung von Mehrfachbelegungsanalysen (z. B.: Reports zur Entdeckung von doppelt vorkommenden Rechnungsnummern). ▪ Selbst erstellte Dokumente können einen längeren Bearbeitungsprozess durchlaufen, wobei im DMS mehrere Zwischenversionen gespeichert werden. Dabei ist technisch und/oder organisatorisch exakt zwischen (internen) Vorversionen und (rechnungsrelevanten) finalen Dokumenten zu unterscheiden. Bestimmte DMS bieten dazu passende »Lebenszyklus«-Funktionen an (z. B.: Status »in Arbeit«, »final« etc.).

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(14)	Vollständigkeit bis zum Ende der Aufbewahrungsfrist	▪ Keine Löschmöglichkeit vor dem Ende der Aufbewahrungsfrist. ▪ Keine automatisierte Löschung nach Ende der Aufbewahrungsfrist (z. B.: Stets alle Daten löschen, die älter als 11 Jahre sind). ▪ Keine automatisierte Löschung von Daten und Dokumenten, sondern für die Löschung zwingend eine organisatorische Freigabe einholen, um dem Umstand gerecht zu werden, dass entsprechend § 147 Abs. 3 S. 3 AO die Aufbewahrungsfrist nicht abläuft, soweit und solange die Unterlagen steuerlich von Bedeutung sind und deren Festsetzungsfrist noch nicht abgelaufen ist. Auch betriebliche Regelungen können eine längere Aufbewahrungsfrist erfordern.
(15)	Langzeitformate für Dokumente zur Sicherstellung der vollständigen Reproduzierbarkeit	▪ Grundsätzliche Beschränkung der Formate für die Langzeitarchivierung. ▪ Konvertierung aller Eingangsformate in ein Langzeitarchivierungsformat, wie PDF/A (Fehler-Handling erforderlich, da Konvertierung nicht immer fehlerfrei). ▪ Ursprungsformate müssen (unter dem gleichen Index) zusätzlich aufbewahrt werden.

2.2.2 Richtigkeit

a) Grundsatz GoBD

Geschäftsvorfälle sind in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften inhaltlich zutreffend durch Belege abzubilden, der Wahrheit entsprechend aufzuzeichnen und anhand von Belegen nachprüfbar zu kontieren (GoBD-Kapitel 3.1; Rz. 44). Demnach haben die Belege, Bücher und Aufzeichnungen die Geschäftsvorfälle inhaltlich zutreffend abzubilden.

b) Kontrollziel

Korrekte Aufzeichnung der Geschäftsvorfälle.

c) Auswirkungen auf ein DMS

Dem Grundsatz der Richtigkeit folgend hat das DMS sicherzustellen, dass die zu archivierenden Dokumente und Daten den geforderten Grad der Übereinstimmung mit dem Original aufweisen. Grundlage dieser Übereinstimmung ist die gesetzlich geforderte bildliche oder inhaltliche Übereinstimmung. Der Grundsatz der Richtigkeit bedeutet insbesondere, dass bei der Erfassung von Daten und Dokumenten durch das DMS keine Belege verloren gehen oder verfälscht werden dürfen. Insbesondere muss auch (die manuelle oder automatische) Indexierung zuverlässig sein.

Spezielle Aspekte beim Scannen (bspw. Belegoptimierung) und bei der Archivierung von E-Mails sind an anderer Stelle beschrieben (siehe Unterkapitel in Kapitel 4 Erfassungs- und Verarbeitungsprozesse im DMS).

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(16)	Korrekte Erfassung der Belege	▪ Betrifft die Eingangsschnittstellen eines DMS. Siehe hierzu die Maßnahmen beim Scannen und bei der E-Mail-Erfassung in Kapitel 4 Erfassungs- und Verarbeitungsprozesse im DMS.
(17)	Bildliche Gleichheit bei Eingangsdokumenten	▪ Siehe Kapitel 4.1 Scannen von Papierdokumenten.
(18)	Inhaltliche Gleichheit bei Ausgangsdokumenten	▪ Siehe Kapitel 4.2 Archivierung von Ausgangsdokumenten.
(19)	Korrekte Erfassung der Dokumente und Indexdaten	▪ Implementierung eines übergreifenden Konzepts im Rahmen des Internen Kontrollsystems (IKS) zur Sicherstellung der korrekten Erfassung (z. B.: Regelwerk für die Indizierung von Dokumenten). ▪ Von den im IKS hier genannten (und anderen) organisatorischen und/oder technischen Maßnahmen müssen die geeigneten ausgewählt und passend kombiniert werden.
(20)	Fehlerhandling	▪ Für fehlerhafte und unleserlich erfasste Seiten sowie fehlerhafte Dokumente und Dateien sollte ein Regelprozess hinsichtlich der Beanstandung bzw. Behebung implementiert sein. Dazu ist festzulegen, wie (im Detail) mit den fehlerhaften Dokumenten/Dateien umgegangen werden soll (z. B.: Clearing-Stelle, Rescan, Protokollierung etc).

2.2.3 Zeitgerechte Buchungen und Aufzeichnungen

a) Grundsatz GoBD

Das Erfordernis der Zeitgerechtheit verlangt, dass ein zeitlicher Zusammenhang zwischen den Vorgängen und der Belegsicherung besteht (GoBD-Kapitel 3.1; Rz. 45-52). Dies lässt sich auf Dauer durch eine geordnete und übersichtliche Belegablage erfüllen. Ist eine entsprechende Belegsicherung und Sicherstellung der Unverlierbarkeit wirksam eingerichtet, kann die eigentliche Buchung grundsätzlich zu einem späteren Zeitpunkt erfolgen.

b) Kontrollziel

Zeitnahe Belegsicherung/Sicherstellung der Unverlierbarkeit und Aufzeichnung der Geschäftsvorfälle.

c) Auswirkungen auf ein DMS

Sofern für die Aufbewahrung von Dokumenten und Daten ein DMS verwendet wird, verlangt die Anforderung der 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. Durch technische Maßnahmen ist zum anderen zu gewährleisten, dass die zur Archivierung vorgesehenen Daten und Dokumente möglichst zeitnah auf das endgültige Archivierungsmedium übertragen werden.

Generell ist diese Anforderung eher eine Aufgabe der allgemeinen Organisation und/oder der Gestaltung der ERP- und Fachsysteme. Aus DMS-Sicht muss dafür gesorgt werden, dass durch die DMS-Prozesse nicht zusätzliche Zeitverzögerungen entstehen, die dem o. g. Grundsatz zuwiderlaufen.

Archivierte Dokumente sollten mit einem Datumsfeld versehen werden, um die zeitnahe Archivierung zu dokumentieren und um den dadurch erfassten Geschäftsvorfall periodengerecht zuordnen zu können sowie um die Aufbewahrungspflicht einzuhalten.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise

(21)	Automatische Übernahme aus Anwendungen	▪ Automatische Übernahme aus Anwendungen, bspw.:
		  ▪ Fachanwendung übergibt aktiv Daten ins DMS (»push«).
		  ▪ DMS holt sich die Daten von der Fachanwendung (»pull«); dabei ggf. Zeitsteuerung durch Scripting o. ä.

(22)	Zeitnahe Überführung von Dokumenten	▪ Arbeitsanweisung zur zeitnahen Überführung von Dokumenten (sofern keine automatische Übernahme erfolgt).
(23)	Datumszuordnung	▪ Verwendung eines Datumsfeldes, aus dem der Archivierungszeitpunkt erkennbar ist (auch in Protokollen). Zeitzonen müssen ggf. beachtet werden. ▪ Verwendung eines Datumsfeldes für das fachlich korrekte Datum (z. B.: Beleg- oder Eingangsdatum).

2.2.4 Ordnung

a) Grundsatz GoBD

Die aufbewahrungspflichtigen Unterlagen müssen geordnet aufbewahrt werden (GoBD-Kapitel 3.1; Rz. 53-57). Insbesondere dürfen die geschäftlichen Unterlagen nicht planlos gesammelt und aufbewahrt werden.

b) Kontrollziel

Die Geschäftsvorfälle liegen geordnet im DMS vor.

c) Auswirkungen auf ein DMS

Die Grundsätze ordnungsmäßiger Buchführung beim Einsatz eines DMS gelten dann als durchgehend erfüllt, wenn die Einhaltung der Ordnungsmäßigkeitskriterien während der gesamten Aufbewahrungsfrist sichergestellt werden kann. Das DMS muss dabei eine ausreichende Indexstruktur vorweisen. Die Dokumente müssen mittels einer Indexstruktur identifizierbar und klassifizierbar sein. Hierzu zählt auch eine eindeutige Nummerierung, die auch automatisch vergeben werden kann.

Eine eindeutige Zuordnung zum jeweiligen Geschäftsvorfall muss möglich sein. Es wird von retrograder und progressiver Prüfbarkeit gesprochen. Der Erhalt dieser Verknüpfung zwischen Geschäftsvorfall, Index und Dokument muss während der gesamten Aufbewahrungsfrist gewährleistet sein.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(24)	Verknüpfung Buchung zu Beleg	▪ Bei Buchungsbelegen muss eine nachvollziehbare Verknüpfung/Navigation von der Buchung zum Beleg im DMS vorhanden sein (z. B.: Verknüpfungen aus dem Fachsystem und den Doc-IDs im DMS). ▪ Bei der Zusammenfassung von mehreren Belegen zu einem elektronischen Dokument (z. B.: Im Rahmen einer Altbestandsübernahme) ist zu gewährleisten, dass eine einfache Identifikation der darin enthaltenen Dokumente weiterhin möglich ist. Des Weiteren muss ersichtlich sein, welches der Ursprungsbeleg ist (ursprünglicher Inhalt).
(25)	Elektronische Ablagestrukturen	▪ Implementierung definierter Indexstrukturen, bspw. numerische Zuordnung, Dokumentarten, Datum etc. ▪ Implementierung definierter Aktenstrukturen, bspw. Kreditor-, Debitor oder Bestellakte (falls erforderlich). ▪ Sicherstellung, dass sich die Indexstrukturen inhaltlich an den buchhalterischen Gegebenheiten orientieren, d. h. Suchanfragen, Trefferlisten etc. müssen die fachlich relevanten Daten enthalten.
(26)	Definition der endgültigen Version/des finalen Dokumentes	▪ Sicherstellung einer eindeutigen Unterscheidbarkeit zwischen Arbeitsversionen und finalen Dokumentversionen. ▪ Implementierung einer eindeutigen Definition, wann ein Objekt in einem DMS, den »Archiv-Status« erreicht hat.
(27)	Keine individuellen Ablagestrukturen	▪ Vorgegebene Ablagestrukturen sind zwingend einzuhalten. Keine individuellen Ablagestrukturen für steuerrelevante Dokumente.
(28)	Mehrfachablage	▪ Im Falle der Notwendigkeit einer Mehrfachablage von Dokumenten (z. B.: Rechnungen zu einer Kundenakte und als Buchungsbeleg) sollten die damit verbundenen Regeln bei der Indizierung transparent sein.
(29)	Löschfunktionen	▪ Löschvorgänge von nicht mehr relevanten Dokumenten müssen nachvollziehbar sein, sodass diese Dokumente wiederhergestellt werden können. ▪ »Nachvollziehbar« wäre bspw. ein Protokoll. ▪ »Wiederherstellbar« wäre bspw. ein elektronischer Papierkorb.
(30)	Korrekte Erfassung von Indexdaten	▪ Implementierung von technischen und/oder organisatorischen Plausibilitätskontrollen bei Eingabe oder Übernahme von Daten. ▪ Verwendung von »typisierten« Indexfeldern und Eingaberegeln ▪ (z. B.: In ein Datumsfeld können keine Buchstaben eingegeben werden; Definition von maximalen Längen sowie von minimalen und maximalen Werten). ▪ Implementierung geeigneter Bedienelemente in den Erfassungsmasken (z. B.: »Datumspicker« statt Freitextfeld). ▪ Befüllung von Indexdaten aus vorhandenen Datenquellen (z. B.: Über Datenbank-Import). ▪ Einführung einer manuellen Qualitätssicherung (z. B.: 4-Augen-Prinzip). ▪ Nutzung der bereits bestehenden Daten in eingehenden Dokumenten (z. B.: Bei elektronischen Eingangsrechnungen im ZUGFeRD-Format sind etliche relevante Indexdaten, wie RE-Nr, RE-Datum etc. bereits im Dateiformat eingebettet und können durch geeignete Tools automatisch für die Indizierung übernommen werden).

2.2.5 Unveränderbarkeit

a) Grundsatz GoBD

Die GoBD fordern, dass das eingesetzte Datenverarbeitungsverfahren so auszugestalten ist, dass alle Informationen, welche in den Verarbeitungsprozess Eingang gefunden haben, nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden dürfen (GoBD-Kapitel 3.1; Rz. 58–60). Demnach darf eine Buchung oder Aufzeichnung (also auch ein Indexdatensatz oder ein archiviertes Dokument) nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist.

Die Unveränderbarkeit ist auch im Zusammenhang mit der Historisierung von Meta- und Stammdaten zu sehen. So sind Änderungen an Stammdaten auszuschließen

oder Stammdaten mit Gültigkeitsangaben zu historisieren, um die Verknüpfungen mit der jeweils korrekten Version der Stammdaten zu gewährleisten.

b) Kontrollziel

Nachvollziehbarkeit von Veränderungen und Löschungen.

c) Auswirkungen auf ein DMS

Das System muss eine Protokollierung von Veränderungen und Löschungen von und an den Dokumenten und Aufzeichnungen ermöglichen. Die Verknüpfung zum Geschäftsvorfall muss erhalten bleiben. Es geht hierbei nicht um die unveränderbare Ablage. Änderungen sind zulässig, solange diese nachvollziehbar sind. Diese Nachvollziehbarkeit kann durch Hardware, Software oder organisatorische Regelungen erzielt werden.

Neben der Nachvollziehbarkeit bei einer Änderung von Dokumenten wird auch die Nachvollziehbarkeit von Änderungen an Systemeinstellungen des DMS adressiert (bspw. Archivierungseinstellungen, Indexstrukturen, Scan-Profile).

In einem DMS vorhandene Kommentarfunktionen (bspw. grafische Hervorhebungen oder elektronische Post-it's) dürfen die Nachvollziehbarkeit nicht beeinflussen.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(31)	Unveränderbarkeit von Dokumenten	▪ Sicherstellung, dass Dokumente und deren Metadatenstrukturen nur nachvollziehbar verändert werden können. ▪ Sicherstellung der Nachvollziehbarkeit kann bspw. durch Versionierung von Indexdaten und Dokumenten erfolgen. ▪ Änderungen könnten auch grundsätzlich verboten werden. ▪ Dokumente in der Entwurfsphase bzw. im Entwurfsstatus können gelöscht und geändert, versioniert oder historisiert werden. ▪ Wenn gescannte Dokumente beim Transport von der Scan-Anwendung in das DMS nicht verändert wurden, kann dies z. B. anhand eines Hashwerts nachgewiesen werden, welcher beim Scanvorgang errechnet und im DMS verifiziert wird.
(32)	Unveränderbarkeit von Verknüpfungen	▪ Bei Verknüpfungen zu externen Systemen ist eine Unveränderbarkeit der Verknüpfungsinformationen (z. B.: Doc-ID) zu gewährleisten. ▪ Auch bei einem DMS-Wechsel (neue Doc-IDs) muss die Verknüpfung erhalten bleiben (z. B.: Protokollierung der Änderungen oder die Vergabe von externen (DMS-unabhängigen) Doc-IDs).
(33)	Technische Maßnahmen zur Unterstützung der Unveränderbarkeit	▪ Einsatz von technischen Sicherheitsmechanismen zur Kontrolle und Vermeidung von Änderungen (z. B.: Durch unveränderbare Speichermedien, Hashwerte, Signaturen). ▪ Es muss zwischen Funktionen unterschieden werden, die Änderungen verhindern (z. B.: Brennen der Dokumente auf DVD), diese nachvollziehbar und umkehrbar machen (z. B.: Protokollierung mit Vorher/Nachher-Werten) und sie nur nachvollziehbar machen, ohne dass ein Rückgängigmachen möglich ist (z. B.: Signatur).
(34)	Unveränderbarkeit von Notizen	▪ Bei Verwendung einer Notizfunktion muss das Original erkennbar bleiben und darf nicht verändert werden (z. B.: Eigener Grafik-Layer im Dokumenten-Viewer, der wieder ausgeblendet werden kann, oder separate Textnotizen/Notizfelder).
(35)	Dokumente mit elektronischen Signaturen	▪ Elektronische Signaturen dürfen nicht gebrochen werden.
(36)	Unveränderbarkeit bei administrativen Zugriffen	▪ Sicherstellung der Unveränderbarkeit/Nachvollziehbarkeit auch bei administrativem Zugriff (auch über Betriebssystem). ▪ Dies ist in der Praxis oft nur begrenzt möglich. Für Forderungen wie »auch der Administrator kann Protokolle nicht löschen/fälschen« ▪ oder »Verbergen der Dokumentinhalte vor dem Administrator«, gibt es oft nur begrenzte technische Umsetzungsmöglichkeiten und Hinweise. Das 4-Augen-Prinzip (z. B.: Geteiltes Admin-Passwort) kann hier Risiken minimieren.
(37)	Löschen (wenn vorhanden)	▪ Der Prozess der Löschung (logisch) von Indizes muss nachvollziehbar sein. ▪ Der Prozess der Löschung (logisch) von Dokumenten muss nachvollziehbar sein. ▪ Der Prozess der Löschung (physikalische Löschung vor Archivierung) von Dokumenten muss nachvollziehbar sein.

3 Anforderungen an einen ordnungsmäßigen IT-Betrieb

3 Anforderungen an einen ordnungsmäßigen IT-Betrieb

Ein verlässlicher, geregelter und nachvollziehbarer IT-Betrieb ist die unverzichtbare Grundlage für einen ordnungsmäßigen IT-gestützten Betrieb von Buchführungs- und Aufzeichnungsverfahren. Die entsprechenden Anforderungen lassen sich aus allgemeinen Grundsätzen der IT-Sicherheit und insbesondere aus folgenden Kapiteln der GoBD ableiten:

6. Internes Kontrollsystem (IKS) (siehe GoBD-Kapitel 6)
7. Datensicherheit (siehe GoBD-Kapitel 7)
8. Unveränderbarkeit, Protokollierung von Änderungen (siehe GoBD-Kapitel 8).

Sie gelten nicht nur für ein DMS, sondern für alle steuerrelevanten Systeme. Im Folgenden soll allerdings ausschließlich auf typische Ausprägungen und Lösungsmöglichkeiten für DMS eingegangen werden.

3.1 Generelle Anforderungen

a) Grundsatz

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 (GoBD-Kapitel 7; Rz. 103ff.). Werden die Daten, Datensätze und elektronischen Dokumente nicht ausreichend geschützt und können daher nicht mehr vorgelegt werden, so ist die Buchführung nicht mehr ordnungsgemäß.

b) Kontrollziel

Der IT-Betrieb ist ordnungsgemäß.

c) Auswirkungen auf ein DMS

Technische Themenbereiche sind hierbei bspw. 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.

d) Lösungen und Beispiele

Die Lösungen und Beispiele beziehen sich auf die grundsätzlichen Anforderungen sowie die technischen Lösungen und finden sich in den folgenden Unterkapiteln wieder.

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(38)	Ordnungsmäßigkeit und Nachvollziehbarkeit der fachlichen Prozesse	▪ Definition und Beschreibung der steuerrelevanten fachbezogenen Prozesse. Diese Prozesse betreffen i. d. R. mehrere IT-Systeme und nicht isoliert das DMS. ▪ Die Gesamtprozesse sind so zu gestalten, dass die Anforderungen der GoBD erfüllt sind. ▪ Oft werden diese übergreifenden Prozesse in einer Verfahrensdokumentation aufgeführt.
(39)	Ordnungsmäßigkeit und Nachvollziehbarkeit der IT-Prozesse	▪ Definition und Beschreibung der technischen Prozesse, die einen störungsfreien und verlässlichen Betrieb des DMS gewährleisten, wie z. B. regelmäßige Datensicherung oder Wiederanlaufprozesse nach Systemstörungen. ▪ Häufige Dokumentation dieser Prozesse in einer IT-nahen Dokumentation, bspw. in einem Betriebskonzept.
(40)	Kenngrößen DMS-Betrieb	▪ Definition und Ermittlung von Messgrößen ▪ Z. B.: Definition, wie lange ein Geschäftsprozess/System vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse ausfallen darf (Recovery Time Objective (RTO)) ▪ Z. B.: Definition, 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). Bei einem DMS dürfte dies gegen Null gehen.

3.2 IT-Infrastruktur und Rechenzentrumsbetrieb

a) Grundsatz

Technischer Betrieb der IT-Komponenten, um die Anforderungen an Verfügbarkeit und Vertraulichkeit umzusetzen. Da die GoBD technikneutral sind, werden keine technischen Vorgaben gemacht.

b) Kontrollziel

Ordnungsmäßiger IT-Betrieb, die DMS-Komponenten werden entsprechend der technischen Anforderungen betrieben.

c) Auswirkungen auf ein DMS

Die DMS-Server-Komponenten unterliegen i. d. R. den gleichen Sicherheitsanforderungen, wie andere IT-Komponenten. Relevante Themen sind Überwachung, Datensicherheit und -sicherung, Verfügbarkeit, Datenschutz, Zugangs- und Zugriffsschutz sowie Restart- und Katastrophenfall-Abdeckung.

Teilweise werden neben DMS-Server-Komponenten spezielle (einmal beschreibbare) Speichersysteme eingesetzt, die nur für die DMS-Umgebung genutzt werden. Diese müssen im Rahmen des allgemeinen Sicherheitskonzepts mit berücksichtigt werden.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(41)	Datensicherheit, Verfügbarkeit	▪ Schaffung gebäudetechnischer Voraussetzungen und Maßnahmen (z. B.: Aufstellung der DMS-Server in einem separaten Rechenzentrum mit Klimaanlage, Alarmanlage, Notstromversorgung, besonderen Brandschutzvorrichtungen etc.).
(42)	Zutritt	▪ Zutrittsregelung zum Rechenzentrum/Rechnerraum. ▪ Zugang zum Rechenzentrum nur für berechtigte Personen gestattet. ▪ Protokollierung des Zutritts.
(43)	Verfügbarkeit	▪ Die Maßnahmen zur Steigerung der Verfügbarkeit werden auf der Basis definierter Verfügbarkeitsziele/Kenngrößen getroffen. ▪ Hinweis: Nicht nur für das DMS, sondern für die gesamte Unternehmens-IT von Relevanz.
(44)	Datensicherung	▪ Implementierung eines übergreifenden Backup-Konzepts für alle IT-Anwendungen (nicht nur für das DMS). Das Konzept beschreibt Verantwortlichkeiten und Prozeduren (z. B.: Welche Datenbestände wann zu sichern sind). ▪ Einführung von regelmäßigen Testings, ob die Backups wieder zurückgeladen werden können (Restore-Test). ▪ Schutz der Sicherungskopien vor unberechtigtem Zugriff und gegen Verlust. ▪ Lagerung der Sicherungsdaten bzw. der Backup-Medien an einem anderen Ort (rechenzentrumsfern), sodass sie auch bei gravierenden Zerstörungen im Rechenzentrum (durch Feuer, Wasser etc.) noch verfügbar sind. ▪ In aktuellen IT-Anwendungen werden die relevanten Daten meist auf einem Server gespeichert, sodass sich ein Backup für Arbeitsplatzrechner erübrigt.
(45)	Storage-Medien	▪ Teilweise Verwendung spezieller Wechselmedien oder Storage-Subsysteme für ein DMS, für die ggf. spezielle Backup-Maßnahmen erforderlich sein können.
(46)	K-Fall-Abdeckung	▪ Implementierung von Reservesystemen, hoch verfügbaren Systemauslegungen (z. B.: Fail-Over-Cluster, ggf. an einem anderen Standort). ▪ Spannbreite reicht von »Reservesystemen für einzelne Komponenten« bis hin zu »kompletten Spiegel-Rechenzentren«.
(47)	Geordneter Wiederanlauf	▪ Erstellung eines Notfallplans für Restart und Recovery für den Fall, dass einzelne Komponenten ausfallen oder das ganze System ausfällt. ▪ »Restart«: Darunter wird der Wiederanlauf des DMS nach einer Betriebsstörung verstanden. Beim Restart werden herkömmliche IT-Mittel eingesetzt wie z. B. das Wiederholen von Importläufen oder das Einspielen von Backup-Daten. ▪ Vorab-Definition der verantwortlichen Rollen und die Prozeduren für einen Restart, ggf. in Form einer Arbeitsanweisung. ▪ Regelmäßige Recovery-Tests, bspw. Wiederaufsetzen des gesamten Systems nur aus den Backup-Medien.
(48)	Geordnetes Test- und Freigabeverfahren	▪ Durchführung geeigneter Tests vor der Freigabe eines neuen Verfahrens/Prozesses. ▪ Für Änderungen an bestehenden Verfahren sollten Regeln dafür existieren, in welchen Fällen Tests durchzuführen sind. Die Ausgestaltung der Tests ist vom jeweiligen Prozess abhängig.
(49)	Service und Support	▪ Wartungs- und Supportverträge mit Lieferanten der Komponenten für die Rechenzentrums-Infrastruktur schließen (z. B.: Klimaanlage, USV etc., s. o.) ▪ Verantwortlichkeiten für die Einschaltung des externen Supports festlegen (z. B.: Rollen, Eskalationsprozesse etc.).

3.3 Betriebsbedingungen und Wartung

a) Grundsatz

Die 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 Update-Regelungen.

b) Kontrollziel

Die Hard- und Software ist gemäß den Vorgaben des Anbieters implementiert.

c) Auswirkungen auf ein DMS

Der Grundsatz gilt für alle IT-Systeme gleichermaßen, sodass sich für ein DMS keine speziellen Aspekte ergeben.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(50)	Betriebsbedingungen Hardware	▪ Einhaltung der Betriebsbedingungen für Hardware (z. B.: Durch Klimatisierung von Räumen, Staubfilter, maximale Leitungslängen bei Netzwerken etc.) ▪ Dies sollte bei der Freigabe der Hardware sowie bspw. bei baulichen Veränderungen überprüft werden.
(51)	Hardware-Wartung	▪ Hardware-Wartung erfolgt nach definierten Wartungsplänen gemäß den Empfehlungen der Hersteller. ▪ Anmerkung: Dies bezieht sich vor allem auf Geräte mit mechanischen Teilen, insbesondere Scanner. Andere Komponenten wie z. B. Server werden oft nicht vorbeugend gewartet, sondern nach wenigen Jahren ausgetauscht. Störungen werden dann bei Bedarf im Rahmen des Supports (s. u.) behoben. Die konkrete Ausgestaltung des Wartungs- und Supportkonzepts hängt sehr stark vom Einzelfall ab und sollte systemübergreifend für alle IT-Anwendungen erfolgen. Entscheidend ist, dass das Konzept die gewünschte Verfügbarkeit gewährleistet.
(52)	Zuverlässigkeit der Hardware	▪ Einrichtung von Zuständigkeiten und Regeln für Austausch und Update von Hardware. Insbesondere soll nur Hardware verwendet werden, für die noch Wartung/Support verfügbar ist. ▪ Anmerkung: I. d. R. wird die Nutzungsdauer von Hardware von Beginn an so geplant, dass die Wahrscheinlichkeit von Störungen während der Nutzungsdauer gering ist.
(53)	Betriebsbedingungen Software	▪ Einhaltung der Betriebsbedingungen für Software. Dabei sind die Freigaben der Hersteller für bestimmte Betriebssysteme, Datenbanken etc. zu beachten. ▪ Dies sollte bei der Freigabe von Softwarekomponenten und Updates sowie bei Veränderungen in der Systemumgebung überprüft werden.
(54)	Software-Wartung	▪ Da Hersteller von Software regelmäßig Updates und neue Produktreleases zur Verfügung stellen, sollten Zuständigkeiten und Regeln definiert sein, ob und wann solche Updates eingespielt werden (Freigabeverfahren).
(55)	Wartungs-Dokumentation	▪ Protokollierung von Wartungsmaßnahmen, Austausch von Hardware sowie das Einspielen von Updates und neuen Releases.

3.4 Problembehebung und Support

a) Grundsatz

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.

b) Kontrollziel

Zeitnahe und vollständige Wiederherstellung der Systeme und Daten bei Störungen und Ausfällen.

c) Auswirkungen auf ein DMS

Der Grundsatz gilt für alle IT-Systeme gleichermaßen, sodass sich für ein DMS keine speziellen Aspekte ergeben.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(56)	Helpdesk	▪ Einrichtung eines technischen IT-Helpdesks für Fachbenutzer. Bei Störungen der technischen Infrastruktur (z. B.: PC startet nicht, Netzwerk nicht verfügbar, Passwort abgelaufen etc.) müssen für Endbenutzer Ansprechpartner verfügbar sein. Diese beraten, können kleinere Probleme selbst lösen und ggf. den externen Support einschalten.
(57)	2nd-Level-Support	▪ Ggf. Einrichtung eines speziellen Helpdesks für Probleme mit dem DMS, das nicht mit dem allgemeinen IT-Helpdesk identisch ist. ▪ Ggf. können auch »Power-User« als erste Anlaufstelle fungieren.
(58)	Problembehebung durch den Hersteller (Hardware)	▪ Abschluss von Wartungs- und Supportverträgen mit den Lieferanten der Hardware mit garantierten Reaktionszeiten. ▪ Definition von Verantwortlichkeiten für die Einschaltung des externen Supports (Rollen, Eskalationsprozesse etc.).
(59)	Problembehebung durch den Hersteller (Software)	▪ Abschluss von Wartungs- und Supportverträgen mit den Lieferanten der Software mit garantierten Reaktionszeiten (»Produktsupport«). ▪ Ggf. Abschluss von Verträgen zum installationsspezifischen Support mit dem Systemintegrator (»Projektsupport«). ▪ Definition von Verantwortlichkeiten für die Einschaltung des externen Supports (Rollen, Eskalationsprozesse etc.).

10 Bei sehr differenziert definierten Berechtigungen steigt der administrative Aufwand und die Transparenz sinkt. Hier sollten Kosten und Nutzen sinnvoll abgewogen werden.

3.5 Berechtigungssystem

a) Grundsatz

Dokumente und Daten müssen gegen unberechtigte Kenntnisnahme, unberechtigte Eingaben, unberechtigte Veränderung und unberechtigtes Löschen wirksam geschützt werden.

b) Kontrollziel

Das Berechtigungssystem verhindert den unberechtigten Zugriff auf Dokumente und Daten und unterstützt somit die Ordnungsmäßigkeit (insbesondere Integrität und Authentizität).

c) Auswirkungen auf ein DMS

Ein wesentliches Mittel zur Erreichung dieses Ziels ist ein differenziertes Berechtigungssystem, das den lesenden und schreibenden Zugriff für einzelne Benutzer oder Benutzergruppen auf bestimmte Daten erlaubt oder verbietet. Die üblichen professionellen DMS-Softwareprodukte stellen entsprechende Funktionen zur Verfügung. Insbesondere sind durch das Berechtigungssystem nicht gewollte Veränderungen zu verhindern und administrative Aktionen nur einer begrenzten Benutzerzahl zur Verfügung zu stellen. Im Hinblick auf den Datenzugriff der Finanzverwaltung (vgl. Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff) bedarf es – bezogen auf die als steuerrelevant einzustufenden Daten und Dokumente – der Einrichtung einer Betriebsprüfer-Rolle mit Nur-Lesezugriff.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(60)	Berechtigungskonzept	▪ 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. ▪ Zugriffsberechtigungen spielen auch beim Schutz personenbezogener Daten (Datenschutz) eine entscheidende Rolle. Es empfiehlt sich daher ein gemeinsames Konzept, das sowohl die Belange der GoBD als auch die des Datenschutzes berücksichtigt.
(61)	Berechtigungen	▪ Als Grundlage jedes Berechtigungssystems müssen die Benutzer im DMS bekannt sein. Es empfiehlt sich insoweit eine rollenbezogene Benutzerverwaltung. ▪ Die Rollen sollten nach fachlichen Kriterien (Buchhalter, Scan-Operator etc.) definiert werden und kompatibel zu den Rollenbeschreibungen in den Prozessdefinitionen sein. ▪ Vergabe der Rechte pro Rolle und Zuordnung der Benutzer zu den einzelnen (ggf. mehreren) Rollen. Dies senkt den Administrationsaufwand und beeinflusst die Nachvollziehbarkeit und Transparenz positiv. ▪ Häufig existiert eine anwendungsübergreifende Benutzerverwaltung (z. B.: »Active Directory«), auf welche DMS-Lösungen i. d. R. zugreifen können. Bei Einsatz des DMS müssen dann in der übergreifenden Benutzerverwaltung ggf. weitere Rollen (z. B. »DMS-Administrator«) definiert werden. ▪ Eine getrennte Benutzerverwaltung nur für das DMS sollte möglichst vermieden werden.
(62)	Login-Regeln	▪ Ein Berechtigungskonzept umfasst auch die sichere Systemanmeldung (z. B.: Log-in-Regeln, Passwort-Regeln, Meldung fehlgeschlagener Log-ins, Sperrung bei mehrfach falsch eingegebenem Passwort etc.). ▪ Restriktivere Ausgestaltung der Regeln für administrative Rollen (z. B.: Passwortkomplexität) im Vergleich zum Standard-Nutzer. ▪ In der Praxis wird oft das sog. »Single Sign-on« verwendet, d. h. der Benutzer meldet sich beim Start seines Rechners einmalig unternehmensweit an und kann dann alle Fachsysteme (wie bspw. das DMS) ohne nochmalige Anmeldung nutzen.
(63)	Berechtigungsstrukturen[10]	▪ Berechtigungen werden i. d. R. nach dem sog. »Need-to-know«-Prinzip vergeben, d. h. jede Rolle bekommt nur die Rechte, die zur Ausführung der jeweiligen Aufgaben erforderlich sind. ▪ Hierbei sind insbesondere Funktionstrennungen und ggf. die Abbildung von internen Kontrollen zu beachten (z. B.: 4-Augen-Prinzip).
(64)	Zugriffsrechte im DMS[10]	▪ Berechtigungen können auf verschiedenen Ebenen vergeben werden, von ganzen Dokumentbereichen (»Rechnungsarchiv«) bis hin zu einzelnen Indexfeldern eines einzelnen Datensatzes bzw. Dokuments mit jeweils individuellen Rechten für Lesen, Ändern und/oder Löschen. ▪ Berechtigungen können ggf. auch von Feldinhalten abhängen (»darf nur auf Akte zugreifen, wenn Feld Gehalt < 5000 €«).
(65)	Rechte auf Dokumenten vs. Rechte auf Indexdaten	▪ Wenn ein Benutzer für bestimmte Objekte keine Rechte besitzt, sollte das System so reagieren, als wären diese Objekte nicht existent. ▪ Gegenbeispiel: Eine Suche ergibt 10 Treffer, von denen aber 3 Dokumente nicht eingesehen werden dürfen. Durch geschickte Suchabfragen kann ein Unberechtigter dann in bestimmten Fällen dennoch unberechtigt Informationen erhalten, auch ohne die Dokumente einzusehen (»suche alle Personalakten von Mitarbeitern, deren Feld Gehalt > 5000 € ist« etc.). Im obigen Beispiel muss die Trefferliste insoweit nur 7 statt 10 Treffer anzeigen.
(66)	Protokollierung von Berechtigungsänderungen	▪ Zur Einrichtung und Änderung von Berechtigungen sind wiederum besondere (administrative) Rechte erforderlich. Solche Änderungen sollten protokolliert werden.
(67)	Mandantentrennung über Berechtigungen	▪ Berücksichtigung von Mandanten (z. B.: SAP-Buchungskreise) im Berechtigungssystem. ▪ Bei entsprechender Anforderung muss eine Trennung der Dokumentbestände nach Mandanten bei der Recherche möglich sein. ▪ Bei entsprechender Anforderung muss eine Trennung der Dokumentbestände jedes rechtlich selbstständigen Partners bei der Archivierung möglich sein.

3.6 Mitarbeiter

a) Grundsatz

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.

b) Kontrollziel

Mitarbeiterqualifikation gemäß dem entsprechenden Anforderungsprofil.

c) Auswirkungen auf ein DMS

Der Grundsatz gilt für alle IT-Systeme gleichermaßen, sodass sich für ein DMS keine speziellen Aspekte ergeben.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(68)	Rollen beim DMS-Betrieb	▪ Rollen für die DMS-Benutzung sind z. B. Sachbearbeiter, Erfassungskräfte, Scan-Operatoren, Indizierer, Lesezugriff etc. ▪ Rollen für die technische DMS-Administration sind z. B. DMS-Systemadministratoren, Hardware-Wartungstechniker etc. ▪ Rollen für die Planung und Gestaltung des DMS sind z. B. IT-Leiter, Leiter von Fachabteilungen oder der Personalabteilung.
(69)	Definierte Aufgaben und Zuständigkeiten	▪ Die Definition der jeweiligen Rollen umfasst die Beschreibung der jeweiligen Aufgaben. Für die Aufgaben können bei Bedarf Arbeitsanweisungen formuliert werden; dies empfiehlt sich vor allem für komplexe und/oder sicherheitsrelevante Aufgaben. Die notwendigen Qualifikationen der Mitarbeiter ergeben sich aus ihren Aufgaben. ▪ Definierte Verantwortung für die Auswahl und Qualifikation der Mitarbeiter.
(70)	Eignung der Mitarbeiter	▪ Bei der Besetzung der Rollen wird auf die Verlässlichkeit und fachliche Eignung der Mitarbeiter geachtet, insbesondere bei administrativen Rollen.
(71)	Qualifizierung der Anwender	▪ Einweisungs- und Schulungsmaßnahmen für Anwender, z. B. als ▪ Inhouse-Kurse. Dies umfasst die technische Systembenutzung wie auch fachliche Regeln, bspw. zur Indexierung.
(72)	Qualifizierung der Administratoren	▪ Einweisungs- und Schulungsmaßnahmen für Administratoren (z. B.: Einweisung durch den Systemintegrator oder durch Kurse beim Hersteller der DMS-Software).
(73)	Nachvollziehbarkeit	▪ Dokumentation der vorhandenen Qualifikationen (z. B. Berufsausbildung) und der zusätzlichen Qualifikationsmaßnahmen. ▪ Anmerkung: Auch hier gibt es in manchen Fällen kurze Einweisungen in triviale Aufgaben, die nicht eigens zu dokumentieren sind (z. B.: Aufruf des Bildes eines gescannten Belegs aus dem ERP heraus)
(74)	Problembewusstsein	▪ Zur Gewährleistung der Sicherheit und Ordnungsmäßigkeit ist ein angemessenes Problembewusstsein für mögliche Risiken beim Einsatz eines DMS sicherzustellen. ▪ Hierfür sind insbesondere ausreichende Schulungen der Mitarbeiter sowie aussagekräftige Dokumentationen hinsichtlich der Risiken von Bedeutung.
(75)	Funktionstrennung	▪ Bezüglich einer Funktionstrennung ist darauf zu achten, dass Prozesse bezüglich eines DMS grundsätzlich eine starke Einbindung von IT-Mitarbeitern mit sich bringt. ▪ Die Funktionstrennung ist insbesondere im kaufmännischen Umfeld, im technischen Umfeld (Administration) sowie bei kritischen Überschneidungen zwischen beiden strikt zu beachten. Vor allem im Hinblick auf die Vertraulichkeit geraten IT-Projektmitarbeiter gerne in Vergessenheit.

4 Erfassungs- und Verarbeitungsprozesse im DMS

4 Erfassungs- und Verarbeitungsprozesse 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 E-Mails
- Archivierung von Rechnungen.

Das Themengebiet der Aufbewahrung von steuerrelevanten Daten wird in einem separaten Kapitel behandelt (vgl. Kapitel 5 Besondere Anforderung aus steuerlicher Sicht).

4.1 Scannen von Papierdokumenten

a) Grundsatz GoBD

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 (GoBD-Kapitel 9.3; Rz. 136–141). Darüber hinaus müssen prozessspezifische Besonderheiten (Farberfassung, OCR-Lesung, Rückseiten, Vernichtung) beachtet werden.

b) Kontrollziel

Die Vollständigkeit, Nachvollziehbarkeit, Nachprüfbarkeit, bildliche Übereinstimmung und Lesbarkeit bei der Umwandlung von Papierdokumenten in elektronische Dokumente ist sichergestellt.

c) Auswirkungen auf ein DMS

Die Anforderungen beziehen sich in erster Linie auf eigenständige Erfassungssoftware oder Scan-Module der DMS-Hersteller. Diese sind auch sinngemäß auf den Einsatz von Multifunktionsgeräten anwendbar, wenn bspw. das Scannen von Papierdokumenten innerhalb einer Fachabteilung erfolgt.

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. 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.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(76)	Ordnungsmäßigkeitsgrundsätze im Allgemeinen	▪ Die in Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze gelten auch für gescannte Papierdokumente. ▪ Im Folgenden wird auf Besonderheiten eingegangen.
(77)	Vollständig gescannte Dokumente	▪ Ggf. Rückseitenerfassung beim Scannen. ▪ Doppeleinzugs-Kontrolle. ▪ Zählen von Seiten zur Vollständigkeitsprüfung. ▪ Kennzeichnung bereits gescannter Dokumente durch den Scanner (Indossierung/ Imprinter).
(78)	Scannen der Papierdokumente	▪ Nutzung von ausreichenden Scan-Einstellungen (Farbe, DPI, Kontrast etc.). ▪ Einsatz von Bildverbesserungssoftware zur Verbesserung der Lesbarkeit. ▪ Sicherstellung der korrekten Dokumententrennung bei Stapelerfassung. ▪ Vermeidung von Doppelerfassungen (Scanner, organisatorisch). ▪ Qualitätssicherung (Software, organisatorisch).
(79)	Farberfassung	▪ Soweit der Farbe in einem Dokument eine Beweisfunktion zukommt, müssen diese Dokumente in Farbe gescannt werden.
(80)	OCR-Verarbeitung	▪ Werden gescannte Dokumente über das OCR-Verfahren mit Volltextinformationen angereichert (z. B. volltext-recherchierbare PDFs), so sind diese Dateien ebenfalls aufzubewahren.
(81)	Arbeitsanweisungen – 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-it's 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.
(82)	Arbeitsanweisungen – 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. ▪ Die Arbeitsnachbereitung beinhaltet die Kontrolle, ob die temporären Verarbeitungsdateien ordnungsgemäß verarbeitet und anschließend gelöscht worden sind.
(83)	Arbeitsanweisungen – 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. ▪ Festlegung, wann welche Scanprofile/Scannereinstellungen genutzt werden sollen. ▪ Umgang mit Sonderformaten oder geösten/gebundenen Dokumenten. ▪ In jedem Fall sind die Bildqualität sowie die korrekte und vollständige Erfassung der Dokumente regelmäßig zu prüfen.
(84)	Arbeitsanweisungen – 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.
(85)	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.
(86)	Vernichtung von Papierdokumenten	▪ Definition von Regelungen, wann und wie welche Papierdokumente nach dem Scannen vernichtet werden. ▪ Definition von Regelungen für Papierdokumente, die weiterhin im Papieroriginal aufzubewahren sind.
(87)	Authentizität (bei Aufbewahrung des Originals)	▪ Die eindeutige Verbindung zwischen dem Original und dem digitalisierten Abbild ist sicherzustellen, z. B. über Barcodes, Archivindex oder ggf. organisatorisch.

4.2 Archivierung von Ausgangsdokumenten

a) Grundsatz GoBD

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.

b) Kontrollziel

Die Verfügbarmachung aufbewahrungspflichtiger Ausgangsdokumente ist sichergestellt.

c) Auswirkungen auf ein DMS

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, bspw. 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- oder TIFF-Datei) der Aufbewahrung zuzuführen. Dieses so vorhandene Dokument besitzt dann keine Abhängigkeiten zu anderen Datenbeständen oder Ressourcen-Dateien.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(88)	Ordnungsmäßigkeitsgrundsätze im Allgemeinen	▪ Die in Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze gelten auch für Ausgangsdokumente. ▪ Im Folgenden wird auf Besonderheiten eingegangen.
(89)	Inhaltliche Gleichheit bei Ausgangsdokumenten	▪ Die aufbewahrungspflichtigen Inhalte, nicht ihre visuelle Gestaltung müssen reproduzierbar sein. ▪ 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 grafische 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 relevante Texte (es geht nicht um Werbung) mitgeliefert werden, sind diese ebenfalls zu dokumentieren. Gegebenenfalls genügt ein Verweis und sie müssen jederzeit verfügbar sein. ▪ Wenn keine Ablage im DMS als eigenes Dokument erfolgt, sondern die Daten in einer anderen Anwendung (z. B.: Fakturierungssystem) bleiben, müssen dort die Anforderungen an die Ordnungsmäßigkeit erfüllt werden. Ist die Anwendung hierzu nicht in der Lage, sollten die erzeugten Dokumente sicherheitshalber im DMS aufbewahrt werden.
(90)	Steuerrelevante Daten im Ausgangsprozess	▪ Entstehen im Rahmen des Ausgangsprozesses zusätzliche steuerrelevante Daten (z. B.: ZUGFeRD- oder EDI-Dateien), fallen diese nicht unter die Festlegungen für Ausgangsdokumente. Hierbei handelt es sich um steuerrelevante Daten, die ebenfalls aufbewahrt werden müssen.

4.3 Archivierung von E-Mails

a) Grundsatz GoBD

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.

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.

b) Kontrollziel

Steuerlich aufbewahrungspflichtige E-Mails werden originär elektronisch aufbewahrt und mit einem eindeutigen Index versehen.

c) Auswirkungen auf ein DMS

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).

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(91)	Ordnungsmäßigkeitsgrundsätze im Allgemeinen	▪ Die in Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze gelten auch für steuerrelevante E-Mails. ▪ Im Folgenden wird auf Besonderheiten eingegangen.
(92)	Nachvollziehbarkeit und Nachprüfbarkeit	▪ Ändernde Aktionen an steuerrelevanten E-Mails müssen nachvollziehbar sein. Dies kann bei der Speicherung von E-Mails in der E-Mail-Umgebung oder im Dateisystem in der Regel nicht sichergestellt werden. ▪ Ändernde Aktionen an Systemen für die Aufbewahrung von steuerrelevanten E-Mails müssen nachvollziehbar sein (z. B.: Systemeinstellungen oder Stammdaten). ▪ Verfahrensdokumentation für den Umgang und die Aufbewahrung von steuerrelevanten E-Mails muss vorliegen.
(93)	Vollständigkeit	▪ Festlegung, in welchen Fällen E-Mails als E-Mail-Objekte (inkl. Attachments) abgelegt werden und wann und wie E-Mails oder Attachments anderen fachlichen Kategorisierungen zugeordnet werden (z. B.: Bsp. E-Mail mit Antrag von Kunde XY. Die E-Mail insgesamt wird bei XY der Kategorie Korrespondenz zugeordnet. Der Antrag (Attachement) wird zusätzlich als eigenes Objekt der Kategorie Anträge zugeordnet). ▪ Sowohl E-Mail-Bodies als auch E-Mail-Anhänge können steuerliche Relevanz besitzen. ▪ 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 bisherige Papierbriefumschlag). ▪ Reine SPAM-Mails/Werbe-Mails sind nicht steuerrelevant und unterliegen nicht der Anforderung an Vollständigkeit.
(94)	Richtigkeit	▪ E-Mails müssen inhaltlich gleich aufbewahrt werden, da sich das technische »Originalformat« nach der Anwendung richtet, in der die E-Mail angezeigt wird. ▪ Das Ausdrucken oder die PDF-Konvertierung von E-Mails erfüllt nicht die Anforderungen an die inhaltlich gleiche Aufbewahrung (originär elektronisch). ▪ Verschlüsselte E-Mails müssen auch entschlüsselt aufbewahrt werden.
(95)	Zeitgerechte Buchungen und Aufzeichnungen	▪ Wenn eine vom E-Mail-System separate Aufbewahrungsumgebung eingesetzt wird, soll eine zeitnahe Überführung der steuerrelevanten E-Mails sichergestellt werden.
(96)	Ordnung	▪ Sind E-Mails eine Buchungsgrundlage/ein Buchungsbeleg, muss eine eindeutige Verknüpfung zwischen Buchung und E-Mail vorhanden sein. ▪ Ohne zusätzliche manuelle oder automatische Maßnahmen stellen die Ordnungsstrukturen einer E-Mail-Umgebung (ein großer Posteingangs-Ordner, E-Mail-Eigenschaften (z. B.: Felder wie VON, AN, CC, BCC, Betreff und technische Felder) nur eine begrenzte Ordnung dar. ▪ In DMS-Umgebungen werden steuerrelevante E-Mails neben einer Buchung oft auch einem fachlichen Vorgang oder ein Kreditor- oder Debitorenakte zugeordnet.

4.4 Archivierung von Rechnungen

a) Grundsatz GoBD

Elektronische bzw. digitalisierte (gescannte) Rechnungen unterliegen insbesondere den Anforderungen des Umsatzsteuergesetzes sowie der GoBD. Sie sind nach

§ 14b UStG grundsätzlich zehn Jahre aufzubewahren.

Hinweis

Bezüglich der umsatzsteuerlichen Anforderungen ist ergänzend 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.

b) Kontrollziel

Rechnungen werden ordnungsgemäß über die Dauer der Aufbewahrungsfrist aufbewahrt.

c) Auswirkungen auf ein DMS

Betreffend der Auswirkungen auf ein DMS wird wie folgt verwiesen:

- Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen für die grundsätzlichen Anforderungen an die Aufbewahrung von Rechnungen
- Kapitel 4.1 Scannen von Papierdokumenten für das Scannen von Eingangsrechnungen
- Kapitel 4.2 Archivierung von Ausgangsdokumenten für die Aufbewahrung von Ausgangsrechnungen
- Kapitel 4.3 Archivierung von E-Mails für Rechnungen, die per E-Mail empfangen oder versendet wurden
- Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff für die Sicherstellung des Datenzugriffs auf Rechnungen und Rechnungsdaten

In der folgenden Tabelle werden ausgewählte Anforderungen und Lösungsansätze mit Fokus auf Rechnungen dargestellt bzw. wiederholt.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(97)	Elektronische Rechnungen per E-Mail	▪ Es besteht keine Aufbewahrungspflicht soweit die E-Mail nur als »Transportmittel«, z. B. für eine angehängte elektronische Rechnung dient und darüber hinaus keine weitergehenden aufbewahrungspflichtigen Informationen enthält.
(98)	Aufbewahrung Verarbeitungsdaten	▪ Sicherstellung der Reproduzierbarkeit von Ausgangsrechnungen erfordert die Historisierung von Stammdaten oder die Speicherung im Dokument. ▪ Bei der frühen Rechnungserfassung müssen bereits bei Prozessbeginn (z. B.: nach der OCR-Lesung) Änderungen und Löschungen protokolliert werden. ▪ Soweit OCR-Daten erzeugt werden, sind diese ebenfalls aufzubewahren. ▪ Vgl. auch Kapitel 4.1 Scannen von Papierdokumenten.
(99)	Rechnungsprüfung	▪ Einrichtung und Dokumentation einer Rechnungseingangsprüfung (Innerbetriebliches Kontrollverfahren mit Prüfpfad). Dies betrifft insbesondere die Prüfung der Pflichtangaben nach § 14 Abs. 4 UStG.
(100)	Konvertierung von elektronischen Rechnungen	▪ Soweit generell eine Umwandlung (Konvertierung) aufbewahrungspflichtiger Unterlagen in ein unternehmenseigenes Format (sog. Inhouse-Format) erfolgt, sind stets beide Versionen aufzubewahren, derselben Aufzeichnung zuzuordnen und mit demselben Index zu verwalten.
(101)	Scannen von Allgemeinen Geschäftsbedingungen	▪ Scannen von AGBs ist erforderlich, sofern nicht durch organisatorische Maßnahmen sichergestellt wird, dass die jeweils gültigen AGBs den einzelnen Dokumenten zugeordnet werden können.

5 Besondere Anforderung aus steuerlicher Sicht

5 Besondere Anforderung aus steuerlicher Sicht

5.1 Maschinelle Auswertbarkeit und Datenzugriff

a) 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.

b) Kontrollziel

Alle steuerrelevanten Daten und Dokumente sind in maschinell auswertbarer Form über die Dauer der Aufbewahrungsfrist verfügbar.

c) Auswirkungen auf ein DMS

Für DMS-Umgebungen sind die Themen maschinelle 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.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(102)	Formatkonvertierung allgemein	▪ Es ist sicherzustellen, dass durch Formatkonvertierungen die maschinellen Auswertungsmöglichkeiten (Sortier-, Summier-, Filterungsmöglichkeiten, Volltextsuche, Nachverfolgung von Verknüpfungen und Verlinkungen) nicht beeinträchtigt werden. ▪ Z. B.: Maschinell auswertbare Buchhaltungsdaten werden in eine nur volltextauswertbare PDF-Textdatei umgewandelt.
(103)	Konvertierung von E-Mails	▪ E-Mail-Attribute müssen erhalten bleiben. ▪ Attachments dürfen nicht so konvertiert werden, dass es zu einer Einschränkung der maschinellen Auswertungsmöglichkeiten, insbesondere der Recherchierbarkeit, kommt.
(104)	Konvertierung von ZUGFeRD-Rechnungen	▪ XML-Attachment muss analog dem PDF/A-3 Container erhalten bleiben.
(105)	Ergänzung von OCR-Layern bei PDF-Dokumenten	▪ Werden Dokumente um einen OCR-Layer ergänzt (z. B.: Gescannte Dokumente), müssen diese durchsuchbaren Dokumente erhalten bleiben und dem Prüfer zur Verfügung gestellt werden.
(106)	Volltext-Indizierung	▪ Ist eine Volltext-Indizierung für Dokumente vorhanden, muss diese erhalten bleiben und dem Prüfer zur Verfügung gestellt werden.
(107)	Verschlüsselung	▪ Beim Einsatz von Verschlüsselungstechniken (Kryptographietechniken) muss sowohl die verschlüsselte als auch die unverschlüsselte Version des Dokumentes inkl. der Schlüssel aufbewahrt werden.
(108)	Historisierung der Systemeinstellung	▪ Die zum Zeitpunkt der Archivierung geltenden Systemeinstellungen müssen transparent gemacht werden können (z. B.: Über entsprechende Protokollierung). ▪ Unternehmensspezifische Einstellungen, Anpassungen, Parametrisierungen und Änderungen in Tabellen müssen vorgehalten werden. ▪ Die zum Zeitpunkt der Archivierung geltenden Stammdaten müssen transparent gemacht werden können (z. B.: Über entsprechende Protokollierung).
(109)	Unmittelbarer Datenzugriff/Z1-Zugriff	▪ Die Index- und Volltextsuche sowie die Dokumentenanzeige eines DMS müssen dem Prüfer zugänglich gemacht werden. Daher sollten Prüfer-Berechtigungsprofile mit den entsprechenden Einschränkungen (Mandant, Prüfungszeitraum, »Nur-Lese-Zugriff« ohne Export-Möglichkeit, ggf. mit Protokollierung) eingerichtet werden können. ▪ Sicherstellung (ggf. organisatorisch), dass durch den Prüferzugriff keine Systeminstabilitäten auftreten (z. B.: Performanceintensive Suchabfragen).
(110)	Datenträgerüberlassung/Z3-Zugriff	▪ Der Export von Trefferlisten und Dokumenten muss gemäß den Vorgaben des Prüfers möglich sein. ▪ Alle zur Auswertung der Daten notwendigen Strukturinformationen müssen in maschinell auswertbarer Form zur Verfügung stehen. ▪ Beschreibung des Export-Formates und der Feldtypen für die exportierten Dokumente.

5.2 Auslagerung und Migration

a) Grundsatz GoBD

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.

b) Kontrollziel

Beibehaltung der vorhandenen Auswertungsmöglichkeiten bei einer Auslagerung von Daten oder bei einem Systemwechsel bzw. einer Systemänderung.

c) Auswirkungen auf ein DMS

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.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(111)	Konzept/Dokumentation für eine Migration	▪ Für die Durchführung der Migration sollte eine entsprechende Dokumentation vorhanden sein, aus der erkennbar ist, welche Regeln, Rahmenbedingungen und Zeiten für die Migration gelten.
(112)	Umfang der Migration	▪ Definition, in welchem Umfang Dokumente migriert wurden. ▪ Dies ist typischerweise zeitraum- oder archivbereich-, stammdaten- ▪ oder dokumentartbezogen. Steuerliche Aufbewahrungsfristen sind zu beachten.
(113)	Protokollierung der Dokumentenmigration	▪ Über die Dokumentenmigration sollten Protokolle vorhanden sein, aus denen hervorgeht, dass diese Dokumente (inkl. der erforderlichen Änderungen, bspw. Formatkonvertierungen) vollständig und unverändert übernommen wurden. ▪ Alle Änderungen an Indexwerten müssen mit altem und neuem Wert protokolliert werden.
(114)	Nachweis der nicht übernommenen Dokumente	▪ Werden Dokumente aus unterschiedlichen Gründen nicht übernommen (z. B.: Abgelaufene Aufbewahrungsfristen, nicht mehr relevante Dokumente), sollte ein entsprechender Nachweis über diese Dokumente vorhanden sein. Dieser sollte zumindest die Identifikation im Quellsystem und eine fachliche Identifikation enthalten (z. B.: Dokumentenart und Kundennummer).
(115)	Formate der Dokumente	▪ Bei Formatkonvertierungen im Rahmen der Migration sind die Anforderungen an die maschinelle Auswertbarkeit zu beachten (siehe Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff).
(116)	Verlinkungen	▪ Verlinkungen müssen im Rahmen der Migration erhalten bleiben (siehe Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff). ▪ Sind in anderen Systemen Indexstrukturen vorhanden (ggf. auch nicht nur die Doc-ID), müssen diese Werte im Rahmen der Migration ebenfalls geändert werden. ▪ Z. B.: Wenn ein externes ERP Referenzen auf die Doc-IDs enthält, so sind diese Doc-IDs im Neusystem als suchbare Indexfelder anzulegen, damit das ERP die Dokumente finden kann.
(117)	Vorgehen bei mehreren Dokumentversionen	▪ Sind im Quellsystem mehrere Dokumentversionen enthalten, muss festgelegt werden, ob alle Dokumentenversionen übernommen werden sollen oder ob nach definierten Regeln nur eine teilweise Übernahme erfolgt. Auch sollte beschrieben sein, wie sich die versionierten Dokumente im Zielsystem darstellen (bspw. entweder als versioniertes Dokument oder als mehrere Einzeldokumente).
(118)	Abbildung von Notizen und grafischen Annotationen	▪ Da Notizen und grafischen Annotationen oft herstellerspezifisch umgesetzt sind, sollte festgelegt werden, wie hiermit im Rahmen der Migration umgangen werden soll. ▪ Es darf zu keinen Auswirkungen auf die maschinelle Auswertbarkeit kommen (z. B.: Annotationstexte sind zwar im Quellsystem, jedoch nicht mehr im Zielsystem recherchierbar).
(119)	Mapping-Regeln (bei Datenbeständen)	▪ Für die Migration der Datenbestände muss das Mapping vom Quelldatenbanksystem zum Zielsystem dokumentiert sein. Gegebenenfalls erforderliche Änderungen, Aufteilungen oder Zusammenfassungen von Indexstrukturen sollten nachvollzogen werden können. ▪ Es darf zu keinen Einschränkungen von vorhandenen Suchmöglichkeiten kommen.
(120)	Volltext-Index	▪ Ist ein Volltext-Index vorhanden, sollte ein Nachweis über die Übernahme oder ggf. den Neuaufbau der Indexstrukturen erfolgen.
(121)	Reports und sonstige Auswertungsmöglichkeiten	▪ Vorhandene Systemreports mit steuerlichem Bezug (z. B.: Übersicht Rechnungen sortiert nach Zahlungsziel) müssen auch im Zielsystem vorhanden sein.

5.3 Outsourcing/Auslagerung von DMS-Funktionen

a) Grundsatz GoBD

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).

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.

b) Kontrollziel

Zugriffsmöglichkeiten im Rahmen einer steuerlichen Außenprüfung sind auch im Rahmen von Outsourcing/einer Verlagerung des IT-Betriebes gewährleistet.

c) Auswirkungen auf ein DMS

Soweit das DMS im Ausland betrieben wird, müssen die angeforderten Unterlagen unverzüglich zur Verfügung gestellt, die angeforderten Auskünfte zeitnah erteilt und Datenzugriffsmöglichkeiten in vollem Umfang gewährleistet werden können. Eine elektronische Aufbewahrung von Rechnungen 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.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(122)	Maschinelle Auswertbarkeit/Datenzugriff	▪ Die in Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff definierten Anforderungen müssen auch bei der Auslagerung von Funktionen erhalten bleiben.
(123)	Kontrollrechte	▪ Grundsätzlich sollte sich der Outsourcing-Geber vertragliche Kontrollrechte bzgl. der Ordnungsmäßigkeit seiner Buchführung vom Dienstleistungsunternehmen zusichern lassen (z. B.: Zusicherung der GoBD-Konformität; Haftung und Schadensersatz). ▪ Ebenso sollten Prüfungs- und Auskunftsrechte (durch den Buchführungs- und Aufzeichnungspflichtigen oder durch Dritte nach Auftrag des Buchführungs- und Aufzeichnungspflichtigen) vereinbart werden. ▪ Regelungen über eine zeitnahe Verfügbarkeit von Daten und Verfahrensdokumentation beim Outsourcing-Geber sollten schriftlich fixiert werden.
(124)	Änderung von Rahmenbedingungen	▪ Das Dienstleistungsunternehmen hat den Buchführungs- und Aufzeichnungspflichtigen über organisatorische oder IT-technische Änderungen einschließlich des dienstleistungsbezogenen IKS im Vorfeld proaktiv und frühzeitig in Kenntnis zu setzen, um rechtzeitig die ggf. davon betroffenen Kontrollen des IKS an die neue Situation anzupassen.
(125)	Verfahrensdokumentation	▪ Die Dokumentation der Verfahren und die des IKS seitens des Dienstleistungsunternehmens sowie des Outsourcing-Gebers sind sicherzustellen. Dabei sollte sich der Outsourcing-Geber einen Einblick bzw. Zugriff auf die gesamte Programmdokumentation und die Verfahrensdokumentation einschließlich der Änderungshistorie zusichern lassen, auch wenn diese originär beim Dienstleistungsunternehmen erstellt und aufbewahrt wird. ▪ Der aktuelle Stand der Verfahrensdokumentation ist vom Dienstleister auf Anforderung zur Verfügung zu stellen.
(126)	Weiterverlagerung	▪ Eine Weiterverlagerung an Subunternehmer durch das Dienstleistungsunternehmen ist durch den Outsourcing-Geber vertraglich zu untersagen bzw. dezidiert zu regeln. Unabhängig von der vertraglichen Regelung ist der Buchführungs- und Aufzeichnungspflichtige auch für die Einhaltung der Ordnungsmäßigkeit beim Subunternehmer verantwortlich.
(127)	Auslagerung ins Ausland	▪ Es ist ein Antrag beim zuständigen Finanzamt zu stellen. ▪ Die Bereitstellung der Möglichkeit des Datenzugriffs im Rahmen der Betriebsprüfung muss sichergestellt werden. Aufgrund der Auslagerung darf es hier nicht zu Einschränkungen kommen. ▪ Der Online-Zugriff für Rechnungen muss gewährleistet sein.

6 Verfahrensdokumentation

6 Verfahrensdokumentation

6.1 Erstellung und Umgang mit der Verfahrensdokumentation

a) Grundsatz GoBD

Die IT-gestützte Buchführung muss von einem sachverständigen Dritten hinsichtlich ihrer formellen und sachlichen Richtigkeit in angemessener Zeit prüfbar sein. Voraussetzung für die Nachvollziehbarkeit des Soll-Verfahrens ist dabei stets eine ordnungsgemäße Verfahrensdokumentation, welche die Beschreibung aller zum Verständnis der Buchführung erforderlichen Verfahrensbestandteile, Daten und Dokumentbestände enthalten muss. Nach den GoBD muss für jedes IT-System eine übersichtlich gegliederte Verfahrensdokumentation vorhanden sein, aus der Inhalt, Aufbau, Ablauf und Ergebnisse des IT-Verfahrens vollständig und schlüssig ersichtlich sind (siehe GoBD-Kapitel 10, Rz. 151ff.).

Unter einer Verfahrensdokumentation versteht die Finanzverwaltung die Beschreibung des organisatorisch und technisch gewollten Verfahrens bei der Verarbeitung steuerlich relevanter Informationen. Dabei hat die Dokumentation stets den in der Praxis eingesetzten Komponenten und Prozessen des IT-Systems zu entsprechen, umgekehrt müssen die Inhalte einer Verfahrensdokumentation auch so »gelebt werden«. Die Zielsetzung einer Verfahrensdokumentation besteht letztlich im Nachweis der Erfüllung der in den GoBD definierten Ordnungsmäßigkeitsgrundsätze.

b) Kontrollziel

Die Verfahrensdokumentation gibt versionsbezogen die organisatorischen und technischen Verfahren des DV-Systems wieder. Die Dokumente entsprechen den jeweilig aktuellen bzw. historischen Versionen des DV-Systems. Umgekehrt sind die Inhalte der aktuell gültigen Verfahrensdokumentation auch aktuell implementiert.

c) Auswirkungen auf ein DMS

Ebenso wie für andere steuerrelevante Systeme muss auch für das DMS eine Verfahrensdokumentation erstellt und vorgehalten werden. Im Gegensatz zu Buchhaltungs- oder ERP-Systemen stellen die Inhalte weniger auf buchhaltungstypische Funktionen, wie etwa die Konten- oder Journalfunktionen ab, als vielmehr auf die Prozesse rund um die Aufbewahrung von steuerrelevanten Daten und Dokumenten. Weitere Details zu den Inhalten siehe Kapitel 6.2 Inhalte einer Verfahrensdokumentation.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(128)	Erstellen der Verfahrensdokumentation	▪ Häufig erfolgt die Erstellung mit den bereits im Unternehmen im Einsatz-befindlichen Büroanwendungen (z. B.: Textverarbeitungs- und Tabellenkalkulationsprogramm) nebst Ablage im Dateisystem oder in der eigenen DMS-Umgebung. ▪ Ist eine »Wiki-Umgebung« im Einsatz, entscheiden sich Kunden häufig für die Pflege der Dokumentation in dieser Umgebung. ▪ Spezielle Tools für die Erstellung und Pflege einer Verfahrensdokumentation gibt es am Markt. ▪ Die Tool-Auswahl wird häufig auch davon beeinflusst, wie erforderliche bzw. bereits vorhandene Dokumentationen erstellt und gepflegt werden (z. B.: IT-Betriebskonzept, Arbeitsanweisungen).
(129)	Aufbewahrung der Verfahrensdokumentation	▪ 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.
(130)	Vorhandene Dokumentationen	▪ Vorhandene Dokumentationen, auf die verwiesen werden könnte, sind typischerweise: Fachkonzepte, IT-Konzepte, Arbeitsanweisungen, Organisationshandbücher etc. ▪ Einfache Verlinkungsmöglichkeiten zum Verweis auf vorhandene Beschreibungen sind einzurichten. ▪ Es ist sicherzustellen, dass bei einem Verweis die Anforderungen an Versionierung mit Änderungsprotokoll erfüllt werden.

(131)	Zuständigkeiten für Erstellung und Pflege regeln	▪ Beispiele für Hersteller-Themen:
		  ▪ Beschreibung der Standardfunktionalitäten.
		  ▪ Beschreibung der internen technischen Prozesse etc.
		  ▪ Möglichkeit der Systemmigration.
		  ▪ Hersteller können eine Mustervorlage zur Verfügung stellen.
		▪ Beispiele für Themen eines Integrators/Systemhauses:
		  ▪ Beschreibung der Einrichtung des Systems (z. B.: Dokumentarten, Indexfelder, Gruppen und Rechte, technische Einstellungen etc.).
		▪ Beispiele für Betreiber-Themen:
		  ▪ Allgemeine Beschreibung des Unternehmens und des Einsatzzweckes.
		  ▪ Arbeitsanweisungen.
		  ▪ Vorgehen bei Test und Abnahme.
		  ▪ Sicherstellung der Betriebssicherheit.
		  ▪ Umfang und Vorgehensweise bei Schulungen.

(132)	Unveränderbarkeit und Pflege der Verfahrens-dokumentation	▪ Es ist auf eine korrekte Versionierung/Historisierung der Dokumentation zu achten. Dazu sollte es Regeln geben, bei welchen Änderungen eine Anpassung der Verfahrens-dokumentation erforderlich ist und wann nur referenzierte Dokumente fortgeschrieben werden. ▪ Eine 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 Geschäftsjahres-ende) 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.
(133)	Übereinstimmung von Verfahrensdokumenta-tion und realem Systembetrieb	▪ Bei relevanten Änderungen muss die Verfahrensdokumentation aktualisiert werden. Nicht jede triviale Änderung (wie z. B. der Austausch einer Tastatur an einem Sachbear-beitungsarbeitsplatz) muss dokumentiert werden. Es sollte aber klare Regeln dafür geben, welche Änderungen als »relevant« angesehen werden und von wem diese zu dokumentieren sind. ▪ Relevante Veränderungen am DMS werden nur nach einer expliziten Freigabe vorge-nommen. Die Zuständigkeiten für die Freigabe sind vom Unternehmen zu definieren.

6.2 Inhalte einer Verfahrensdokumentation

a) Grundsatz GoBD

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.

b) Kontrollziel

Die Inhalte einer Verfahrensdokumentation sind so zu wählen, dass ein sachverständiger Dritter schnell einen vollständigen Überblick über die Prozesse erhält.

c) Auswirkungen auf ein DMS

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.

d) Lösungen und Beispiele

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(134)	Beschreibung der steuerrelevanten Dokumente	▪ Zusammenstellung der Dokumentarten, die Steuerrelevanz besitzen.
(135)	Beschreibung der steuerrelevanten Daten	▪ Zusammenstellung der Datenbestände, die Steuerrelevanz besitzen.
(136)	Prüfung auf weitere Rechtsgrundlagen	▪ Prüfung, ob neben den steuerlichen Anforderungen an die Aufbewahrung weitere Rechtsgrundlagen relevant sind.
(137)	Kapitel: Aufbau- und Ablauforganisation	▪ 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.
(138)	Kapitel: Sachlogische Lösung	▪ 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.
(139)	Kapitel: IT-Infrastruktur	▪ 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).
(140)	Kapitel: Prozesse allgemein	▪ 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.

(141)	Kapitel: Erfassungsprozesse	▪ Beispielsweise:
		  ▪ Digitalisierung (Scannen).
		  ▪ Übernahme von originär digitalen Dokumenten (Dateien, E-Mails).
		  ▪ Automatisierte Übernahme von digitalen Massendaten (COLD, Import, EDI).
		  ▪ Indizierung.
		  ▪ Archivierung.

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(142)	Kapitel: Bearbeitungsprozesse	▪ Beispielsweise: ▪ Ändern von Objekten. ▪ Änderung der Indexstrukturen. ▪ Weiterleiten. ▪ Genehmigen. ▪ Speichern/Versionierung.
(143)	Kapitel: Recherche und Reproduktionsprozesse	▪ Zugriff über Client. ▪ Anwendungsintegration. ▪ Anzeige, Ausdruck, Export. ▪ Datenzugriff gemäß GoBD.
(144)	Kapitel: Internes Kontrollsystem	▪ Beschreibung des IKS. ▪ Zeitnahe Aktualisierung der Verfahrensdokumentation bei Systemänderungen. ▪ Auflistung der automatischen und manuellen Kontrollfunktionen in der Verfahrensdokumentation.
(145)	Sonstige relevante Dokumentationen und Inhalte	▪ 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).

7 Glossar

AO
Abgabenordnung. In der Regel ist die Abgabenordnung vom 16. März 1976 gemeint (AO 1977, BGBl. I S. 613, ber. 1977 I S. 269) mit den jüngsten Änderungen durch Gesetz vom 26. Juni 2001 (BGBl. I 2001 S. 1310). »Steuergrundgesetz«, das verschiedene materielle und verfahrensrechtliche Vorschriften der Steuergesetzgebung zusammenfasst. Die AO regelt im Wesentlichen die Erhebung von Steuern, Besteuerungsverfahren sowie Straf- und Bußgeldvorschriften.

DMS-relevant ist die AO, weil sie die Grundlagen der Sorgfaltspflichten bei der Aufbewahrung der steuerlich relevanten Unterlagen definiert. Konkret verlangt die AO in den §§ 146 und 147 AO die »ordnungsgemäße Aufbewahrung« der aufbewahrungspflichtigen Unterlagen, was in zahlreichen BMF-Schreiben und der GOBS von 1995 konkretisiert wurde. Die Abgabenordnung wurde mit Wirkung vom 1. Januar 2002 dahingehend geändert, dass solche Unterlagen, die in digitaler Form entstanden oder zugegangen sind für die Dauer der Aufbewahrungsfrist in maschinell auswertbarer Form zur Verfügung gestellt werden müssen. Dies bedeutet in der Regel ein Verbot des – früher erlaubten – Ausdruckens/Verfilmens und nachfolgender Vernichtung der elektronischen Informationen.

Barcode
Ein Barcode ist eine Aneinanderreihung von binären Informationen. Die vertikalen, dunklen Striche unterschiedlicher Breite eines Barcodes nennt man »Balken« und die hellen Zwischenräume »Lücken«. Balken und Lücken werden zusammen als »Elemente« bezeichnet. Es gibt verschiedene Barcodetypen, die unterschiedliche Zeichensätze unterstützen. Je nach Kombination von Balken und Lücken werden die verschiedenen Zeichen innerhalb eines Barcodes dargestellt.

Die Daten in einem Barcode sind lediglich Referenznummern, anhand derer der Computer einen entsprechenden Datensatz auf einem elektronischen Datenträger identifizieren kann. Im Normalfall enthält ein Barcode keine beschreibenden Daten, wie z. B. vollständige Texte.

Erst die mehrdimensionalen Barcodes (z. B. PDF417) können mehr als nur eine ID-Nummer enthalten. Mit ihnen lassen sich komplette Texte, Datenbank-Records und Indexstrukturen abbilden.

Beleg
Der Beleg dient dem Nachweis einer Buchung bzw. eines Geschäftsvorfalls (Belegfunktion). Jede Buchung muss vollständig belegmäßig nachgewiesen sein.

Buchführung
Die Buchführung muss alle Geschäftsvorfälle vollständig, richtig, zeitgerecht und geordnet aufzeichnen. Alle Veränderungen, die nach Handels- oder Steuerrecht die Vermögens-, Finanz- und Ertragslage des Buchführungs- und Aufzeichnungspflichtigen beeinflussen, sind abzubilden und zu dokumentieren.

Dabei muss die Buchführung so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über alle Geschäftsvorfälle und über die Lage des Unternehmens verschaffen kann.

COLD
Computer Output on Laser Disk. Der Begriff ist zwar veraltet (Laser Disk sind nicht mehr verfügbar), aber viele Anbieter verwenden die Bezeichnung immer noch zur Kennzeichnung von Systemen zur Verwaltung computergenerierter Daten wie Ausgangspost, Drucklisten, Reports, Journale etc. COLD-Daten wurden früher häufig auf optischen Platten (engl. Laser Disks) archiviert, daher der Name in Anlehnung an das COM-Verfahren (Computer Output on Microfilm), zu dessen Ablösung COLD-Systeme angetreten sind. Begriff wird von manchen Anbietern auch nur für Stapelimport- und Parserfunktionen verwendet.

Datenzugriff
Die Finanzbehörde hat das Recht, diejenigen Unterlagen, die mit Hilfe eines IT Systems erstellt wurden, und aufbewahrungspflichtig sind, im Rahmen einer steuerlichen Außenprüfung durch Datenzugriff zu prüfen. Es werden folgende Zugriffsarten unterschieden:

- Z1 (unmittelbarer Datenzugriff):
  Der Betriebsprüfer greift mit der Hard- und Software des Steuerpflichtigen selbst auf das IT System des Steuerpflichtigen zu und zwar nur lesend auf die steuerlich relevanten Daten.

- Z2 (mittelbarer Datenzugriff):
  Der Steuerpflichtige greift mit der eigenen Hard- und Software auf sein IT-System nach den Vorgaben des Betriebsprüfers zu.
- Z3 (Datenträgerüberlassung):
  Der Steuerpflichtige erstellt einen Datenträger mit den steuerlich relevanten Daten und Strukturinformationen und übergibt diesen an den Betriebsprüfer, der die Daten mit eigenen Mitteln (Prüfsoftware IDEA) auswertet.

DMS
Dokumentenmanagement-System

Häufig verwendeter Oberbegriff für informationstechnische Systeme zur Verwaltung elektronischer Dokumente und deren Prozesse. DMS-Komplettlösungen umfassen typischerweise:
- Unterstützung des kompletten Dokumentenlebenszyklus inkl. Erfassung/Erstellung.
- Versionierung inkl. der dazu notwendigen Check-Out/Check-In-Funktionen.
- Metadatenverwaltung, ggf. auch Organisation in Aktenstrukturen.
- Inhaltssuche (erfordert Volltext-DB).
- Genehmigungs-, Freizeichnungs-, Publishingprozesse.
- Postkorb/Workflow-Funktionen.
- Rendition/Formatkonvertierung.
- Unveränderbare (revisionssichere) Ablage und Archivierung.
- Integration in Fachsysteme für Output- und Retrievalintegration.

Doc-ID, Dok-ID
Dokumenten-ID. Eindeutige Dokumentennummer in einem DMS. Die Dok-ID kann von der eigentlichen Objekt-ID abweichen, weil sich ein Dokument aus mehreren zu speichernden physischen Objekten zusammensetzen kann. Das war früher bereits bei den Single-Page-TIFF-Dokumenten der Fall und gilt heute auch bei Webseiten und ggf. anderen Konstrukten.

DPI
Dots per Inch (Punkte pro Zoll), Maßeinheit zur Darstellung der Auflösung von Bildschirmen, Druckern, Scannern etc.

ECM
Enterprise Content Management. Über DMS hinausgehender Begriff, der alle relevanten Informationsobjekte eines Unternehmens umfasst und nicht nur diejenigen, die sich als Dokument definieren lassen. In ECM-Lösungen würden also auch Buchungsrecords in einer Kundenakte als Bestandteil der Lösung definiert werden, obwohl ein Datensatz von den meisten Fachleuten nicht als »Dokument« definiert werden würde. Der Begriff Enterprise steht weniger für »Großunternehmen«, sondern vielmehr für den abteilungsübergreifenden Ansatz in einem Unternehmen mit unterschiedlichen Bereichen und Prozessen. Es sollen daher ALLE in einer Unternehmung (oder einer Organisation, einer Behörde) relevanten Content-Objekte betrachtet werden und nicht nur Insellösungen. Auch Content-Funktionen wie Enterprise Search, Portale, Web Content Management, Blogs, Wikis, virtuelle Projekt- und Teamräume sind häufig dem Thema ECM zugeordnet.

EDI
Electronic Data Interchange

Als »elektronischer Datenaustausch« wird die Übertragung kommerzieller und administrativer Daten zwischen Computern nach einer vereinbarten Norm zur Strukturierung einer EDI-Nachricht bezeichnet.

Einnahmen-Überschuss-Rechner
Steuerpflichtige, die ihren Gewinn nach den Vorschriften des § 4 Abs. 3 EStG ermitteln.

E Mail
electronic mail (Deutsch: Elektronische Post)

Die E Mail ist eine briefähnliche Nachricht, die auf elektronischem Weg über Computernetzwerke an einen oder mehrere Empfänger geschickt werden kann.

Eine E Mail besteht i. d. R. aus:
- Header,
- Body,
- Signatur,
- Footer,
- Anhänge.

ERP-System

Ein ERP (Enterprise Resource Planning)-System ist eine betriebswirtschaftliche Anwendungssoftware zur umfassenden Integration, Steuerung und Optimierung der ressourcenbezogenen Unternehmensaktivitäten. Ein Schwerpunkt liegt dabei auf der Verknüpfung und Abbildung von rechnungslegungsbezogenen Abläufen mit Daten aus anderen Unternehmensbereichen (z. B. Produktion, Beschaffung, Lagerhaltung). ERP-Software besteht meist aus mehreren Modulen, die jeweils betriebliche Funktionen (Materialwirtschaft, Produktion, Finanzen, Personalwirtschaft etc.) abbilden.

GDPdU

»Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen« (GDPdU). Verwaltungsanweisung, die mit Schreiben des Bundesfinanzministeriums vom 17. Juli 2001 an die obersten Finanzbehörden der Länder verteilt wurden. Sie definieren die Regeln für steuerliche Außenprüfungen ab dem 1. Januar 2002. Im Herbst 2012 aktualisiert wegen des Wegfalls der Signaturpflicht bei vorsteuerabzugsfähigen, elektronischen Eingangsrechnungen.

Am 14. November 2014 wurden die GDPdU (und gleichzeitig die GoBS) ersetzt durch die GoBD.

GoBD

»Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff«. Veröffentlicht am 14. November 2014 und anwendbar für Veranlagungszeiträume, die nach dem 31. Dezember 2014 beginnen. Die GoBD ersetzt die bisher geltenden GoBS sowie die GDPdU.

GoBIT

Die »Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz« (GoBIT) waren ein Arbeitsvorhaben der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV). Nach Erscheinen der GoBD wurde die Arbeit an den GoBIT nicht weitergeführt. Der letzte veröffentlichte Entwurf enthält allerdings etliche wertvolle Aussagen, die zur Umsetzung der GoBD hilfreich sein können. GoBIT (Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz) mit Stand: 13. Oktober 2012, unter: http://www.awv-net.de/cms/Fachinformationen/GoBIT/_AktuellerEntwurfderGoBIT,cat267.html

GoBS

»Grundsätze ordnungsmäßiger IT-gestützter Buchführungssysteme« (GoBS). Die GoBS wurden von der AWV Arbeitsgemeinschaft für wirtschaftliche Verwaltung erarbeitet und mit einem BMF-Begleitschreiben am 7. November 1995 veröffentlicht. Die Referenzierung GoBS bezieht sich in der Regel auf beide Dokumente, die eigentlichen GoBS und das BMF-Begleitschreiben.

Am 14. November 2014 wurden die GoBS (und gleichzeitig die GDPdU) durch die GoBD ersetzt.

Handelsbrief

Handelsbriefe sind alle Dokumente, die ein Handelsgeschäft betreffen (§ 257, Abs. 2 HGB), also Geschäfte eines Kaufmanns, die zum Betrieb eines Handelsgewerbes gehören (§ 343 HGB), wie z. B. Mängelrügen, Angebote zum Abschluss eines Handelsgeschäfts, Rechnungen. Somit unterliegen die Handelsbriefe den buchhalterischen Aufbewahrungsfristen immer dann, wenn sie folgende Inhalte aufweisen:

- Wertbewegungen,
- Mengenbewegungen,
- vereinbarte Mengendispositionen oder
- vertragliche Verpflichtungen.

Korrespondenz, die nicht zum Abschluss von Handelsgeschäften geführt hat (z. B. Prospekte, nicht erfolgreiche Angebote), ist ebenso wenig Handels-/Geschäftsbrief wie der Austausch allgemeiner, unverbindlicher Informationen.

Hashwert

Ein Hashwert ist ein eindeutiger Zahlenwert, der durch einen mathematischen Algorithmus aus dem Inhalt einer Information gebildet wird. Somit ist Integrität einer Information überprüfbar, da die erneute Bildung des Hashwerts bei einem kollisionsresistenten Hash-Verfahren den gleichen Hashwert als Ergebnis liefern muss. Wird also ein Dokumente absichtlich oder versehentlich manipuliert, wird eine spätere Hashwert-Berechnung ein anderes Ergebnis als bei der ersten Berechnung erbringen. Diese »Prüfsummen«-Verfahren kommen immer dann zum Einsatz, wenn mit hoher Aussagesicherheit eine nachträgliche Veränderung von Information geprüft werden soll, also bei Archivspeichern als auch bei fortgeschrittenen oder qualifizierten Signaturen und Zeitstempeln usw.

HGB
Handelsgesetzbuch. Aufbewahrungsrelevante Vorschriften finden sich vor allem im Dritten Buch (Handelsbücher), erster Abschnitt (Vorschriften für alle Kaufleute) in den §§ 239 und 257 HGB. Die Aufbewahrungsvorschriften in HBG waren bis 1. Januar 2002 weitgehend identisch mit den Vorschriften der Abgabenordnung (AO). Erst danach kam es im Bereich der steuerlichen Aufbewahrung zu weiteren Anforderungen (siehe hierzu GDPdU) und damit bis heute zu einer Abweichung bei den Aufbewahrungsvorschriften zwischen AO und HGB.

IDEA
Interactive Data Extraction and Analysis

IDEA ist eine Software zur Analyse großer Datenmengen. Die Software wurde ursprünglich in der internen Revision und im Controlling eingesetzt. Seit 1. Januar 2002 setzt die Finanzverwaltung die Software bei Außenprüfungen zur Analyse der ihr übergebenen Daten auf einem Datenträger (Z3-Zugriff) ein. Die Software wird mittlerweile auch von der Zollverwaltung verwendet.

IKS
Im Folgenden werden als Internes Kontrollsystem (IKS) die vom Buchführungspflichtigen zur Einhaltung der GoB umgesetzten organisatorischen Regelungen und technischen Maßnahmen bezeichnet, welche die Steuerung und Überwachung des IT-gestützten Buchführungssystems zum Gegenstand haben. Daher umfasst das IKS die Gesamtheit aller aufeinander abgestimmten Grundsätze, Maßnahmen und Vorkehrungen eines Unternehmens, die zur Bewältigung der Risiken aus dem Einsatz eines IT-gestützten Buchführungssystems eingerichtet werden. Es dient insbesondere zur Vermeidung, Aufdeckung und Beseitigung von Fehlern in den buchführungsrelevanten Arbeitsabläufen. Die Verantwortung für die Einrichtung eines wirksamen IKS liegt beim Buchführungspflichtigen.

Das IKS beinhaltet prozessintegrierte (Kontroll-)Maßnahmen und prozessunabhängige (Überwachungs-)Maßnahmen. Es stellt damit einen wesentlichen Bestandteil des gesamten betrieblichen Risiko-Management-Systems dar. Dessen konkrete Ausgestaltung erfolgt in Abhängigkeit von der Unternehmensgröße, -branche und -komplexität und den daraus resultierenden Risiken (Risikoäquivalenzprinzip). Die Einhaltung der Ordnungsmäßigkeit ist bei der Einrichtung eines solchen Systems als Rahmenvoraussetzung sicherzustellen.

Indossierung/Imprinter
Kennzeichnung von gescannten Dokumenten im Rahmen des Scan-Prozesses. Ein Imprinter ist ein spezieller, im Scanner eingebauter Drucker. Alle Seiten, die gescannt werden, erhalten bspw. an einer bestimmten Stelle einen kleinen Aufdruck (Imprinting). Dies kann ein immer gleicher Code sein, ein Datumswert, eine fortlaufende Nummer oder eine Kombination aus diesen Möglichkeiten.

IT System
Hard- und Softwarekomponenten mit denen das Erstellen, Bearbeiten, Verarbeiten und Speichern von Informationen möglich ist.

Die Begriffe IT System und EDV System werden meist synonym verwendet.

Journalfunktion
Die Journalfunktion verlangt, dass alle Geschäftsvorfälle zeitnah nach ihrer Entstehung vollständig und verständlich sowie formal richtig in zeitlicher Reihenfolge aufgezeichnet werden (Journal).

Kontenfunktion
Zur Erfüllung der Kontenfunktion müssen die Geschäftsvorfälle nach Sach- und Personenkonten geordnet dargestellt werden können. Die Kontenfunktion kann auch durch Führung von Haupt- und Nebenbüchern in unterschiedlichen IT-Anwendungen erfüllt werden.

Konvertierung
Bezeichnet die Umwandlung von Daten mittels sogenannter Konvertierungsprogramme von einem in ein anderes Datenformat. Die Formatkonvertierung ermöglicht z. B. die Weiterverarbeitung der Daten in anderen Programmen, auch wenn ein Import nicht möglich wäre.

Maschinelle Auswertbarkeit
Maschinell auswertbar sind Unterlagen, wenn sie maschinell gelesen, maschinell gefiltert/selektiert und maschinell sortiert werden können.

Migration von Daten und Dokumenten

Transfer von Daten in eine andere Umgebung einschließlich der dazu erforderlichen technischen Anpassungen ohne inhaltliche Veränderung der Informationen.

Nettoimaging

Der Verfahrensablauf des Nettoimaging entspricht dem des Bruttoimaging mit folgendem wesentlichen Unterschied: Beim Nettoimaging werden beim Scannen bestimmte Bildinformationen herausgefiltert, wodurch nur ein Teil der Bildinformationen des Originals in dem im System gespeicherten Image (Nettoimage) enthalten sind.

Das Verfahren des Nettoimaging ist beispielsweise beim Scannen von Formularen anwendbar, da ausschließlich die ausfüllbaren Bereiche und nicht die Formularinformationen gespeichert werden, was zu einem deutlich verringerten Speicherbedarf führt.

OCR

Optical Character Recognition. Ursprünglich Name für Verfahren zur Erkennung genormter Schriften wie OCR-A (nur Großbuchstaben) und OCR-B (Groß- und Kleinbuchstaben) über optische Leseeinheiten. Heute steht der Begriff allgemeiner für die Erkennung von maschinell oder auch handschriftlich aufgebrachten Zeichen aus einem Rasterbild. Die erkannten Zeichen werden in Zeichencode (ASCII oder ISO-8859) gewandelt und stehen somit für eine maschinelle Weiterverarbeitung zur Verfügung.

Originär digitale Unterlagen

In einem IT System erzeugte Daten bzw. mit einer Software erzeugte Dokumente

oder: Daten, die in einer elektronischen Form in ein IT System eingegangen sind bzw. Dokumente, die elektronisch empfangen wurden.

Outsourcing

Aus dem Englischen »Outsource – Resource – Using«; steht für Nutzen fremder Quellen und Kapazitäten.

Verlagerung von betrieblichen Aktivitäten eines Unternehmens an einen Fremdanbieter (Outsourcing-Nehmer). Ziel ist meist eine Verringerung von Gemeinkosten im eigenen Unternehmen und die Konzentration auf das Kerngeschäft.

PDF

Portable Document Format, entwickelt von Adobe und 1993 vorgestellt. PDF basiert auf Postscript und erlaubt die plattformunabhängige Erstellung und Verteilung von Dokumenten, gerade auch bei grafisch anspruchsvollen Inhalten. PDF ist ein Containerformat, es kann sowohl CI- (z. B. Texte) als auch NCI-Komponenten (z. B. CCITT G4 oder JPEG-Bilder) beinhalten. PDF-Viewer sind meistens kostenlos und für alle gängigen Client-Plattformen verfügbar. PDF entwickelt sich zunehmend zum dominierenden Format auch im Archivumfeld, weil neben der universellen Verfügbarkeit des Formates mit PDF/A ein von der ISO verabschiedeter Standard auf PDF-Basis für die Langzeitarchivierung verfügbar ist.

PDF/A

Kurzbezeichnung für die ISO-Norm 19005-1 »ISO 19005-1, Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)«. PDF/A wurde als Dokumentenformat für die Langzeitarchivierung konzipiert. Teil 1 der ISO-Norm basiert auf PDF-Version 1.4 und macht Vorgaben zu erlaubten und verbotenen Inhalten eines PDF-Dokuments. Die ISO-Norm wurde im September 2005 veröffentlicht.

Die Spezifikation unterscheidet im Teil 1 die Varianten a und b. Variante a beinhaltet zusätzliche Funktionen zur Textextraktion wie PDF-Tagging, um den barrierefreien Zugang zu ermöglichen. Die meisten Produkte unterstützen nur PDF/A 1-b.

PDF/A ist mittlerweile in der dritten Version verfügbar, um neuere Funktionen nutzen zu können. Bei einer neuen Version ist immer die Rückwärtskompatibilität sichergestellt, d. h. wer keine der neueren Funktionen benötigt (z. B.: Transparenzen, eingebettete Dateien etc.), kann auch weiterhin im PDF/A-1 Format archivieren.

Revisionssichere Archivierung

Der Begriff »Revisionssicherheit« ist gesetzlich nicht verankert und es existiert keine offizielle Zertifizierung für »revisionssichere« Archivsystemprodukte.

Man bezeichnet solche Systeme und Verfahren als revisionssicher, die den Anforderungen der §§ 146, 147 AO, §§ 239, 257 HGB sowie der GoBS vollständig entsprechen. Hier gehören vor allem eine gegen unzulässige Manipulation geschützte Aufbewahrung und die

Sicherstellung der Reproduktionsfähigkeit über die Dauer der Aufbewahrungsfrist sowie die Dokumentation der Ordnungsmäßigkeit des Verfahrens zur Herstellung der Prüfbarkeit für Dritte. Statt »revisionssicher« wäre die Formulierung »auf Ordnungsmäßigkeit prüfbar« daher die bessere, aber vielleicht auch weniger griffige und daher weniger populäre Formulierung.

Scannen Hierbei wird mit einer Hardware (Scanner) zum rasterförmigen Auflösen eines Bildes in Bildpunkte und Umwandlung der im Bild enthaltenen schwarzen, weißen, grauen oder farbigen Werte in ein entsprechendes Bit-Muster nicht kodierter Daten erstellt. Die Abtastung der Bildpunkte erfolgt zeilenweise.

TIFF

Tagged Image File Format. Entwickelt von Aldus ab 1986 unter Beteiligung anderer Firmen (Microsoft, HP u. a.). 70 Tags (Merkmalskennzeichner) zur Beschreibung der Eigenschaften wie z. B. Kompressionsalgorithmus, Anzahl Bits per Pixel, Anzahl vertikale und horizontale Pixel. Seit TIFF Version 5.0 werden 5 Coding-Schemata unterstützt: ->CCITT G3, Fax G3, Fax-kompatibles ->CCITT G4, ->LZW und PackBit. Entwickler können TIFF um eigene Tags erweitern. TIFF-Dateien können nicht immer von jedem TIFF-Viewer gelesen werden, weil die Flexibilität der TIFF-Spezifikationen unterschiedliche Kompressionsalgorithmen erlaubt. Derzeit aktuelle Version ist 6.0, gültig seit Juni 1992, damals noch von Aldus veröffentlicht.

Aldus – und damit auch die TIFF-Spezifikation – wurde 1994 von Adobe übernommen. TIFF spielt heute als Rohformat beim Scanning immer noch eine große Rolle, weil sich hier noch relativ einfach Strukturkorrekturen an den Scan-Stapeln vornehmen lassen. Als Ablageformat in DMS-/Archivlösung wird TIFF aber zunehmend von PDF abgelöst.

Verfahrensdokumentation Die Verfahrensdokumentation ist i. d. R. ein Dokument, welches in verschiedenen Abschnitten auch Querverweise auf andere Dokumente (z. B.: Arbeitsanweisungen, Bedienungsanleitungen, Installationsleitfäden etc.), die im Unternehmen gültig sind, enthält. Die Verfahrensdokumentation soll so geschrieben sein, dass ein sachverständiger Dritter in angemessener Zeit den ordnungsgemäßen Einsatz des Buchhaltungssystems und/oder des Archivsystems prüfen und nachvollziehen kann.

Volltextdatenbank

Eine Volltextdatenbank dient hauptsächlich der Indexierung der Dokumentinhalte und nicht nur ihrer Metadaten. Somit sind auch Inhaltssuchen möglich. Fast alle ECM-/DMS-Lösungen erlauben neben der strukturierten Indexierung (in relationalen oder anderen Datenbanken zur Verwaltung der Metadaten) auch die Nutzung der Volltextindexierung. Um die Volltextsuche zu ermöglichen, sind neben der eigentlichen Volltextengine weitere Komponenten notwendig, wie zum Beispiel die Filter zum Indexieren von MS Office oder anderen Dateien in den jeweils notwendigen Software- und Sprachversionen.

XML

eXtensible Markup Language, abgeleitet von SGML. XML ist sowohl ein Datenformat als auch eine Metasprache zur Beschreibung der formalen Eigenschaften eines Textes. XML kann Metadaten wie z. B. Versionsinformationen oder selbstdefinierte Indexwerte beinhalten und eignet sich daher zur Kommunikation zwischen verschiedenen Anwendungen.

Z1, Z2, Z3

siehe Datenzugriff

ZUGFeRD

ZUGFeRD (Akronym für Zentraler User Guide des Forums elektronische Rechnung Deutschland) ist eine Spezifikation für das gleichnamige Format elektronischer Rechnungen. Das Format wurde vom Forum elektronische Rechnung Deutschland in Zusammenarbeit mit Verbänden, Ministerien und Unternehmen entwickelt. Am 25. Juni 2014 wurde die Version 1.0 der Spezifikation veröffentlicht.

8 Die Autoren

Thorsten Brand
ist seit 1992 als produktneutraler Berater im Bereich ECM tätig. Seine Tätigkeitsschwerpunkte umfassen:

- Prozess- und Organisationsberatung
- Erstellung von Vor-/Machbarkeitsstudien
- Begutachtung bestehender Systemumgebungen/-konzepte
- Anforderungsanalysen
- Erstellen von Lösungskonzepten
- Unterstützung bei der Systemauswahl
- Begleitung/Qualitätssicherung bei der Systemeinführung
- Unterstützung bei Abnahmetests/Systemabnahme
- Erstellung von Verfahrensbeschreibungen
- Durchführung von Projekt-Reviews
- Projektbegleitung-/Projektmanagement

Er ist stlv. Leiter des Arbeitskreises »ECM-Compliance« des Bitkom e. V.
Seit 2000 ist Thorsten Brand Senior-Berater der Zöller & Partner GmbH.

Stefan Groß
ist als Steuerberater und Certified Information Systems Auditor (CISA) an der Schnittstelle zwischen IT und Steuerrecht tätig. Seine Tätigkeitsschwerpunkte liegen in den Bereichen:

- Steuerrecht und Neue Medien
- IT-Revision und EDV-Sonderprüfungen
- GoBD-Audits und GoBD-Beratung
- Fragen zum Datenzugriff der Finanzverwaltung (GDPdU)
- Electronic Invoicing
- Prüfungen nach IDW PS 330, PS 951, SAS 70, FAIT 3
- Datenanalysesoftware in der Jahresabschlussprüfung
- Umsatzsteuer-Risikomanagement

Stefan Groß ist Partner der Kanzlei Peters, Schönberger & Partner mbB in München.

Weitere Funktionen: Vorstandsvorsitzender der VeR (Verband elektronische Rechnung e. V.), Leiter des Arbeitskreises Qualität des VeR, Leiter des Arbeitskreises »ECM-Compliance« des Bitkom e. V.

Wolfgang Heinrich
ist Diplominformatiker und als Produktmanager an der Schnittstelle zwischen technischen und rechtlichen

Aspekten des Enterprise Content Managements tätig. Seine Tätigkeitsschwerpunkte liegen in den Bereichen:

- Rechtliche Rahmenbedingungen des Dokumentenmanagements
- Elektronische Signaturen
- Prozess- und Organisationsberatung
- E-Mail-Management und E-Mail-Archivierung
- Erstellung von Verfahrensdokumentationen
- Gestaltung und Einsatz von DMS-Softwareprodukten
- Prüfkriterien für Dokumentenmanagementsysteme
- Begleitung von Systemprüfungen und Audits

Er ist langjährig aktives Mitglied der Arbeitskreise »ECM-Compliance«, »ECM-Standards« und »Anwendung elektronischer Vertrauensdienste« des Bitkom e. V.

Seit 1995 ist Wolfgang Heinrich als Mitarbeiter bei der EASY SOFTWARE AG tätig.

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom