GoBD-Checkliste

für Dokumentenmanagement-Systeme
Version 2.0

www.bitkom.org

bitkom

Herausgeber

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

Ansprechpartner

Nils Britze | Bereichsleiter Digitale Geschäftsprozesse
T 030 27576-201 | n.britze@bitkom.org

Verantwortliches Bitkom Gremium

AK ECM-Compliance

Besonderer Dank gilt dem Autorenteam, bestehend aus:
- Thorsten Brand | Zöller & Partner GmbH
- Stefan Groß | PSP Peters Schönberger GmbH Wirtschaftsprüfungsgesellschaft, Steuerberatungsgesellschaft
- Lukas Büttner | PSP Peters Schönberger GmbH Wirtschaftsprüfungsgesellschaft, Steuerberatungsgesellschaft.

Satz & Layout

Sabrina Flemming | Bitkom

Titelbild

© mnirat – adobe.stock.com

GoBD-Checkliste

für Dokumentenmanagement-Systeme
Version 2.0

Inhaltsverzeichnis

1 Einleitung

1 Einleitung

1.1 Vorwort zur neuen Auflage

Nach über fünf Jahren wurde mit Datum vom 28. November 2019 eine Neufassung der GoBD verabschiedet, in der gerade innovative Prozesse wie etwa das »Mobile Scannen« sowie Vereinfachungen in Bezug auf »Ersetzende Konvertierungen« und im Zusammenhang mit Systemwechseln und Datenauslagerungen ihren Niederschlag gefunden haben. So stellt die Finanzverwaltung nun unmissverständlich klar, dass eine Erfassung von Handels- oder Geschäftsbriefen sowie Buchungsbelegen, welche in Papierform empfangen wurden, mit den verschiedensten Arten von Geräten wie Smartphones, Multifunktionsgeräten oder Scanstraßen erfolgen kann. Eine weitere wesentliche Nachjustierung betrifft Erleichterungen im Zusammenhang mit Formatkonvertierungen. Auch hier hat die Finanzverwaltung die Zeichen der Zeit erkannt und gesteht den Unternehmen in ausgewählten Fällen nun die isolierte Aufbewahrung der konvertierten Fassung zu. Mit den am digitalen Fortschritt ausgerichteten Änderungen stellt das Update einen deutlichen Zugewinn an Rechtssicherheit und Klarheit für die Unternehmenspraxis dar. Damit wird die Neufassung der GoBD sowohl der Unternehmensrealität als auch den IT-technischen Gegebenheiten gerecht, gehen damit doch auch erhebliche Vereinfachungen sowie Möglichkeiten zur Prozessoptimierung einher. Die nun vorliegende Version 2.0 der GoBD-Checkliste für Dokumentenmanagement-Systeme stellt vollumfänglich auf die Neufassung der GoBD ab und berücksichtigt die entsprechenden Änderungen.

1.2 Zielsetzung dieser Checkliste

Mit einem Dokumentenmanagement-System (DMS) lassen sich originär elektronische sowie digitalisierte Dokumente verwalten.[1] Eine DMS-Anwendung dient der Organisation und Koordination der Erstellung, Überarbeitung, Überwachung und Verteilung sowie 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 für Zwecke der Betriebsprüfung vorgehalten werden müssen.

Hinweis

Besonderheiten des Datenschutzes sowie der Datenschutz-Grundverordnung (DSGVO) sind nicht Gegenstand dieser Checkliste und müssen ggf. gesondert Beachtung finden.

Die Vorgaben für die Aufbewahrung und Verfügbarmachung sind in den 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.

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.

Ausgehend von den Anforderungen der GoBD stellt die vorliegende Checkliste die daraus sich 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 von entsprechenden Softwarelösungen.

1.3 Die GoBD

Mit Schreiben vom 28. November 2019, den »Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer 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]. Mit der Neufassung folgt das BMF letztlich auch den Forderungen der Wirtschaft nach einer erforderlichen Modernisierung der GoBD und richtet diese damit am digitalen Fortschritt aus. Die wichtigsten Änderungen im Überblick:

- Das Fotografieren von Belegen durch mobile Endgeräte (Mobiles Scannen) wird dem stationären Scanvorgang gleichgestellt
- Die bildliche Erfassung durch mobile Endgeräte im Ausland ist zulässig
- Das Verbringen von Papierbelegen ins Ausland mit anschließender Digitalisierung ist zulässig
- Möglichkeit des ersetzenden bzw. verlustfreien Konvertierens
- Beschränkungsmöglichkeit auf Z3-Zugriff nach Systemwechsel oder Auslagerung

Die Neufassung der GoBD ist auf Besteuerungszeiträume anzuwenden, die nach dem 31. Dezember 2019 beginnen. Es wird nicht beanstandet, wenn der Steuerpflichtige die Grundsätze dieses Schreibens auf Besteuerungszeiträume anwendet, die vor dem 1. Januar 2020 enden.

2 BMF v. 28. November 2019 – IV A 4 – S 0316 / 19 / 10003 :001, tritt an die Stelle des BMF-Schreibens 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.

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

1.4 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 entsprechend auch von einem DMS erfüllt werden. Dabei muss sichergestellt sein, dass die Daten, respektive deren Wiedergabe, mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich sowie mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. Weiter ist 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 sind daher nicht mehr ausschließlich in ausgedruckter Form aufzubewahren, sondern 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 zutage. Zugleich muss sich – bei Einsatz eines DMS – dieses an den Vorgaben der GoBD messen lassen. Das betrifft insbesondere die Vorgaben an die Aufbewahrung und Bereitstellung (insbesondere für den Datenzugriff der Finanzverwaltung) entsprechender Dokumente und Datenbestände.

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

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

1.5 Weitere relevante Vorschriften für die elektronische Aufbewahrung

Auf Basis der wesentlichen Anforderungen der GoBD zeigt diese Checkliste Handlungsempfehlungen auf, 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 Dokumentationen in die Betrachtung einbezogen werden:

- IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie
- IDW PS 880: Die Prüfung von Softwareprodukten
- IDW PS 951 n.F.: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen
- IDW PS 980: Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen
- IDW RS FAIT 1: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie
- IDW RS FAIT 3: Grundsätze ordnungsmäßiger Buchführung bei Einsatz elektronischer Archivierungsverfahren
- IDW RS FAIT 5: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing

1.6 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 im konkreten Einzelfall erfüllen kann. Der Grund hierfür liegt in der Technologieneutralität, 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-Halbwertzeiten sowie der zum Teil sehr großen Unterschiede im organisatorischen Umfeld der verschiedenen Unternehmen nicht festgeschrieben werden können.

Es wird daher durchaus Fallkonstellationen geben, bei denen 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 (im Allgemeinen 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 System- bzw. Softwarelösungen ableiten.

Die Checkliste führt von den grundsätzlichen Anforderungen an die Ordnungsmäßigkeit zu den Anforderungen für den IT-Betrieb im Allgemeinen. Danach 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 den ordnungsmäßigen IT-Betrieb	Allgemeine Anforderungen an den IT-Betrieb und das Cloud Computing werden unabhängig vom Einsatz einer DMS-Umgebung betrachtet.
Ausgewählte Erfassungs- und Verarbeitungsprozesse im DMS	Besonderheiten von einzelnen DMS-Prozessen wie z. B. Scanning, mobile Erfassung, E-Mail-Archivierung oder die Verarbeitung von elektronischen Rechnungen werden aufgezeigt.
Besondere Anforderungen aus steuerlicher Sicht	Bezugnahme auf besondere Anforderungen, die sich aus steuerlicher Sicht ergeben, die aber nicht direkt im Zusammenhang mit der Aufbewahrung von Dokumenten stehen.
Verfahrensdokumentation	Hinweise zum Aufbau (Gliederung) und zu den Inhalten einer DMS-Verfahrensdokumentation.

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 (vgl. ↗ GoBD-Kapitel 2.1)
- Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung (vgl. ↗ GoBD-Kapitel 2.2), mit den Einzelthemen
  - Vollständigkeit (vgl. ↗ GoBD-Kapitel 2.2.1)
  - Richtigkeit (vgl. ↗ GoBD-Kapitel 2.2.2)
  - Zeitgerechte Belegsicherung (vgl. ↗ GoBD-Kapitel 2.2.3)
  - Ordnung (vgl. ↗ GoBD-Kapitel 2.2.4)
  - Unveränderbarkeit (vgl. ↗ GoBD-Kapitel 2.2.5)

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. Als Neben- oder Hilfssystem ist dabei auch ein DMS von entsprechender Relevanz. Es enthält erfasste Daten sowie Belege (z. B. durch Scannen von Papierunterlagen) und übernimmt die längerfristige Speicherung (Aufbewahrung) von Daten bzw. Dokumenten. Dabei ist zum einen die vollständige und fehlerfreie Erfassung der Unterlagen (inkl. der Stamm- und Indexdaten) sicherzustellen. Zum anderen dürfen während der Aufbewahrung keine Daten oder Dokumente verloren gehen oder verfälscht werden.

Nachfolgend werden zunächst die generellen, wesentlichen 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 Ausgewählte Erfassungs- und Verarbeitungsprozesse im DMS behandelt.

Anmerkung: Diverse aktuelle 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 und Kontrollziel

Die Verarbeitung der einzelnen Geschäftsvorfälle sowie das dabei angewandte Buchführungs- und Aufzeichnungsverfahren müssen nachvollziehbar und nachprüfbar sein. Die Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung lückenlos verfolgen lassen (progressive und retrograde Prüfbarkeit). Hieraus ergibt sich insbesondere auch das Erfordernis einer aussagekräftigen und vollständigen Verfahrensdokumentation.

b) DMS-Kontext

Dem Kontrollziel entsprechend müssen die rechnungslegungsrelevanten DMS-Prozesse durch eine geeignete Dokumentation nachvollziehbar sein (vgl. ↗ Kapitel 6 Verfahrensdokumentation).

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 sowie Verfälschung zu sichern. Hier bietet es sich meist an, die Archivkomponente des DMS zur Speicherung der Protokolle zu verwenden. Auch die Verfahrensdokumentation selbst (inkl. mitgeltender Unterlagen) sollte im elektronischen Archiv gespeichert werden.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Umsetzungsmöglichkeiten und Hinweise
(1)	Nachvollziehbarkeit bei der Erfassung von Daten und Dokumenten	▪ Protokollierung der Erfassungsaktionen (Import, elektronisch bildliche Erfassung via Scan oder Fotografie, Indizierung, Konvertierung, Archivierung, Qualitätssicherung) mit Datum / Uhrzeit und ggf. der beteiligten Personen.
(2)	Nachvollziehbarkeit von Änderungen an Daten und Dokumenten	▪ Protokollierung der zu ändernden Aktionen mit Datum / Uhrzeit und ggf. der beteiligten Personen. ▪ Eine Änderung erzeugt stets eine neue Version des Dokuments, sodass frühere Inhalte uneingeschränkt nachvollziehbar bleiben. ▪ Hinweis: Vgl. auch ↗ Kapitel 2.2.5 Unveränderbarkeit.
(3)	Progressive und retrograde Prüfbarkeit	▪ Geschäftsvorfälle lassen sich in ihrer Entstehung und Abwicklung lückenlos verfolgen. ▪ Mithilfe von Indexdaten oder technisch eindeutigen IDs soll die Nachvollziehbarkeit gewährleistet werden; sowohl vom Eingangsbeleg zur Buchung (progressiv) als auch von der Buchung zurück zum Beleg (retrograd).
(4)	Belegprinzip	▪ Die Buchungen und die sonst erforderlichen Aufzeichnungen müssen durch einen Beleg nachgewiesen sein oder nachgewiesen werden können. ▪ Bei einem elektronischen Beleg kann die mit der Prüfbarkeit einhergehende Belegfunktion durch die Verbindung des Datensatzes mit den korrespondierenden Angaben zur Kontierung bzw. durch eine elektronische Verknüpfung erfolgen.
(5)	Kein Informationsverlust bei Konvertierungen	▪ Soweit eine Umwandlung (Konvertierung) aufbewahrungspflichtiger Unterlagen in ein unternehmenseigenes Format (sog. Inhouse-Format) erfolgt, sind beide Versionen aufzubewahren, derselben Aufzeichnung zuzuordnen und mit demselben Index zu verwalten. Bei einer Prüfung sind diese auf Anforderung zur Verfügung zu stellen. ▪ Die Aufbewahrung beider Versionen ist bei Beachtung bestimmter Anforderungen (keine bildliche oder inhaltliche Veränderung, kein Verlust aufbewahrungspflichtiger Informationen, keine Einschränkung der maschinellen Auswertbarkeit und des Datenzugriffs, Vorhandensein einer Verfahrensdokumentation, welche die verlustfrei Konvertierung dokumentiert) nicht erforderlich, sondern es ist die Aufbewahrung der konvertierten Fassung ausreichend (»Ersetzendes Konvertieren«). ▪ Im Falle von Datenkonvertierungen und / oder Datenkompression werden geeignete Datenformate und Verfahren gewählt, sodass die Lesbarkeit der Daten und Dokumente sowie die maschinelle Auswertbarkeit von Daten erhalten bleiben. ▪ Hinweis: Zu besonderen Anforderungen aus steuerlicher Sicht, vgl. ↗ Kapitel 5 Besondere Anforderung aus steuerlicher Sicht.
(6)	Nachvollziehbarkeit von administrativen Änderungen	▪ Protokollierung der Änderungen an Systemeinstellungen, einschließlich der Protokollierung bei direkten Datenbankzugriffen (bspw. seitens der Datenbankadministratoren).
(7)	Nachvollziehbarkeit des gesamten DMS-Verfahrens	▪ Erstellung einer aussagekräftigen und vollständigen Verfahrensdokumentation (inkl. Änderungs- bzw. Review-Historie mit Datum / Uhrzeit und beteiligten Personen). ▪ Vorhandensein eines regelmäßigen Review-Prozesses der Verfahrensdokumentation zur Sicherstellung der tatsächlichen Identität von Prozess und Dokumentation. ▪ Vorhandensein eines Freigabekonzepts für Änderungen der relevanten, beschriebenen IT-Prozesse (z. B. Prozessrollen). ▪ Hinweis: Zur Verfahrensdokumentation vgl. ausführlich ↗ Kapitel 6 Verfahrensdokumentation.
(8)	Nachvollziehbarkeit während der gesamten Aufbewahrungsfrist	▪ Vorhandensein eines Prozesses, durch den die Aufbewahrung der erforderlichen Bücher und sonst erforderlichen Aufzeichnungen sowie der jeweils gültigen Verfahrensdokumentation über die Dauer der gesetzlichen Aufbewahrungsfrist sichergestellt wird. ▪ Verlust- und fälschungssichere Aufbewahrung der erforderlichen Protokolle entsprechend der gesetzlich vorgeschriebenen Aufbewahrungsfrist der Daten und Dokumente (im DMS sowie in anderen Systemen).

2.2 Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung

2.2.1 Vollständigkeit

a) Grundsatz und Kontrollziel

Die Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen.

b) DMS-Kontext

Dem Kontrollziel entsprechend hat im DMS eine lückenlose Erfassung aller rechnungslegungsrelevanten Dokumente und Daten zu erfolgen. 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 auch mit Blick auf etwa vorhandene Schnittstellen von zentraler Bedeutung. Neben der Vollständigkeit von angelieferten Daten- und Dokumentbeständen geht es auch um die Vollständigkeit von Dokumenten an sich, bspw. E-Mails inkl. der dazugehörigen Anhänge sowie um eine vollständige Indizierung von Dokumenten.

Die Vollständigkeit ist auch im Hinblick auf die Art der Aufbewahrung 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 bildlich darstellbaren 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 ggfs. nicht immer über die Dauer der Aufbewahrungsfrist reproduzierbar bleiben, insbesondere dann, wenn sich Stammdaten ändern und die Versionsstände keiner Historisierung unterliegen.

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

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(9)	Vollständige und lückenlose Erfassung allgemein	▪ Implementierung eines übergreifenden Konzepts zur Sicherstellung der vollzähligen und lückenlosen Erfassung (Einzelaufzeichnungspflicht). ▪ Sicherstellung, dass die zu archivierenden Daten und Dokumente für jede Erfassungsart vollständig erfasst werden. ▪ Sicherstellung, dass sämtliche Daten und Dokumente einzeln erfasst werden. ▪ Durchführung technischer und / oder organisatorischer Plausibilitätskontrollen bei Eingabe oder Übernahme von Daten und Dokumenten. ▪ Zählen von Belegen und Abgleich mit den Verarbeitungsdaten. ▪ Definition von Import- / Stapelgrößen (z. B. im Stapel von 100 Dokumenten).
(10)	Vollständige Erfassung der Daten und Dokumente	▪ Alle Daten und Dokumente, die für eine Archivierung angeliefert werden, müssen vollständig verarbeitet werden (betrifft insbesondere die Systemschnittstelle eines DMS). ▪ Fehler betreffend Vollständigkeit müssen angezeigt werden und nachvollziehbar sein. ▪ Neben technischen Systemprotokollen und Überwachungswerkzeugen sind organisatorische Regelungen in Betracht zu ziehen (z. B. regelmäßige Prüfung, ob eine Anlieferung komplett verarbeitet wurde). ▪ Ergänzend sind Regeln für die manuelle Erfassung 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). ▪ Hinweis: Maßnahmen bei der bildlichen Erfassung und bei der E-Mail-Erfassung, vgl. ↗ Kapitel 4 Ausgewählte Erfassungs- und Verarbeitungsprozesse im DMS.
(11)	Vermeidung doppelter Erfassung von Geschäftsvorfällen	▪ Implementierung automatischer Funktionen bzw. Kontrollen, welche die Doppelerfassung verhindern (z. B. durch die Definition des Indexfeldes »Rechnungsnummer« als »unique« im DMS wird darauf hingewiesen, dass mehrere Daten oder Dokumente mit der gleichen Rechnungsnummer erfasst wurden). ▪ Implementierung von Mehrfachbelegungsanalysen (z. B. Reports zur Entdeckung von doppelt vorhandenen Rechnungsnummern oder Unterbinden von Mehrfachbelegungen durch technische Sperre). ▪ Hinweis: Selbst erstellte Dokumente können einen längeren Bearbeitungsprozess durchlaufen, wobei im DMS mehrere Zwischenversionen gespeichert werden. Dabei ist technisch und / oder organisatorisch zwischen (internen) Vorversionen und (rechnungsrelevanten) finalen Dokumenten zu unterscheiden. Bestimmte DMS bieten dazu passende »Lebenszyklus«-Funktionen an (z. B. Status »in Arbeit«, »final« etc.).
(12)	Vollständigkeit und Korrektheit von Daten, die von anderen Daten abhängen	▪ Sicherstellung durch historisierte (versionierte) Speicherung bei Änderung von Stammdaten. ▪ Sicherstellung, dass ein Dokument auf Basis der historischen Stammdaten rekonstruiert werden kann (z. B. Rechnung an Kunden, dessen Adresse später in den Stammdaten geändert wurde). ▪ Hinweis: Vgl. auch ↗ Kapitel 4.1 Archivierung von Ausgangsdokumenten.
(13)	Vollständigkeit und Korrektheit von Daten, die von Konfigurationsdaten abhängen	▪ Sicherstellung durch historisierte (versionierte) Speicherung von bestimmten Konfigurationsdaten des Systems. ▪ Beispiel: 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 einer späteren Änderung des Briefkopfs, 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 (bildhafte) Kopien im Archiv abgelegt. Die Dokumente können somit jederzeit ohne Zugriff auf andere Daten im DMS recherchiert und angezeigt werden. ▪ Hinweis: Vgl. auch ↗ Kapitel 4.1 Archivierung von Ausgangsdokumenten.

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(14)	Vollständige und lückenlose Übernahme von Daten und Dokumenten aus Fremdsystemen	▪ Sicherstellung durch manuelle oder automatische Prüfung / Abgleich von Protokollen (z. B. systemseitige Summenprüfung: System A hat lt. Protokoll 1.000 Dokumente exportiert; somit muss auch das DMS 1.000 Dokumente importiert haben). ▪ Sicherstellung durch alternative Abgleiche mit externen Systemen (z. B. Identifikation gescannter Barcode-Belege, die keiner Buchung im ERP zugeordnet werden können). ▪ Implementierung einer Transaktionskontrolle bei Datenübernahme. Im Fehlerfall wird ersichtlich, welche Daten und Dokumente nicht angekommen sind und daher erneut importiert werden müssen. ▪ Vorhandensein von Kontrollen, welche sicherstellen, dass die Inhalte bestimmter Indexfelder eines Datenbestands lückenlos sind (z. B. Lückenanalyse auf Basis von Belegnummern). Hier bietet sich ggf. die Nutzung von DMS-Funktionen (Auswertung von Trefferlisten, Reports, Skripts) an.
(15)	Die Erfassung und Verarbeitung darf nicht unterdrückt werden	▪ Es existieren keine Funktionen, die die Erfassung und Verarbeitung von Daten und Dokumenten unterdrücken. ▪ Vorhandensein eines Prozesses, der bei Änderungen weiterhin die ordnungsgemäße Erfassung / Verarbeitung der Daten sicherstellt (u. a. Test- und Abnahmeverfahren).
(16)	Keine Zusammenfassung und Verdichtung von Daten und Dokumenten	▪ Es wird sichergestellt, dass Daten und Dokumente nicht derart zusammengefasst oder verdichtet werden können, dass relevante Informationen nicht mehr vorhanden sind. ▪ Das Zusammenfassen von Dokumenten, bspw. im Rahmen einer Bestandskonvertierung von Papierdokumenten ist zulässig, wenn die Ordnung und Struktur der Papierdokumente erhalten bleibt.
(17)	Vollständigkeit von Daten und Dokumenten über die gesamte Aufbewahrungsfrist	▪ Keine Löschmöglichkeit vor dem Ende der Aufbewahrungsfrist. ▪ Keine automatisierte Löschung von Daten und Dokumenten nach Ende der Aufbewahrungsfrist (z. B. stets alle Daten oder Dokumente löschen, die älter als X Jahre sind). ▪ Für die Löschung ist zwingend eine organisatorische Freigabe einzuholen, 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 (Ablaufhemmung). ▪ Hinweis: Außersteuerliche Regelungen können eine längere Aufbewahrungsfrist erfordern.
(18)	Langzeitformate für Dokumente zur Sicherstellung der vollständigen Reproduzierbarkeit	▪ Grundsätzliche Beschränkung der Formate für die Langzeitarchivierung. ▪ Bspw. Konvertierung aller Eingangsformate in ein Langzeitarchivierungsformat, wie PDF / A (Fehler-Handling erforderlich, da Konvertierung nicht immer fehlerfrei). ▪ Hinweis: Nicht alle Formate können in PDF / A konvertiert werden (Bsp. CAD-Dateien, Filme, Tonaufzeichnungen, anwendungsspezifische Formate). Hier sollte weiter das Originalformat aufbewahrt werden. ▪ Hinweis: Ursprungsformate müssen (unter dem gleichen Index) zusätzlich aufbewahrt werden. Unter bestimmten Voraussetzungen bestehen hierzu Ausnahmen (vgl. auch Vorgaben zur Konvertierung in ↗ Kapitel 2.1 Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit).

2.2.2 Richtigkeit

a) Grundsatz

Geschäftsvorfälle sind in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften inhaltlich zutreffend durch Belege abzubilden.

b) DMS-Kontext

Dem Kontrollziel entsprechend 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 vor allem, dass bei der Erfassung von Daten und Dokumenten durch das DMS weder Belege verloren gehen noch verfälscht werden. Insbesondere muss auch die (manuelle oder automatische) Indexierung zuverlässig sein.

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

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(19)	Bildliche Übereinstimmung bei Eingangsdokumenten	▪ Vgl. ↗ Kapitel 4.2 Archivierung von Eingangsdokumenten und ↗ Kapitel 4.3 Bildliche Erfassung von Papierdokumenten.
(20)	Inhaltliche Übereinstimmung bei Ausgangsdokumenten	▪ Vgl. ↗ Kapitel 4.1 Archivierung von Ausgangsdokumenten.
(21)	Korrekte Erfassung der Belege	▪ Betrifft insbesondere die Eingangsschnittstellen eines DMS. ▪ Vgl. hierzu die Maßnahmen beim bildlichen Erfassen und bei der E-Mail-Erfassung in ↗ Kapitel 4 Ausgewählte Erfassungs- und Verarbeitungsprozesse im DMS.
(22)	Korrekte Erfassung der Dokumente und Indexdaten	▪ Implementierung eines übergreifenden Konzepts im Rahmen des IKS zur Sicherstellung der korrekten Erfassung (z. B. Regelwerk für die Indizierung von Dokumenten). ▪ Hinweis: Vgl. ↗ Kapitel 2.2.4 Ordnung.
(23)	Fehlerhandling	▪ Vorhandensein eines Regelprozesses bzw. Eskalationsverfahrens zur Beanstandung und Korrektur von fehlerhaften und unleserlich erfassten Belegen sowie fehlerhaften Dokumenten und Dateien. ▪ Vorhandensein eines Prozesses, wie (im Detail) mit den fehlerhaften Daten / Dokumenten umgegangen werden soll (z. B. Clearing-Stelle, Rescan, Protokollierung etc.).

2.2.3 Zeitgerechte Belegsicherung

a) Grundsatz und Kontrollziel

Belege sind zeitnah einer Belegsicherung zuzuführen und gegen Verlust zu sichern.

b) DMS-Kontext

Dem Kontrollziel entsprechend hat die Archivierung der Dokumente und Daten zum frühestmöglichen Zeitpunkt zu erfolgen, um mögliche Verluste oder 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 Dokumente und Daten möglichst zeitnah auf das endgültige Archivierungsmedium übertragen werden.

Generell ist diese Anforderung 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.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(24)	Belegsicherung	▪ Gewährleistung der Belegsicherung sowie Sicherung der aufgezeichneten Geschäftsvorfälle vor Verlust. ▪ Die Daten und Dokumente müssen unmittelbar nach Eingang gegen Verlust gesichert werden. ▪ Sicherstellung einer zeitnahen Überführung der Daten und Dokumente in das DMS, um mögliche Verluste und Manipulationen vor der Archivierung auszuschließen. ▪ Vorhandensein technischer und organisatorischer Maßnahmen, die gewährleisten, dass die Daten und Dokumente möglichst zeitnah auf das endgültige Archivierungsmedium übertragen werden. ▪ Vergabe einer fortlaufenden Nummerierung ein- und ausgehender Belege / Rechnungen sowie Übernahme dieser eindeutigen Belegnummer in die Aufzeichnungen. ▪ Hinweis: Vgl. auch ↗ Kapitel 2.2.4 Ordnung.
(25)	Automatische Übernahme aus Anwendungen	▪ Fachanwendung übergibt aktiv Daten in das DMS (»push«). ▪ DMS holt sich die Daten von der Fachanwendung (»pull«); dabei ggf. Zeitsteuerung durch Scripting, Batch-Lauf etc.
(26)	Zeitnahe Überführung von Daten und Dokumenten	▪ Die automatische Übernahme hat zeitnah zu erfolgen. ▪ Sofern keine automatische Übernahme erfolgt: Implementierung einer Arbeitsanweisung zur zeitnahen Überführung von Daten und Dokumenten.
(27)	Datumszuordnung	▪ Verwendung eines Datumsfeldes, aus dem der Archivierungszeitpunkt erkennbar ist (auch in Protokollen). Zeitzonen müssen ggf. berücksichtigt werden / erkennbar sein. ▪ Verwendung eines Datumsfeldes für das fachlich korrekte Datum (z. B. Beleg- oder Eingangsdatum).

2.2.4 Ordnung

a) Grundsatz und Kontrollziel

Geschäftsvorfälle sind systematisch, übersichtlich, eindeutig und identifizierbar festzuhalten.

b) DMS-Kontext

Dem Kontrollziel entsprechend ist die Einhaltung bestimmter Ordnungsmäßigkeitskriterien während der gesamten Aufbewahrungsfrist zu gewährleisten. Das DMS muss dabei eine ausreichende Indexstruktur vorweisen. Die Dokumente müssen mittels dieser Indexstruktur identifizierbar, recherchierbar und klassifizierbar sein.

Eine eindeutige Zuordnung zum jeweiligen Geschäftsvorfall muss möglich sein (vgl. auch retrograde und progressive Prüfbarkeit). Der Erhalt dieser Verknüpfung zwischen Geschäftsvorfall, Index und Dokument ist während der gesamten Aufbewahrungsfrist zu gewährleisten.

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

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(28)	Elektronische Ablagestrukturen	▪ Sicherstellung, dass jedem archivierten Dokument oder Datensatz eine eindeutige Dokument-Identifikation zugewiesen wird. ▪ Vergabe einer fortlaufenden Nummerierung ein- und ausgehender Belege sowie Übernahme dieser eindeutigen Belegnummer in die Aufzeichnungen. ▪ 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. ▪ Sicherstellung, dass zwei Dokumenten nicht die gleiche Dokument-Identifikation zugewiesen werden kann. ▪ Zwingende Einhaltung vorgegebener Ablagestrukturen. ▪ Keine individuellen Ablagestrukturen für steuerrelevante Daten und Dokumente.
(29)	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. Kalendersteuerelement statt Freitextfeld). ▪ Befüllung von Indexdaten aus vorhandenen Datenquellen (z. B. über Datenbank-Import). ▪ Einführung einer (manuellen) Qualitätssicherung (z. B. Vier-Augen-Prinzip). ▪ Nutzung der bereits bestehenden Daten in eingehenden Dokumenten (z. B. bei elektronischen Eingangsrechnungen im Format ZUGFeRD oder XRechnung sind etliche relevante Indexdaten, wie Rechnungsnummer, Rechnungsdatum etc., bereits im Dateiformat eingebettet und können durch geeignete Tools automatisch für die Indizierung übernommen werden).
(30)	Verknüpfung Buchung zu Beleg	▪ Implementierung einer nachvollziehbaren Verknüpfung / Navigation von der Buchung zum Beleg. Dies kann z. B. über eine technische Verknüpfung aus dem IT-Buchführungssystem und Doc-IDs im DMS erfolgen. ▪ Hinweis: Wenn Belege zu einem elektronischen Dokument zusammengefasst werden (z. B. im Rahmen einer Altbestandsübernahme) ist sicherzustellen, dass die einfache Identifikation der darin enthaltenen Einzeldokumente weiterhin möglich ist. Des Weiteren muss ersichtlich sein, welches Einzeldokument der Ursprungsbeleg ist (ursprünglicher Inhalt).
(31)	Definition der endgültigen Version / des finalen Dokumentes	▪ Wenn Dokumente versioniert werden, ist die Unterscheidung zwischen Arbeitsversionen und finalen Dokumentenversionen sicherzustellen (z. B. über eine Änderungshistorie mit Angaben zu Autor / Reviewer und Bearbeitungs- bzw. Freigabestatus). ▪ Es sollte eine eindeutige Definition geben, wann ein Objekt in einem DMS als archiviert gilt, d. h. den »Archiv-Status« erreicht hat.
(32)	Mehrfachablage	▪ Müssen Daten oder Dokumente mehrfach abgelegt werden (z. B. die Rechnungen zu einer Kundenakte werden zusätzlich als Buchungsbeleg abgelegt), sollten die damit verbundenen Regeln bei der Indizierung transparent sein. ▪ Im Falle einer Mehrfachablage ist zu definieren, welcher Beleg die Belegfunktion im Rahmen der Buchung übernimmt.
(33)	Konvertierungen	▪ Bei Konvertierungen sind die Ursprungsformate (unter dem gleichen Index) zusätzlich aufzubewahren. Unter bestimmten Voraussetzungen bestehen hierzu Ausnahmen. ▪ Hinweis: Vgl. auch Vorgaben zur Konvertierung in ↗ Kapitel 2.1 Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit und ↗ Kapitel 5.2 Konvertierung.
(34)	Löschfunktionen	▪ Löschvorgänge von nicht mehr relevanten Daten und Dokumenten müssen nachvollziehbar sein, sodass diese Daten oder Dokumente wiederhergestellt werden können. ▪ »Nachvollziehbar« ist bspw. ein Protokoll. ▪ »Wiederherstellbar« ist bspw. ein elektronischer Papierkorb. ▪ Hinweis: Vgl. auch ↗ Kapitel 2.2.1 Vollständigkeit und ↗ Kapitel 2.2.5 Unveränderbarkeit. ▪ Hinweis: Besonderheiten der Datenschutz-Grundverordnung (DS-GVO) sind ggf. zu beachten.

2.2.5 Unveränderbarkeit

a) Grundsatz und Kontrollziel

Informationen, die einmal in den Verarbeitungsprozess eingeführt werden, dürfen nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden, sodass deren ursprünglicher Inhalt nicht mehr feststellbar ist. Spätere Änderungen sind ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, erkennbar bleiben.

b) DMS-Kontext

Dem Kontrollziel entsprechend muss das System eine Protokollierung von Veränderungen und Löschungen von sowie an den Dokumenten und Aufzeichnungen ermöglichen. Es geht hierbei nicht um die unveränderbare Ablage. Änderungen sind zulässig, solange diese nachvollziehbar sind.

Die Unveränderbarkeit kann sowohl hardwaremäßig (z. B. unveränderbare und fälschungssichere Datenträger) als auch softwaremäßig (z. B. Sicherungen, Sperren, Festschreibung, Löschmerker, automatische Protokollierung, Historisierungen, Versionierungen) als auch organisatorisch (z. B. mittels Zugriffsberechtigungskonzepten) gewährleistet werden. Eine bloße Ablage im Dateisystem erfüllt die Anforderungen zur Unveränderbarkeit ohne zusätzliche Maßnahmen regelmäßig nicht.

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

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

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(35)	Unveränderbarkeit von Daten und Dokumenten	▪ Sicherstellung, dass Informationen, welche in den Verarbeitungsprozess Eingang gefunden haben, nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden können (etwa Vorhandensein einer Versionsverwaltung). ▪ Sicherstellen, dass Daten, Dokumente und deren Metadatenstrukturen nur nachvollziehbar verändert werden können. ▪ Protokollierung von Änderungsaktionen an Daten, Dokumenten und Systemeinstellungen sowie der beteiligten Personen (z. B. mittels Benutzerkennung oder Personalnummer). ▪ Hinweis: Dokumente in der Entwurfsphase bzw. im Entwurfsstatus können gelöscht und geändert, versioniert oder historisiert werden. ▪ Hinweis: Änderungen können auch grundsätzlich verboten werden.
(36)	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).
(37)	Technische Maßnahmen zur Unterstützung der Unveränderbarkeit	▪ Einsatz von technischen Sicherheitsmechanismen zur Kontrolle und Vermeidung von Änderungen (z. B. durch unveränderbare Speichermedien, Hashwerte, Signaturen). ▪ Einsatz von Speichersystemen, welche die Unveränderbarkeit auf technischer Ebene sicherstellen. In der Vergangenheit basierten diese Systeme im Regelfall auf optischen WORM-Medien. Mittlerweile werden hierzu festplattenbasierte Systeme mit Softwareschutz eingesetzt. ▪ Hinweis: 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).
(38)	Organisatorische Maßnahmen zur Unterstützung der Unveränderbarkeit	▪ Vorhandensein organisatorischer Regelungen (z. B. Vier-Augen-Prinzip, regelmäßige Audits, Zugangskontrollen, Arbeitsanweisungen zum Systembetrieb etc.).
(39)	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 bzw. separate Textnotizen / Notizfelder).
(40)	Dokumente mit elektronischen Signaturen	▪ Elektronische Signaturen dürfen nicht gebrochen werden.
(41)	Unveränderbarkeit bei administrativen Zugriffen	▪ Sicherstellung der Unveränderbarkeit / Nachvollziehbarkeit auch bei administrativem Zugriff (dies betrifft ebenso den Zugriff über das Betriebssystem). ▪ Hinweis: Dies ist in der Praxis oft nur eingeschränkt möglich und von den technischen Umsetzungsmöglichkeiten begrenzt. Ein Vier-Augen-Prinzip (z. B. geteiltes Admin-Passwort) kann dazu beitragen Risiken zu minimieren.
(42)	Löschen (wenn vorhanden)	▪ Der Prozess der Löschung (logisch) von Daten und Dokumenten muss nachvollziehbar sein. ▪ Der Prozess der Löschung (physikalische Löschung vor Archivierung) von Daten und Dokumenten muss nachvollziehbar sein. ▪ Der Prozess der Löschung (logisch) von Indizes muss nachvollziehbar sein. ▪ Hinweis: Besonderheiten der Datenschutz-Grundverordnung (DS-GVO) sind bei personenbezogenen Daten und Dokumenten zu beachten.

3 Anforderungen an den ordnungsmäßigen IT-Betrieb

3 Anforderungen an den ordnungsmäßigen IT-Betrieb

Ein verlässlicher, geregelter und nachvollziehbarer IT-Betrieb nebst korrespondierender IT General Controls (ITGC) 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:

- Internes Kontrollsystem (IKS) (vgl. ↗ **BMF GoBD-Kapitel 6**)
- Datensicherheit (vgl. ↗ **BMF GoBD-Kapitel 7**)
- Unveränderbarkeit, Protokollierung von Änderungen (vgl. ↗ **BMF 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 und Kontrollziel

Die GoBD fordern, dass der Steuerpflichtige sein IT-System gegen Verlust (z. B. Unauffindbarkeit, Vernichtung, Untergang sowie Diebstahl) zu sichern und gegen unberechtigte Eingaben und Veränderungen (Zugangs- und Zugriffskontrollen) zu schützen hat. Werden die Daten, Datensätze und elektronischen Dokumente nicht ausreichend geschützt und können daher nicht mehr vorgelegt werden, steht die Ordnungsmäßigkeit der Buchführung in Frage.

b) DMS-Kontext

Dem Kontrollziel entsprechend betreffen generelle Anforderungen an einen ordnungsgemäßen IT-Betrieb insbesondere den technischen Betrieb von Systemen gemäß den Betriebsvoraussetzungen und -bedingungen, die Datensicherung (Backup), die Restart- und Recovery-Fähigkeit oder das Krisen- und Notfallmanagement.

Dazu ist ein ordnungsgemäßer IT-Betrieb ergänzend durch organisatorische Maßnahmen wie Schulung der Mitarbeiter, Awareness-Kampagnen oder Arbeitsanweisungen für Systemadministration sicherzustellen.

Neben der Beachtung sowohl technischer als auch organisatorischer Aspekte ist für einen ordnungsmäßen IT-Betrieb schließlich auch die Dokumentation von Maßnahmen innerhalb von Betriebskonzepten oder Arbeits- und Verfahrensanweisungen, Regelungen zum Katastrophenfall (K-Fall) oder eine vollständige und ordnungsgemäße Verfahrensdokumentation von Relevanz.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(43)	Ordnungsmäßigkeit und Nachvollziehbarkeit der fachlichen Prozesse	▪ Definition und Beschreibung der steuerrelevanten fachbezogenen Prozesse. Diese Prozesse betreffen i. d. R. mehrere IT-Anwendungen und nicht isoliert das DMS. ▪ Die Gesamtprozesse sind so zu gestalten, dass die Anforderungen der GoBD erfüllt sind. ▪ Hinweis: Häufig werden diese übergreifenden Prozesse in einer Verfahrensdokumentation aufgeführt.
(44)	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. ▪ Hinweis: Häufig findet die Dokumentation dieser Prozesse in einer separaten IT-nahen Dokumentation, bspw. in einem Betriebskonzept, statt. Dies ist regelmäßig Bestandteil der Verfahrensdokumentation (zur Verfahrensdokumentation vgl. ausführlich ↗ Kapitel 6 Verfahrensdokumentation).
(45)	Definierter Leistungsumfang	▪ Vorhandensein einer vertraglichen Vereinbarung in Bezug auf die zwischen Leistungserbringer und Leistungsempfänger vereinbarte Dienstleistung (Service-Level-Agreement, kurz »SLA«). Wesentlicher Inhalt des SLA sind Umfang, Aktivitätensplit und Kontrollaufbau der konkreten Dienstleistungserbringung. ▪ Zur Dienstleistungssteuerung sind dabei regelmäßig Vorgaben zur Verfügbarkeit der Services, ein Eskalationsmanagement, vereinbarte Vertragslaufzeiten, Pönalevereinbarung und Key Perfomance Indicators (KPIs) schriftlich fixiert.
(46)	Kenngrößen DMS-Betrieb	▪ Definition und Ermittlung von Messgrößen (bspw. Verfügbarkeit der Anwendung). ▪ Definition, wie lange ein Geschäftsprozess / System vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse ausfallen darf (Recovery Time Objective, kurz »RTO«). ▪ Definition, wieviel Datenverlust in Kauf genommen werden darf und wie viele Daten / Transaktionen zwischen der letzten Sicherung und dem Systemausfall höchstens verloren gehen dürfen (Recovery Point Objective (kurz »RPO«). ▪ Hinweis: Bei einem DMS dürfte dies gegen Null gehen.
(47)	Kontrollrechte und Kontrollmaßnahmen	▪ Grundsätzlich sollte sich das outsourcende Unternehmen in Bezug auf die vereinbarte Dienstleistung / Service vertragliche Kontrollrechte bzgl. der Einhaltung von Ordnungsmäßigkeits- und Sicherheitsmaßnahmen vom Dienstleistungsunternehmen zusichern lassen. ▪ Ebenso sollten Prüfungs- und Auskunftsrechte (durch den Buchführungs- und Aufzeichnungspflichtigen selbst oder durch von diesem beauftragte Dritte) vereinbart werden. ▪ Regelungen über eine zeitnahe Verfügbarkeit von Daten und Verfahrensdokumentation beim Outsourcing-Geber sollten schriftlich fixiert werden. ▪ Vorhandensein vertraglicher Prüfungs- und Kontrollrechte, Berichterstattungen gemäß IDW PS 951 n.F. / ISAE 3402 oder vergleichbarer Berichterstattungen, um sich von der Angemessenheit und Wirksamkeit des IKS beim Dienstleistungsunternehmen zu überzeugen. ▪ Vorhandensein eines Prozesses, der die regelmäßige Überprüfung des dienstleistungsbezogenen IKS durch den Leistungsempfänger gewährleistet (bspw. jährliche Auswertung der Berichterstattung i. S. d. IDW PS 951 n.F.). ▪ Vorhandensein von Reports oder Berichterstattungen (bspw. monatlicher KPI-Report) über die Einhaltung der zugesicherten Eigenschaften der Dienstleistung. ▪ Existieren von regelmäßigen Prüfungen beim Dienstleistungsunternehmen durch unabhängige Dritte bzw. entsprechende Zertifizierungen.
(48)	Eskalationsverfahren	▪ Vorhandensein von Eskalationsverfahren mit den Dienstleistungsunternehmen bei nicht vertragsgemäßer Leistungserbringung (bspw. eingeschränkte Verfügbarkeit bzw. Schlechtleistung).

3.2 Rechenzentrum und Cloud Computing

a) Grundsatz und Kontrollziel

Der technische Betrieb der IT-Komponenten hat die Anforderungen der GoBD an die Verfügbarkeit und Vertraulichkeit sicherzustellen. Da die GoBD technikneutral sind, werden keine spezifischen technischen Vorgaben gemacht. Die gesetzlichen Ordnungsmäßigkeitsanforderungen einschließlich der Anforderungen der GoBD gelten uneingeschränkt auch für den Fall des IT-Outsourcings sowie den Betrieb von Cloud Lösungen.

Hinweis: Soweit rechnungslegungsrelevante Dienstleistungen ausgelagert werden, ist der IDW-Stellungnahme zur Rechnungslegung »Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing« (IDW RS 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.

b) DMS-Kontext

Dem Kontrollziel entsprechend unterliegen die DMS-Server-Komponenten i. d. R. den gleichen Sicherheitsanforderungen wie andere IT-Komponenten. Relevante Themen sind Überwachung, Datensicherheit und -sicherung, Verfügbarkeit, Datenschutz, Zugangs- und Zugriffsschutz, die Restart- und Recovery-Fähigkeit sowie das Krisen- und Notfallmanagement.

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.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(49)	Zertifizierungen	▪ Liegen einschlägige Zertifizierungen vor (u. a. ISO 27001, EN 50600 TüvIT, IDW PS 951 n.F., ISAE 3402)?
(50)	Physische Sicherungsmaßnahmen, Zutrittskontrollen	▪ Schaffung gebäudetechnischer Voraussetzungen und Maßnahmen (z. B. Aufstellung der DMS-Server in einem separaten Rechenzentrum mit Klimaanlage, Alarmanlage, Notstromversorgung, besonderen Brandschutzvorrichtungen etc.). ▪ Kein unberechtigter Zutritt zu Räumen, in denen IT-Anwendungen bedient oder Daten aufbewahrt werden. Der Zutritt ist ausschließlich berechtigten Personen gestattet. Dritten (bspw. Fremdfirmen zu Wartungszwecken) wird der Zutritt nur in Begleitung gewährt. ▪ Restriktiv gestaltete Zutrittsregelung zum Rechenzentrum / Rechnerraum (u. a. 2-Faktor-Authentifizierung). ▪ Es erfolgt eine Protokollierung des Zutritts.

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(51)	Logische Sicherungsmaßnahmen und Zugriffsschutz	▪ Ausschließlich autorisierten Anwendern wird das Recht eingeräumt, einen Service zu nutzen. ▪ Der Zugriff für unautorisierte Anwender wird unterbunden.
(52)	Datensicherung, Backup & Recovery	▪ Implementierung eines übergreifenden Backup-Konzepts für alle IT-Anwendungen (einschließlich DMS). Das Konzept beschreibt Verantwortlichkeiten und Prozeduren (z. B. welche Datenbestände wann zu sichern sind). ▪ Einführung / Durchführung regelmäßiger Testings, die das ordnungsgemäße Zurückladen der Backup-Daten sicherstellen (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. ▪ Hinweis: In aktuellen IT-Anwendungen werden die relevanten Daten meist auf einem Server gespeichert, sodass sich ein Backup für Arbeitsplatzrechner erübrigt. ▪ Hinweis: Für DMS teilweise Verwendung spezieller Wechselmedien oder Storage-Subsysteme, für die ggf. spezielle Backup-Maßnahmen erforderlich sein können.
(53)	Monitoring	▪ Einsatz von Überwachungs- bzw. Monitoringtools zur laufenden Überwachung der kritischen IT-Infrastruktur-Komponenten wie Anwendungen, Dienste, Betriebssysteme, Netzwerke, Server, Datenbanken und Virtualisierung. ▪ Die verantwortlichen Mitarbeiter werden regelmäßig in diesen Monitoringtools geschult.
(54)	Verfügbarkeit und Betriebsbereitschaft	▪ 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.
(55)	Notfallmanagement, geordneter Wiederanlauf	▪ Vorhandensein von Maßnahmen für den Notbetrieb zur Wiederherstellung der IT nach teilweisem oder vollständigem Ausfall der IT-Infrastruktur im Katastrophen- und Schadensfall. ▪ Vorhandensein eines IT-Notfallhandbuchs, in dem insbesondere entsprechende Verantwortlichkeiten und Entscheidungswege schriftlich fixiert sind. ▪ Vorhandensein eines Notfallplans (Disaster Recovery Plan) für Restart und Recovery für den Fall, dass einzelne Komponenten oder das ganze System ausfallen. ▪ Vorhandensein eines »Restart«-Prozederes (Wiederanlauf des DMS nach einer Betriebsstörung. 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.
(56)	K-Fall-Abdeckung	▪ Implementierung / Vorhalten von Reservesystemen, hoch verfügbaren Systemauslegungen (z. B. Fail-Over-Cluster, ggf. an einem anderen Standort). ▪ Hinweis: Spannbreite reicht von »Reservesystemen für einzelne Komponenten« bis hin zu (geo-)redundant ausgelegten Rechenzentren (»Spiegel-Rechenzentren«).
(57)	Geordnetes Test- und Freigabeverfahren, Change-Management	▪ Durchführung geeigneter Tests vor der Freigabe eines neuen Verfahrens / Prozesses. ▪ Vorhandensein von Regeln und Testvorgaben für Änderungen an bestehenden Verfahren. Die Ausgestaltung der Tests ist vom jeweiligen Prozess abhängig. ▪ Hinweis: Klar definierte Rollen / Verantwortlichkeiten (Entwickler, Tester, Freigeber etc.) sind unabdingbar. ▪ Vorhandensein von Maßnahmen welche den Lebenszyklus aller Veränderungen steuern.
(58)	Service und Support	▪ Vorhandensein von Wartungs- und Supportverträgen mit Lieferanten für die eingesetzten Komponenten und die Rechenzentrums-Infrastruktur. ▪ Vorhandensein von Verantwortlichkeiten für die Einschaltung des externen Supports (z. B. Rollen, Eskalationsprozesse etc.).

3.3 Betriebsbedingungen und Wartung

a) Grundsatz und Kontrollziel

Die Hersteller von Hard- und Softwarekomponenten definieren für ihre Produkte eine Umgebung, die sowohl getestet als auch für das jeweilige Produkt freigegeben ist. Für einen sicheren IT-Betrieb ist es erforderlich, dass diese Bedingungen eingehalten werden und die Hard- und Software gemäß den Herstellervorgaben implementiert ist. Dies gilt auch für die Wartungs- und Update-Regelungen.

b) DMS-Kontext

Da sich für den DMS-Einsatz keine speziellen Aspekte ergeben, sind für das Kontrollziel die allgemeinen Grundsätze heranzuziehen.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(59)	Betriebsbedingungen Hardware	▪ Einhaltung der Betriebsbedingungen für Hardware (z. B. durch Klimatisierung von Räumen, Feuchtigkeitsmessgeräte, Staubfilter, maximale Leitungslängen bei Netzwerken etc.). ▪ Die Einhaltung der Betriebsbedingungen sollte bei der Freigabe der Hardware sowie bspw. bei baulichen Veränderungen überprüft werden.
(60)	Hardware-Wartung	▪ Hardware-Wartung erfolgt nach definierten Wartungsplänen gemäß den Empfehlungen der Hersteller. ▪ Hinweis: 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 stets vom Einzelfall ab und sollte systemübergreifend für alle IT-Anwendungen erfolgen. Entscheidend ist, dass das Konzept die gewünschte Verfügbarkeit gewährleistet.
(61)	Zuverlässigkeit der Hardware	▪ Einrichtung von Zuständigkeiten und Regeln für Austausch und Update von Hardware. Insbesondere sollte nur Hardware verwendet werden, für die noch Wartung / Support verfügbar ist. ▪ Hinweis: I. d. R. wird die Nutzungsdauer von Hardware von Beginn an so geplant, dass die Wahrscheinlichkeit von Störungen während der Nutzungsdauer gering ist. Entsprechende Hardwarereserven werden zudem vorgehalten (bspw. Hot-Spare-Festplatten).
(62)	Betriebsbedingungen Software	▪ Für die Einhaltung der Betriebsbedingungen von Software sind insbesondere die Freigaben der Hersteller für bestimmte Betriebssysteme, Datenbanken etc. zu beachten. ▪ Die Einhaltung der Betriebsbedingungen sollte bei der Freigabe von Softwarekomponenten und Updates sowie bei Veränderungen in der Systemumgebung überprüft werden.
(63)	Software-Wartung	▪ Definition von Zuständigkeiten und Regeln, ob und wann Updates und Produktreleases eingespielt werden (Freigabeverfahren). ▪ Hinweis: Soweit einschlägig, restriktive Ausgestaltung von Remotezugriffen durch Wartungsmitarbeiter (u. a. eindeutige Benutzerkennung, autom. Time-Out, Wartungsfenster, Zugriffsprotokollierung etc.).
(64)	Wartungs-Dokumentation	▪ Protokollierung von Wartungsmaßnahmen, Austausch von Hardware sowie Einspielen von Updates und neuen Releases.

3.4 Problembehebung und Support

a) Grundsatz und Kontrollziel

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. Entsprechend ist eine zeitnahe und vollständige Wiederherstellung der Systeme und Daten bei Störungen und Ausfällen zu gewährleisten.

b) DMS-Kontext

Da sich für den DMS-Einsatz keine speziellen Aspekte ergeben, sind für das Kontrollziel die allgemeinen Grundsätze heranzuziehen.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(65)	Incident-Management	▪ Vorhandensein eines organisatorisch und technisch implementierten Prozesses für die Erfassung, Bearbeitung und Verfolgung von IT-Störungen bzw. Problemen sowie IT-Sicherheitsvorfällen. Dies umfasst auch vorbereitende Maßnahmen und Prozesse. (Vollständige Erfassung von Incidents (Ticketsystem, telefonisch, E-Mail etc.), Priorisierung einzelner Incidents, Eskalationsverfahren etc.). ▪ Hinweis: Sicherheitsrelevante Vorfälle sind von klassischen IT-Störungen eindeutig abzugrenzen und bedürfen einer separaten / besonderen (priorisierten) Abarbeitung in angemessener Zeit.
(66)	Problem-Management	▪ Unbekannte Ursachen für tatsächliche und potenzielle Störungen (Incidents) innerhalb der IT-Services werden untersucht und die Behebung gesteuert.
(67)	Helpdesk	▪ Einrichtung eines technischen IT-Helpdesks für Fachbenutzer. Bei Störungen der technischen Infrastruktur (z. B. Rechner startet nicht, Netzwerk nicht verfügbar, Passwort abgelaufen etc.) müssen für Endbenutzer Ansprechpartner verfügbar sein. ▪ Hinweis: Der IT-Helpdesk berät, kann kleinere Probleme selbst lösen und ggf. den externen Support einschalten.
(68)	2nd-Level-Support	▪ Gegebenenfalls Einrichtung eines speziellen Helpdesks für Probleme mit dem DMS, das nicht mit dem allgemeinen IT-Helpdesk identisch ist. ▪ Gegebenenfalls können auch »Power-User« als erste Anlaufstelle fungieren.
(69)	3rd-Level-Support / Problembehebung durch den Hersteller (Hardware)	▪ Abschluss von Wartungs- und Supportverträgen mit den Hardwarelieferanten, die insbesondere garantierte Service- und Reaktionszeiten regeln. ▪ Definition von Verantwortlichkeiten für die Einschaltung des externen Supports (Rollen, Eskalationsprozesse etc.). ▪ Hinweis: Wissenstransfer durch enge Verknüpfung des 2nd- und 3rd-Level-Supports (Einrichtung entsprechender Verfahrens- und Kommunikationswege).
(70)	3rd-Level-Support / Problembehebung durch den Hersteller (Hardware)	▪ Abschluss von Wartungs- und Supportverträgen mit den Softwarelieferanten, die garantierte Service- und Reaktionszeiten (»Produktsupport«) regeln. ▪ Gegebenenfalls Abschluss von Verträgen zum installationsspezifischen Support mit dem Systemintegrator (»Projektsupport«). ▪ Definition von Verantwortlichkeiten für die Einschaltung des externen Supports (Rollen, Eskalationsprozesse etc.). ▪ Hinweis: Wissenstransfer durch enge Verknüpfung des 2nd- und 3rd-Level-Supports (Einrichtung entsprechender Verfahrens- und Kommunikationswege).

3.5 Berechtigungssystem

a) Grundsatz und Kontrollziel

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

b) DMS-Kontext

Dem Kontrollziel entsprechend bedarf es der Etablierung eines differenzierten Berechtigungssystems, das den lesenden und schreibenden Zugriff für einzelne Benutzer oder Benutzergruppen auf bestimmte Daten erlaubt bzw. verbietet. Vor allem sind durch das Berechtigungssystem nicht autorisierte 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.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(71)	Berechtigungskonzept	▪ Erstellung eines übergreifenden Berechtigungskonzepts, ggf. auch für andere IT-Anwendungen außerhalb des DMS. Das Konzept sollte generelle Regeln enthalten, aus denen die jeweilige Berechtigung im Einzelfall abgeleitet werden kann. ▪ Eine getrennte Benutzerverwaltung nur für das DMS ist i. d. R. nicht zu empfehlen. ▪ Hinweis: Zugriffsberechtigungen spielen gerade beim Schutz personenbezogener Daten (Datenschutz, DS-GVO) eine wichtige Rolle. Es empfiehlt sich ein gemeinsames Konzept, in dem sowohl die Belange der GoBD als auch die des Datenschutzes Berücksichtigung finden.
(72)	Funktionstrennung	▪ Bei einer Funktionstrennung ist darauf zu achten, dass Prozesse bezüglich eines DMS grundsätzlich eine starke Einbindung von IT-Mitarbeitern mit sich bringen. ▪ Die Funktionstrennung ist insbesondere im kaufmännischen Umfeld, im technischen Umfeld (Administration) sowie bei kritischen Überschneidungen beider Bereiche strikt zu beachten. Vor allem im Hinblick auf die Vertraulichkeit geraten IT-Projektmitarbeiter gerne in Vergessenheit. ▪ Hinweis: Es empfiehlt sich der Aufbau einer Funktionstrennungsmatrix (Segregation of duties), die einer regelmäßigen Überprüfung / Aktualisierung unterliegt.
(73)	Berechtigungen	▪ Die Benutzer sind im Berechtigungssystem des DMS zu hinterlegen. Dabei empfiehlt sich eine rollenbezogene Benutzerverwaltung (vgl. auch ↗ Kapitel 3.6 Mitarbeiter). ▪ Die Rollen sollten nach fachlichen Kriterien (Buchhalter, Scan-Operator etc.) definiert werden und kompatibel zu den Rollenbeschreibungen sowie den damit verbundenen Prozessen 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 in der übergreifenden Benutzerverwaltung ggf. weitere Rollen (z. B. »DMS-Administrator«) definiert werden.

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(74)	Berechtigungsstrukturen	▪ 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. Vier-Augen-Prinzip).
(75)	Zugriffsrechte im DMS	▪ Berechtigungen können auf verschiedenen Ebenen vergeben werden, von ganzen Dokumentbereichen (z. B. »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 (z. B. »darf nur auf Akte zugreifen, wenn Feld Gehalt < 5.000 €«). ▪ Hinweis: Bei sehr differenziert definierten Berechtigungen steigt der Administrationsaufwand während zugleich die Transparenz sinkt. Hier sollten Kosten und Nutzen stets sinnvoll abgewogen werden.
(76)	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 Dokumententreffer, von denen aber 3 Dokumente nicht eingesehen werden dürfen. Durch geschickte Suchabfragen kann eine unbefugte Person dann in bestimmten Fällen dennoch unberechtigt Informationen erhalten, auch ohne die Dokumente einzusehen (z. B. »suche alle Personalakten von Mitarbeitern, deren Feld Gehalt > 5.000 € ist« etc.). Im obigen Beispiel muss die Trefferliste insoweit nur 7 statt 10 Treffer anzeigen.
(77)	Zugangskontrollen	▪ 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. ▪ Hinweis: In der Praxis wird häufig das sog. »Single Sign-on« (kurz »SSO«) verwendet, d. h. der Benutzer meldet sich beim Start seines Rechners einmalig unternehmensweit an und kann dann alle Fachsysteme (wie z. B. das DMS), die über eine SSO-Anbindung verfügen, ohne nochmalige Anmeldung nutzen. Hierbei kann ein zeitnaher Berechtigungsentzug bei den Fachsystemen bereits über die Sperrung des Benutzer-accounts, der zur Anmeldung via SSO dient, erfolgen.
(78)	Speicherung und Übermittlung von Passwörtern	▪ Vorhandensein von Maßnahmen zur softwareseitigen Umsetzung der Berechtigungsprüfung. ▪ Vorhandensein von Maßnahmen zur verschlüsselten Speicherung von Passwörtern. ▪ Vorhandensein von Maßnahmen zur gesicherten Verwendung von Private Keys.
(79)	Protokollierung von Berechtigungsänderungen	▪ Zur Einrichtung und Änderung von Berechtigungen sind wiederum besondere (administrative) Rechte erforderlich. ▪ Derartige Änderungen bzw. Zugriffe von Administratoren sollten protokolliert und über die jeweils gültigen Aufbewahrungsfristen zur Auswertung vorgehalten werden.
(80)	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 Mandanten bei der Archivierung möglich sein.

3.6 Mitarbeiter

a) Grundsatz und Kontrollziel

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

b) DMS-Kontext

Da sich für den DMS-Einsatz keine speziellen Aspekte ergeben, sind für das Kontrollziel die allgemeinen Grundsätze heranzuziehen.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(81)	Allgemeines 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. ▪ Hinweis: Neben regelmäßigen »Awareness-Kampagnen« bieten sich Online- und Präsenzschulungen an.
(82)	Rollen beim DMS-Betrieb	▪ Rollen für die DMS-Benutzung sind z. B. Sachbearbeiter, Erfassungskräfte, Scan-Operatoren, Indizierer, Lesezugriffsberechtigte 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 Fach- oder Personalabteilung.
(83)	Definierte Aufgaben und Zuständigkeiten	▪ Die Definition der entsprechenden Rollen umfasst die Beschreibung der jeweiligen Aufgaben. ▪ Für die Aufgaben können bei Bedarf Arbeitsanweisungen (Teil der Verfahrensdokumentation) formuliert werden; dies empfiehlt sich vor allem für komplexe und / oder sicherheitsrelevante Aufgaben. Die notwendigen Qualifikationen der Mitarbeiter ergeben sich aus der vorgesehenen Tätigkeit. ▪ Definierte Verantwortlichkeiten für die Auswahl und Qualifikation der Mitarbeiter.
(84)	Eignung der Mitarbeiter	▪ Bei der Besetzung der Rollen ist auf die Verlässlichkeit und fachliche Eignung der Mitarbeiter zu achten. Dies gilt insbesondere für administrative Rollen.
(85)	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. ▪ Hinweis: Eine stets aktuell gehaltene Anwenderdokumentation, die auch Teil der ordnungsgemäßen Verfahrensdokumentation darstellt, ist für den Mitarbeiter unabdingbar (zur Verfahrensdokumentation vgl. ausführlich ↗Kapitel 6 Verfahrensdokumentation). Die Qualifizierung des Anwenders muss ggf. durch regelmäßige Schulungsmaßnahmen sichergestellt werden.
(86)	Qualifizierung der Administratoren	▪ Einweisungs- und Schulungsmaßnahmen für Administratoren (z. B. Einweisung durch den Systemintegrator oder durch Kurse beim Hersteller der DMS-Software). ▪ Hinweis: Die Qualifizierung des Administrators muss ggf. durch regelmäßige Schulungsmaßnahmen sichergestellt werden.
(87)	Dokumentation	▪ Dokumentation der vorhandenen Qualifikationen (z. B. Berufsausbildung) und der zusätzlichen Qualifikationsmaßnahmen.

4 Ausgewählte Erfassungs- und Verarbeitungsprozesse im DMS

4 Ausgewählte 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:

- Archivierung von Ausgangsdokumenten
- Archivierung von Eingangsdokumenten
- Bildliche Erfassung von Papierdokumenten
- 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 Archivierung von Ausgangsdokumenten

a) Grundsatz und Kontrollziel

Die in ↗ Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze besitzen auch für Ausgangsdokumente ihre Gültigkeit. Entsprechend wird im Folgenden auf ausgewählte Besonderheiten eingegangen. Im Kern geht es dabei um die Sicherstellung der Verfügbarkeit aufbewahrungspflichtiger Ausgangsdokumente über die Dauer der gesetzlichen Aufbewahrungsfrist.

b) DMS-Kontext

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

Soweit es sich um Archivierungsszenarien handelt, bei denen die inhaltlichen Informationen eines Ausgangsdokuments in einem DMS aufbewahrt werden, muss das DMS die Ordnungsmäßigkeit der Daten sicherstellen. Die Nutzung historisierter Stammdaten ist jedoch nicht trivial, sodass es sich in der Praxis häufig empfiehlt, die entsprechenden Ausgangsbelege zum Zeitpunkt der Erstellung in einem Bildformat (z. B. PDF- oder TIFF-Datei) der Aufbewahrung zuzuführen. Entsprechend zugeführte Dokumente besitzen somit keine Abhängigkeiten zu anderen Datenbeständen oder Ressourcen-Dateien.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(88)	Inhaltliche Übereinstimmung bei Lesbarmachung	▪ Im Rahmen der inhaltlichen Übereinstimmung ist eine Reproduzierbarkeit der aufbewahrungspflichtigen Inhalte sicherzustellen. ▪ Es ist sicherzustellen, dass alle erforderlichen Stamm- und Bewegungsdaten sowie Verlinkungen / Verknüpfungen und ggf. historische Daten berücksichtigt werden. Hierbei ist insbesondere auf deren korrekte Versionierung zu achten, um die Daten und Dokumente mit ihrem historischen Inhalt lesbar machen zu können. ▪ 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. ▪ Soweit bei standardisierten Belegen wiederkehrende Informationen (z. B. Briefkopf) ausgefiltert (sog. Netto-Imaging) werden, muss sichergestellt sein, dass das Netto-Image zum Zeitpunkt der Wiedergabe mit den ausgefilterten Informationen kombiniert werden kann. ▪ 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. ▪ Wenn im Original der ausgehenden Handels- und Geschäftsbriefe Allgemeine Geschäftsbedingungen oder andere relevante Texte (es geht nicht um Werbung) mitgeliefert werden, sind diese ebenfalls historisiert vorzuhalten. Gegebenenfalls genügt ein Verweis und sie müssen jederzeit verfügbar sein. ▪ Soweit eine Reproduzierbarkeit fraglich erscheint, empfiehlt sich die entsprechenden Ausgangsbelege zum Zeitpunkt der Erstellung in einem Bildformat (z. B. PDF- oder TIFF-Datei) zu erstellen und elektronisch aufzubewahren.
(89)	Verfügbarkeit, Lesbarkeit und maschinelle Auswertbarkeit	▪ Es ist sicherzustellen, dass die Daten während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können. (D. h. neben den aufbewahrungspflichtigen Unterlagen ist u. U. auch die notwendige Infrastruktur [bspw. bestehend aus Soft- und Hardwarekomponenten] für die maschinelle Auswertbarkeit vorzuhalten.)

4.2 Archivierung von Eingangsdokumenten

a) Grundsatz und Kontrollziel

Die in ↗ Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze besitzen auch für Eingangsdokumente ihre Gültigkeit. Entsprechend wird im Folgenden auf ausgewählte Besonderheiten eingegangen. Im Kern geht es dabei um die Sicherstellung der Verfügbarkeit aufbewahrungspflichtiger Eingangsdokumente über die Dauer der gesetzlichen Aufbewahrungsfrist.

b) DMS-Kontext

Dem Kontrollziel entsprechend muss die Wiedergabe mit dem Original bildlich übereinstimmen, wenn diese lesbar gemacht wird. Soweit es sich um reine Datenformate handelt, ist ergänzend sicherzustellen, dass Rechnungen in Formaten wie beispielsweise XML oder EDIFACT für das prüferische Auge lesbar dargestellt werden können und damit auch prüfbar im Rahmen einer Sichtprüfung sind. Dem steuerpflichtigen Unternehmen ist insoweit zu empfehlen, zusammen mit der Rechnung auch ein geeignetes Anzeigeprogramm (XML-Viewer, Texteditor usw.) vorzuhalten.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(90)	Bildliche Übereinstimmung bei Lesbarmachung	▪ Die Wiedergabe muss mit dem Original bildlich übereinstimmen, wenn diese lesbar gemacht wird. ▪ Das Dokument muss für eine Sichtprüfung, etwa zur Prüfung der Pflichtbestandteile einer Rechnung, zugänglich sein.
(91)	Verfügbarkeit, Lesbarkeit und maschinelle Auswertbarkeit	▪ Sicherstellung, dass die Wiedergabe während der Dauer der Aufbewahrungsfrist jederzeit verfügbar ist, unverzüglich lesbar gemacht und maschinell ausgewertet werden kann. D. h. neben den aufbewahrungspflichtigen Unterlagen ist u. U. auch die notwendige Infrastruktur (bspw. bestehend aus Soft- und Hardwarekomponenten) für die maschinelle Auswertbarkeit vorzuhalten.
(92)	Konvertierung	▪ Soweit eine Konvertierung in ein unternehmenseigenes Format (sog. Inhouse-Format) erfolgt, sind stets beide Versionen aufzubewahren, derselben Aufzeichnung zuzuordnen und mit demselben Index zu verwalten. Unter bestimmten Voraussetzungen bestehen hierzu Ausnahmen. ▪ Hinweis: Vgl. ↗ Kapitel 2.1 Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit und ↗ Kapitel 5.2 Konvertierung.
(93)	Sonderfall Rechnungen	▪ Einrichtung und Dokumentation einer Rechnungseingangsprüfung (innerbetriebliches Kontrollverfahren mit Prüfpfad). ▪ Dies betrifft insbesondere die Prüfung der Pflichtangaben nach § 14 Abs. 4 UStG. ▪ Soweit Rechnungen in einem strukturierten elektronischen Format (EDI, XML, XRechnung etc.) eingehen, ist sicherzustellen, dass die Lesbarkeit über die Dauer der Aufbewahrungsfrist durch entsprechende Anzeigeprogramme ermöglicht wird. ▪ Vgl. ausführlich ↗ Kapitel 4.5. Archivierung von Rechnungen.

4.3 Bildliche Erfassung von Papierdokumenten

a) Grundsatz und Kontrollziel

Die in ↗ Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze besitzen auch für bildlich erfasste (»gescannte« / »fotografierte«) Papierdokumente ihre Gültigkeit. Im Kern geht es dabei um die Sicherstellung der Vollständigkeit, Nachvollziehbarkeit, Nachprüfbarkeit, bildlichen Übereinstimmung und Lesbarkeit bei der Umwandlung von Papierdokumenten in elektronische Dokumente (auch »Digitalisat« genannt).

Dabei gilt entsprechend der Neufassung der GoBD vom 28. November 2019, dass die Erfassung mit den verschiedensten Arten von Geräten wie z. B. Smartphones, Multifunktionsgeräten oder Scan-Straßen erfolgen kann.

Weiter gestattet die Neufassung unter bestimmten Voraussetzungen (vgl. ↗ Kapitel 5.4 Outsourcing / Auslagerung von DMS-Funktionen) auch das Verbringen von Papierbelegen ins Ausland mit anschließender bildlicher Erfassung.

b) DMS-Kontext

Werden Handels- oder Geschäftsbriefe und Buchungsbelege in Papierform empfangen und danach elektronisch erfasst (Scannen / Fotografieren), ist das Digitalisat 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. Für die Prüfung der Nachvollziehbarkeit und Nachprüfbarkeit ist nach den GoBD eine aussagekräftige, vollständige und aktuelle Verfahrensdokumentation erforderlich (vgl. ↗ Kapitel 6 Verfahrensdokumentation). Insbesondere muss sich daraus ergeben, wie die in den GoBD dokumentierten Ordnungsvorschriften bzw. Anforderungen beachtet werden. Nach dem bildlichen Erfassen dürfen Papierdokumente unter bestimmten Voraussetzungen (insbesondere Einhaltung der Vorgaben entsprechend §§ 145 bis 147 AO) vernichtet werden, soweit sie nicht nach außersteuerlichen oder steuerlichen Vorschriften im Original aufzubewahren sind. Im Zusammenhang mit der Vernichtung von Originalbelegen bedarf es insbesondere einer Organisationsanweisung.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten – bildliche Erfassung allgemein

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(94)	Prozess allgemein	▪ Soweit analoge Dokumente in ein digitales Format überführt werden, bedarf es insbesondere entsprechender Organisationsanweisungen, die festlegen, welche Dokumente bildlich erfasst (gescannt / fotografiert) werden und wie eine Kontrolle auf Vollständigkeit, Qualität und Lesbarkeit sichergestellt wird.
(95)	Bildliche Erfassung der Papierdokumente	▪ Maßnahmen zur Nutzung von ausreichenden Scan- bzw. Fotografier-Einstellungen (Farbe, DPI, Kontrast etc.). ▪ Einsatz von Software zur Verbesserung der Lesbarkeit. ▪ Sicherstellung der korrekten Dokumententrennung bei Stapelerfassung. ▪ Sicherstellung der korrekten Dokumententrennung beim mobilen Scannen. ▪ Vermeidung von Doppelerfassungen (organisatorisch sowie technisch durch bspw. das Erfassungsgerät). ▪ Maßnahmen zur Qualitätssicherung (organisatorisch sowie technisch durch bspw. entsprechende Software).
(96)	Vollständigkeit	▪ Jedes Dokument ist grundsätzlich einzeln und mit allen Bestandteilen bildlich zu erfassen. ▪ Gegebenenfalls ist eine Rückseitenerfassung vorzunehmen. ▪ Ausschluss von Dubletten durch Doppeleinzugs- bzw. Doppelerfassungs-Kontrolle (sog. Dubletten-Prüfung). ▪ Durchführung einer Vollständigkeitsprüfung durch Zählen der Seiten. ▪ Automatisierte Kennzeichnung bereits erfasster Dokumente durch das Erfassungsgerät (Indossierung / Imprinter). ▪ Hinweis: Allgemeine Geschäftsbedingungen (AGB) sind zu erfassen, sofern nicht durch organisatorische Maßnahmen sichergestellt wird, dass die jeweils gültigen AGB den einzelnen Dokumenten zugeordnet werden können.
(97)	Lesbarkeit, bildliche Wiedergabe	▪ Sicherstellung der originalgetreuen Übertragung des Abbilds auf das Speichersystem. ▪ Sicherstellung der originalgetreuen Übertragung ins Unternehmen (mobile und dezentrale bildliche Erfassung). ▪ Wiedergabe aller auf der Originalunterlage enthaltenen Angaben zur Aussage- und Beweiskraft des jeweiligen Geschäftsvorfalls. ▪ Sicherstellung einer lesbaren bildlichen Wiedergabe.
(98)	Farberfassung	▪ Soweit der Farbe in einem Dokument eine Beweisfunktion zukommt (z. B. Minusbeträge in rot), müssen diese Dokumente zwingend in Farbe erfasst werden.
(99)	OCR-Verarbeitung	▪ Werden bildlich erfasste Dokumente per OCR-Verfahren um Volltextinformationen angereichert (z. B. volltext-recherchierbares PDF-Format), so ist dieser Volltext nach Verifikation sowie Korrektur über die Dauer der Aufbewahrungsfrist ergänzend aufzubewahren und für Prüfzwecke verfügbar zu machen.
(100)	Verfahrensdokumentation	▪ Vorhandensein einer aussagekräftigen und vollständigen Verfahrensdokumentation (zur Verfahrensdokumentation vgl. ausführlich ↗ Kapitel 6 Verfahrensdokumentation) zzgl. entsprechender Arbeitsanweisungen (vgl. nachfolgende Ausführung).
(101)	Vorbereitung (Arbeitsanweisung)	▪ Bei dem Prozess der Arbeitsvorbereitung geht es für die bildliche Erfassung im Wesentlichen darum, bei der Vorbereitung den richtigen Zusammenhang und die Vollständigkeit sicherzustellen, insbesondere bei Tätigkeiten, wie des Entklammern gehefteter Dokumente, dem Öffnen der Eingangspost sowie dem Auflösen von Ordnern, für die aufgebrachten Post-its etc. Umgang mit Sonderformaten oder geösten / gebundenen Dokumenten. ▪ Die Arbeitsvorbereitung beim Import von bildlich erfassten Dateien beinhaltet eine Kontrollfunktion, welche sicherstellt, dass die richtigen Dateien in die entsprechenden Übergabeverzeichnisse eingestellt werden.
(102)	Nachbereitung (Arbeitsanweisung)	▪ Die Arbeitsnachbereitung beim bildlichen Erfassen beinhaltet das Aussortieren von Originalen, die in Papierform aufbewahrt werden müssen, die Vernichtung von nicht aufbewahrungspflichtigem oder -würdigem Material, die Vollständigkeitskontrolle der Erfassung etc. ▪ Die Arbeitsnachbereitung beinhaltet zudem die Kontrolle, inwieweit die temporären Verarbeitungsdateien ordnungsgemäß verarbeitet und anschließend gelöscht worden sind.

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(103)	Bildliche Erfassung (Arbeitsanweisung)	▪ Die Arbeitsanweisung hat zu beschreiben: Wer darf, zu welchem Zeitpunkt, was bzw. welches Schriftgut erfassen? ▪ Festlegung, zu welchem Zeitpunkt Scanprofile oder Scanner- bzw. Erfassungsgeräte-Einstellungen genutzt werden sollen. ▪ In jedem Fall sind sowohl die Bildqualität als auch die korrekte und vollständige Erfassung der Dokumente regelmäßig zu prüfen. ▪ Protokollierung und Eskalation von Fehlern während des Erfassungs-Prozesses. ▪ Hinweis: Die vorgenannten Ausführungen gelten für das bildliche Erfassen einzelner Dokumente und für Stapel-Erfassung gleichermaßen.
(104)	Qualitätssicherung (Arbeitsanweisung)	▪ 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 bildlichen Erfassung von 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 sind Regelungen zu bspw. einem Vier-Augen-Prinzip für Stichprobenprüfungen von Dokumenten und Indexdaten zu implementieren.
(105)	OCR	▪ Im Rahmen von OCR gewonnene Volltextinformationen sind aufzubewahren.
(106)	Weiterbearbeitung der Papierbelege nach der bildlichen Erfassung	▪ Erfolgt im Rahmen des frühen Archivierens eine Weiterbearbeitung der Papierbelege nach der bildlichen Erfassung, sind diese Papierbelege erneut zu erfassen und mit den Ursprungsdokumenten zu verknüpfen (gemeinsamer Index).
(107)	Maschinelle Auswertbarkeit	▪ Im Falle des bildlichen Erfassens von Papierbelegen und der korrespondierenden elektronischen Belegarchivierung muss der Steuerpflichtige im Rahmen einer steuerlichen Außenprüfung auf die entsprechenden Digitalisate über die betriebsinterne Hard- und Software die Einsicht in die elektronischen Belege unmittelbar am Bildschirm gestatten. ▪ Im Rahmen der Datenträgerüberlassung sind Dokumente und Unterlagen elektronisch zur Verfügung zu stellen. ▪ Hinweis: Zu Details vgl. ↗ Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff.
(108)	Vernichtung von Papierdokumenten	▪ Definition von Regelungen, wann und wie welche Papierdokumente nach dem bildlichen Erfassen vernichtet werden. ▪ Definition von Regelungen für Papierdokumente, die weiterhin im Papieroriginal aufzubewahren sind.
(109)	Bildliche Erfassung im Ausland	▪ Im Zusammenhang mit einer nach § 146 Abs. 2a AO genehmigten Verlagerung der elektronischen Buchführung (vgl. ↗ Kapitel 5.4 Outsourcing / Auslagerung von DMS-Funktionen) dürfen Papierbelege ins Ausland verbracht und bildlich erfasst werden. ▪ Die bildliche Erfassung hat dabei zeitnah zur Verbringung ins Ausland zu erfolgen.

d) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten – Mobile Erfassung

In Ergänzung zu den allgemeinen Ausführungen sind im Kontext der mobilen Belegerfassung insbesondere folgende Aspekte ins Kalkül zu ziehen:

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(110)	Vorbereitung	▪ Regelwerk für die Belegvorbereitung siehe oben. ▪ Definition der Dokumentarten, für die eine mobile Erfassung zulässig ist. ▪ Festlegung Prozedere für nicht personalisierte Belege (Kleinbetragsrechnungen ohne Firmierung).
(111)	Scanvorgang	▪ Unterstützung der passenden Endgeräte (iOS, Android etc.). ▪ Autorisierungsmöglichkeit zur Sicherstellung der Vertraulichkeit. ▪ Einsatz von Scan-Apps vs. Nutzung der Fotofunktion des mobilen Endgerätes. ▪ Scan-App sollte neben der Unterstützung der eingebauten Kamera auch die Verarbeitung originär elektronischer Belege ermöglichen. ▪ Ggf. Einsatz einer Halterung / Stativ bei umfangreicher Erfassung. ▪ Beleuchtungsverhältnisse festlegen / Einsatz der Blitzfunktion. ▪ Formatfestlegung für mobile Erfassung bspw. JPG, PDF, PDF / A (auch abhängig von der Nutzung der jeweiligen Scan-App). ▪ Nutzung der Zusatzfunktionen von eingesetzten Scan-Apps (Zoomen, Ausschneiden, Aufbereiten, Bildstabilisator).
(112)	Kompression	▪ Beim Einsatz von Scan-Apps kann durch die App eine Kompression erfolgen. ▪ Festlegung vom Kompressionssoftware für die Erfassung mit Scannern, die auch für die Kompression bei der mobilen Erfassung genutzt werden soll / kann.
(113)	Vollständigkeit	▪ Beim Abfotografieren kann eine Vollständigkeitskontrolle nur durch den Anwender manuell erfolgen. ▪ Beim Einsatz von Scan-Apps können diese bei der Erfassung von Seiten ggf. steuernd eingreifen (z. B. Button für Rückseite oder Button für Ende Dokument / neues Dokument).
(114)	OCR	▪ Scan-Apps ermöglichen bereits OCR / Volltexterstellung. Dabei ist jedoch auf eine hinreichende Qualität zu achten. ▪ Ggf. Nutzung der Komponenten, die auch für die Papiererfassung genutzt werden.
(115)	Indexierung	▪ Bei der mobilen Erfassung sind häufig nur beschränkte Möglichkeiten vorhanden. ▪ Die Benennung der Seiten / Dateien ist mit Scan-Apps möglich. ▪ Für die weitere Indizierung werden in der Regel keine mobilen Komponenten verwendet, sondern die Werkzeuge, die auch für die Indexierung von Papierdokumenten genutzt werden.
(116)	Export, Weitergabe	▪ Typischerweise »lockere« Schnittstelle zwischen mobilem Endgerät und weiterverarbeitender Anwendung, daher ist hier besonders die Vollständigkeit und Unveränderbarkeit sicherzustellen. ▪ Offline-Verarbeitung / Zwischenspeicherung der Dokumente kann erforderlich sein, da die Weitergabeschnittstelle nicht immer verfügbar ist. ▪ Scan-Apps bieten idealerweise Möglichkeiten, die eine sichere Übertragung gewährleisten (PDF- / PDF / A-Erstellung mit Passwortschutz der Dokumente, Weitergabe an Cloud oder per Fax etc.).
(117)	Belegprüfung	▪ Sicherstellung, dass dem Beleg ein Leistungsbezug für das Unternehmen zugrunde liegt. ▪ Gewährleistung einer Funktionstrennung zwischen der Person, die den Beleg einreicht und der Person, die den Beleg prüft.
(118)	Vernichtung	▪ Definition von Regelungen, wann und wie welche Papierdokumente nach dem bildlichen Erfassen vernichtet werden. ▪ Empfehlung: Vernichtung frühestens nach Auszahlung. ▪ Definition von Regelungen für Papierdokumente, die weiterhin im Papieroriginal aufzubewahren sind (z. B. Vorsteuervergütungsverfahren).
(119)	Bildliche Erfassung im Ausland	▪ Die bildliche Erfassung im Ausland ist gestattet, wenn die Belege im Ausland entstanden sind bzw. empfangen wurden und dort direkt erfasst werden.

4.4 Archivierung von E-Mails

a) Grundsatz und Kontrollziel

Die in ↗ Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze besitzen auch für steuerrelevante E-Mails ihre Gültigkeit. Entsprechend wird im Folgenden auf ausgewählte Besonderheiten eingegangen. Im Kern geht es dabei um die Sicherstellung der Verfügbarkeit steuerlich aufbewahrungspflichtiger E-Mails über die Dauer der gesetzlichen Aufbewahrungsfrist.

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.

b) DMS-Kontext

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

Werden steuerrelevante E-Mails in einer DMS-Umgebung aufbewahrt, müssen die allgemeinen Ordnungsmäßigkeitsanforderungen beachtet werden. Besonderheiten bestehen dahingehend, dass E-Mails aus mehreren Komponenten (Mail-Body, Attachement) bestehen.

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 aus Sicht der GoBD nicht aufbewahrungspflichtig (wie der Briefumschlag bei Papierdokumenten).

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(120)	Vollständigkeit	▪ E-Mails mit der Funktion eines Handels- bzw. Geschäftsbriefs oder eines Buchungsbelegs sind in elektronischer Form aufbewahrungspflichtig. ▪ Hinweis: Sowohl E-Mail-Bodies als auch E-Mail-Anhänge können steuerliche Relevanz besitzen. ▪ 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. E-Mail mit Antrag von Kunde XY. Die E-Mail insgesamt wird bei XY der Kategorie »Korrespondenz« zugeordnet. Der Anhang (Attachment) wird zusätzlich als eigenes Objekt der Kategorie »Anträge« zugeordnet). ▪ 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 aus rein steuerlicher Sicht grundsätzlich nicht aufbewahrungspflichtig (wie der Briefumschlag bei Papierdokumenten). ▪ Reine SPAM-E-Mails / Werbe-E-Mails sind nicht steuerrelevant.
(121)	Nachvollziehbarkeit und Nachprüfbarkeit	▪ Ändernde Aktionen an steuerrelevanten E-Mails müssen nachvollziehbar sein. ▪ Hinweis: Dies kann bei der reinen 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). ▪ Erstellung einer Verfahrensdokumentation für den Umgang und die Aufbewahrung von steuerrelevanten E-Mails.
(122)	Ordnung	▪ Ändernde Aktionen an steuerrelevanten E-Mails müssen nachvollziehbar sein. ▪ Hinweis: Dies kann bei der reinen 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). ▪ Erstellung einer Verfahrensdokumentation für den Umgang und die Aufbewahrung von steuerrelevanten E-Mails.
(123)	Zeitgerechte Belegsicherung	▪ Wenn eine vom E-Mail-System separate Aufbewahrungsumgebung eingesetzt wird, ist eine zeitnahe Überführung der steuerrelevanten E-Mails sicherzustellen.
(124)	Unveränderbarkeit und Konvertierung	▪ Bei der Konvertierung vom Ursprungsformat (bspw. MSG oder EML) darf die maschinelle Auswertbarkeit nicht eingeschränkt werden und es dürfen keine inhaltlichen Veränderungen vorgenommen werden, insbesondere muss die Möglichkeit der Recherche von Volltexten erhalten bleiben. ▪ Bei E-Mails mit Anhang gelten die in ↗ Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze entsprechend.

4.5 Archivierung von Rechnungen

a) Grundsatz und Kontrollziel

Die in ↗ Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen dargestellten Grundsätze besitzen auch für Rechnungsdokumente ihre Gültigkeit. Entsprechend wird im Folgenden auf ausgewählte Besonderheiten eingegangen. Im Kern geht es dabei um die Sicherstellung der Verfügbarkeit steuerlich aufbewahrungspflichtiger Rechnungen über die Dauer der gesetzlichen Aufbewahrungsfrist.

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 v. 2. Juli 2012 - IV D 2 - S 7287-a/09/10004 :003, BStBl. I 2012, S. 726) zu berücksichtigen.

b) DMS-Kontext

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 Archivierung von Ausgangsdokumenten (für die Aufbewahrung von Ausgangsrechnungen)
- ↗ Kapitel 4.2 Archivierung von Eingangsdokumenten (für elektronische Rechnungen)
- ↗ Kapitel 4.3 Bildliche Erfassung von Papierdokumenten (für Eingangsrechnungen in Papier)
- ↗ Kapitel 4.4 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.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(125)	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.
(126)	Rechnungsprüfung	▪ Einrichtung und Dokumentation einer Rechnungseingangsprüfung (Innerbetriebliches Kontrollverfahren mit Prüfpfad). Dies betrifft insbesondere die Prüfung der Pflichtangaben nach § 14 Abs. 4 UStG.
(127)	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.
(128)	Strukturierte Formate	▪ Soweit Rechnungen in einem strukturierten elektronischen Format (EDI, XML, XRechnung etc.) eingehen, ist sicherzustellen, dass die Lesbarkeit über die Dauer der Aufbewahrungsfrist durch entsprechende Anzeigeprogramme ermöglicht wird.
(129)	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. Unter bestimmten Voraussetzungen bestehen hierzu Ausnahmen. ▪ Hinweis: Vgl. ↗ Kapitel 2.1 Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit und ↗ Kapitel 5.2 Konvertierung.
(130)	Umgang mit inhaltlich identischen Mehrstücken	▪ Im Zusammenhang mit Hybridformaten wie ZUGFeRD stellt sich die Frage, welche der beiden Komponenten – PDF oder XML – den Beleg im steuerrechtlichen, insbesondere umsatzsteuerlichen Sinne darstellt. Da allerdings beide Komponenten (PDF und XML) für sich gesehen als Beleg fungieren können, ist den Vorgaben des § 14c UStG besondere Aufmerksamkeit zu widmen. ▪ Demnach läuft der Rechnungsaussteller Gefahr, die Umsatzsteuer doppelt zu schulden, wenn die PDF- und die XML-Datei inhaltlich divergieren und damit als jeweils eigenständige Rechnungen zu werten sind. Umgekehrt besteht bei sog. »inhaltlich identischen Mehrstücken« derselben Rechnung keine Gefahr einer umsatzsteuerlichen Mehrbelastung. ▪ Sind neben einer bildhaften Rechnung auch elektronische Daten vorhanden (identische Mehrstücke derselben Beleg-Art), ist die Aufbewahrung der tatsächlich weiterverarbeiteten Formate (buchungsbegründende Belege) ausreichend, sofern diese über die höchste maschinelle Auswertbarkeit verfügen. In diesem Fall erfüllt das Format mit der höchsten maschinellen Auswertbarkeit mit dessen vollständigem Dateninhalt die Belegfunktion und muss mit dessen vollständigem Inhalt gespeichert werden. Andernfalls sind beide Formate aufzubewahren.
(131)	Aufbewahrung im Ausland	▪ Zur Aufbewahrung im Ausland vgl. ↗ Kapitel 5.4 Outsourcing / Auslagerung von DMS-Funktionen.
(132)	Umgang mit Ausgangsrechnungen und AGB	▪ In der Randziffer 76 der GoBD werden die Anforderungen an den Umgang mit Ausgangsrechnungen detailliert beschrieben. Hier gilt wie bisher die inhaltliche Aufbewahrung (also die Aufbewahrung der Rechnungsdaten anstatt des erstellten Dokumentes) als ausreichend, wenn sichergestellt ist, dass diese Daten unverändert aufbewahrt werden – also bspw. unabhängig von Stammdatenänderungen sind. Hier stellt sich oft die Frage nach dem Umgang mit den in der Rechnung enthaltenen AGB. ▪ In diesem Zusammenhang wird festgestellt, dass die Aufbewahrung der AGBs zusammen mit einer Rechnung nicht erforderlich ist, wenn die AGB separat aufbewahrt sowie historisiert werden und es jederzeit erkennbar ist, welche AGB-Version für welches Rechnungsdokument gilt. ▪ Bezüglich der Layout-Informationen einer Ausgangsrechnung (Logos, Geschäftsführer-Informationen, grafische Gestaltung der Rechnung) sollte ebenfalls eine Übersicht vorhanden sein, welche Variante für welchen Zeitraum gegolten hat. Entsprechende Verfahren sollten in der Verfahrensdokumentation beschrieben sein.

5 Besondere Anforderung aus steuerlicher Sicht

5 Besondere Anforderung aus steuerlicher Sicht

Die besonderen Anforderungen aus steuerlicher Sicht betreffen die Themenbereiche:

- Maschinelle Auswertbarkeit und Datenzugriff
- Konvertierung
- Auslagerung und Migration
- Outsourcing / Auslagerung von DMS-Funktionen

5.1 Maschinelle Auswertbarkeit und Datenzugriff

a) Grundsatz und Kontrollziel

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 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«). Entsprechend sind alle steuerrelevanten Daten und Dokumente in maschinell auswertbarer Form über die Dauer der gesetzlichen Aufbewahrungsfrist vorzuhalten.

b) DMS-Kontext

Dem Kontrollziel entsprechend ergeben sich für DMS-Umgebungen – neben den bereits dargestellten Anforderungen – spezifische Aspekte:

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 und -struktur, der Datenfelder, der verwendeten Zeichensatztabellen sowie der internen und externen Verknüpfungen des zugrunde liegenden IT-Systems. 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.

Während eine maschinelle Auswertbarkeit bei Daten, Datensätzen, elektronischen Dokumenten und elektronischen Unterlagen unstrittig scheint, soweit diese mathematisch-technische Auswertungen ermöglichen, soll dies auch gegeben sein, wenn ausschließlich eine Volltextsuche möglich ist. Mittels Volltextsuche ergibt sich für die Finanzverwaltung die Möglichkeit einer nicht spezifizierten dateiübergreifenden Auswertung. Über frei wählbare Stichworte können jegliche Textdokumente wie E-Mails, Briefe, Buchungstexte oder Reisekostenabrechnungen durchsucht werden. Es ist also in der Praxis davon auszugehen, dass der Prüfer auch die vorhandenen Auswertungsmöglichkeiten eines DMS nutzt. Daher sollte hierfür ein entsprechendes Berechtigungsprofil vorhanden sein.

Auslagerung von steuerrelevanten Daten in ein DMS: Vgl. hierzu ↗ Kapitel 5.3 Auslagerung und Migration.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(133)	Unmittelbarer Datenzugriff / Z1-Zugriff sowie mittelbarer Datenzugriff / Z2-Zugriff	▪ Die Index- und Volltextsuche sowie die Dokumentenanzeige eines DMS müssen dem Prüfer bzw. unterstützenden Mitarbeiter zugänglich gemacht werden. ▪ Einrichtung eines Prüfer-Berechtigungsprofils mit den entsprechenden Einschränkungen (Mandant, Prüfungszeitraum, »Nur-Lese-Zugriff« ohne Export-Möglichkeit, ggf. mit Protokollierung). ▪ Sicherstellung (ggf. organisatorisch), dass durch den Prüferzugriff keine Systeminstabilitäten und Veränderungen auftreten (z. B. performance-intensive Suchabfragen, Änderungen, Löschungen).
(134)	Datenträgerüberlassung / Z3-Zugriff	▪ Möglichkeit der Zurverfügungstellung aller steuerlich relevanten Daten und Dokumente gemäß Prüfungsanordnung. ▪ Der Export von Trefferlisten und Dokumenten muss gemäß den Vorgaben des Prüfers möglich sein. ▪ Sicherstellung der zeitlichen Abgrenzbarkeit von aufbewahrungspflichtigen Daten und Dokumenten. ▪ Beschreibung des Export-Formates und der Feldtypen für die exportierten Daten und Dokumente. ▪ Sicherstellung, dass alle zur Auswertung der Dokumente und Daten notwendigen Strukturinformationen in maschinell auswertbarer Form zur Verfügung gestellt werden können (z. B. Feldbenennungen, Feldbeschreibungen, Feldtypen, Bedeutung von Werten in Werte-Tabellen).
(135)	Maschinelle Auswertbarkeit – Grundsatz	▪ Sicherstellung der maschinellen Auswertbarkeit der Daten und Dokumente. ▪ Neben den eigentlichen Daten und Dokumenten sind auch alle zur maschinellen Auswertung notwendigen Strukturinformationen (z. B. über die Dateiherkunft, die Dateistruktur, die Datenfelder, verwendete Zeichensatztabellen) sowie interne und externe Verknüpfungen sowohl vollständig als auch in nicht verdichteter Form aufzubewahren. ▪ Ermöglichung von mathematisch-technischen Auswertungen, Volltextsuchen oder einer Prüfung im weitesten Sinne (z. B. Bildschirmabfrage, die Nachverfolgung von Verknüpfungen und Verlinkungen, Textsuche nach bestimmten Eingabekriterien).
(136)	Ergänzung von OCR-Layern bei PDF-Dokumenten	▪ Werden bildlich erfasste Dokumente per OCR-Verfahren um Volltextinformationen angereichert (z. B. volltext-recherchierbare PDF-Dateien), so ist dieser Volltext nach Verifikation und Korrektur über die Dauer der Aufbewahrungsfrist ergänzend aufzubewahren und für Prüfzwecke verfügbar zu machen bzw. vorzuhalten.
(137)	Verschlüsselungstechnik	▪ Beim Einsatz von Verschlüsselungstechniken (Kryptographietechniken) muss sowohl die verschlüsselte als auch die unverschlüsselte Version des Dokumentes inkl. der Schlüssel aufbewahrt werden.
(138)	Historisierung der Systemeinstellung	▪ Die zum Zeitpunkt der Archivierung geltenden Stammdaten sowie Systemeinstellungen müssen transparent gemacht werden können (z. B. über eine entsprechende Protokollierung). ▪ Unternehmensspezifische Einstellungen, Anpassungen und Parametrisierungen am System sowie Änderungen in Tabellen müssen vorgehalten werden.

5.2 Konvertierung

a) Grundsatz und Kontrollziel

Nach den GoBD sind bei einer Umwandlung (Konvertierung) aufbewahrungspflichtiger Unterlagen in ein sogenanntes Inhouse-Format beide Versionen zu archivieren, unter demselben Index zu verwalten und die konvertierte Version als solche zu kennzeichnen. Dies stellt letztlich einen Ausfluss des progressiven und retrograden Prüfungserfordernisses dar.

Entsprechend der Neufassung der GoBD vom 28. November 2019 ist die Aufbewahrung beider Versionen bei Beachtung bestimmter Anforderungen entbehrlich. Die isolierte Aufbewahrung der konvertierten Fassung (»Ersetzendes oder verlustfreies Konvertieren«) ist dabei unter folgenden Voraussetzungen möglich:

- Es wird keine bildliche oder inhaltliche Veränderung vorgenommen.
- Bei der Konvertierung gehen keine sonstigen aufbewahrungspflichtigen Informationen verloren.
- Die ordnungsgemäße und verlustfreie Konvertierung wird nachvollziehbar dokumentiert (Verfahrensdokumentation).
- Die maschinelle Auswertbarkeit und der Datenzugriff durch die Finanzbehörde werden nicht eingeschränkt; dabei ist es zulässig, wenn bei der Konvertierung Zwischenaggregationsstufen nicht gespeichert, aber in der Verfahrensdokumentation so dargestellt werden, dass die retrograde und progressive Prüfbarkeit sichergestellt ist.

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.

b) DMS-Kontext

Dem Kontrollziel entsprechend sind – mit Ausnahme des ersetzenden Konvertierens – beide Versionen (originäre und konvertierte Fassung) entsprechend den Vorgaben der GoBD aufzubewahren.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(139)	Formatkonvertierung allgemein	▪ 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 und bei Prüfung auf Anforderung zur Verfügung zu stellen. ▪ Bei allen technischen Prozessen, bei denen Formatkonvertierungen erfolgen, ist sicherzustellen, dass die maschinellen Auswertungsmöglichkeiten (Sortier-, Summier-, Filterungsmöglichkeiten, Volltextsuche, Nachverfolgung von Verknüpfungen und Verlinkungen) nicht beeinträchtigt werden. ▪ Bei der Konvertierung dürfen keine sonstigen Informationen verloren gehen, die aufbewahrungspflichtig sind. ▪ 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 ausschließlich dem automatisierten Import dienen).
(140)	Ersetzendes Konvertieren	▪ Soweit nur die konvertierte Fassung (»Ersetzendes Konvertieren«) aufbewahrt werden soll, sind entsprechend der Neufassung der GoBD vom 28. November 2019 bestimmte Voraussetzungen zu erfüllen (keine bildliche und inhaltliche Veränderung, kein Verlust aufbewahrungspflichtiger Informationen, keine Einschränkung der maschinellen Auswertbarkeit und des Datenzugriffs, Vorhandensein einer Verfahrensdokumentation).
(141)	Konvertierung von E-Mails	▪ Bei der Konvertierung vom Ursprungsformat (MSG) darf die maschinelle Auswertbarkeit nicht eingeschränkt werden und es dürfen keine inhaltlichen Veränderungen vorgenommen werden, insbesondere muss die Möglichkeit der Recherche von Volltexten erhalten bleiben. ▪ E-Mail-Attribute müssen erhalten bleiben. ▪ Bei E-Mail-Attachments ist sicherzustellen, dass es zu keiner Einschränkung der maschinellen Auswertungsmöglichkeiten (insbesondere zu Zwecken der Recherche) kommt.
(142)	Konvertierung von ZUGFeRD-Rechnungen	▪ Das XML-Attachment muss analog dem PDF- / A-3-Container erhalten bleiben.
(143)	Dokumentation	▪ Die ordnungsgemäße und verlustfreie Konvertierung muss dokumentiert werden. ▪ Hinweis: Zur Verfahrensdokumentation vgl. ausführlich ↗ Kapitel 6 Verfahrensdokumentation.

5.3 Auslagerung und Migration

a) Grundsatz und Kontrollziel

Im Fall eines Systemwechsels, einer Systemänderung oder einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem darf nach den GoBD 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. Entsprechend müssen im Fall eines Systemwechsels, einer Systemänderung oder einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem die aufzeichnungs- und aufbewahrungspflichtigen Daten quantitativ und qualitativ gleichwertig in ein neues System überführt werden.

Sofern noch nicht mit der Außenprüfung begonnen wurde, ist es im Falle eines Systemwechsels oder einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem ausreichend, wenn nach Ablauf des 5. Kalenderjahres, das auf die Umstellung folgt, nur noch der Z3-Zugriff zur Verfügung gestellt wird (vgl. Neufassung der GoBD vom 28. November 2019).

b) DMS-Kontext

Bei der Migration von DMS-Umgebungen können die Anforderungen an die Beibehaltung der Auswertungsmöglichkeiten in der Regel 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 zumeist 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 (soweit originär digital). Ansonsten muss 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 die Beibehaltung der Auswertungsmöglichkeiten deutlich höher, da eine ERP-Umgebung über einen Funktionsumfang verfügt, der nicht ohne Weiteres durch ein DMS abgedeckt werden kann.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(144)	Konzept / Dokumentation	▪ Für die Durchführung von Migrationen muss ein entsprechendes Konzept (sog. Migrationskonzept) vorhanden sein, aus dem erkennbar wird, welche Regeln, Rahmenbedingungen und Zeiten für die Migration gelten (Analyse der IST-Situation, Bestimmung der Systemanforderungen, ggf. Konzeption von Funktionen und Schnittstellen, Festlegung Testmanagement zu Qualitätssicherungszwecken etc.).
(145)	Umfang der Migration	▪ Im Rahmen eines Migrationskonzepts ist zu definieren und zu dokumentieren, welcher Umfang an Daten und Dokumenten migriert werden soll. ▪ Dies ist typischerweise zeitraum- oder archivbereich-, stammdaten- oder dokumentartbezogen. ▪ Steuerliche Aufbewahrungsfristen sind dabei stets zu beachten.
(146)	Protokollierung der Dokumentenmigration	▪ Für die Daten- und Dokumentenmigration sind Protokolle zu erstellen, aus denen die Vollständigkeit und Unveränderbarkeit (inkl. der technischen Änderungen) nachvollziehbar werden. ▪ Alle Änderungen an Indexwerten müssen sowohl mit dem alten als auch dem neuen Wert protokolliert werden.
(147)	Vollständigkeit	▪ Die Daten und Dokumente (einschließlich Metadaten, Stammdaten, Bewegungsdaten sowie die erforderlichen Verknüpfungen) müssen quantitativ und qualitativ gleichwertig überführt werden. ▪ Hierfür sind entsprechende Prüfprozesse, die die Vollständigkeit zwischen Alt- und Neusystem gewährleisten, »aufzusetzen«.
(148)	Nachweis nicht übernommener Dokumente	▪ Für Daten und Dokumente, die aus unterschiedlichen Gründen nicht übernommen werden konnten (z. B. aufgrund abgelaufener Aufbewahrungsfristen, mangelnder Relevanz etc.), sollte sichergestellt werden, dass ein entsprechender Nachweis über diese Daten und Dokumente vorhanden ist. ▪ Der entsprechende Nachweis sollte zumindest die Identifikation im Quellsystem und eine fachliche Identifikation enthalten (z. B. Dokumentenart und Kundennummer).
(149)	Vorgehen bei mehreren Dokumentversionen	▪ Sind im Quellsystem mehrere Dokumentversionen enthalten, muss festgelegt werden, inwieweit alle Daten- und Dokumentenversionen übernommen werden oder ob nach definierten Regeln nur eine teilweise Übernahme zu erfolgen hat. ▪ Hierbei sollte beschrieben sein, wie sich die versionierten Dokumente im Zielsystem darstellen (z. B. auch als versioniertes Dokument oder als mehrere Einzeldokumente).
(150)	Auswertungsmöglichkeiten	▪ Sicherstellung der maschinellen Auswertbarkeit im Falle von Systemwechseln, Systemänderungen oder Auslagerung. ▪ Aufrechterhaltung quantitativ und qualitativ gleicher Auswertungsmöglichkeiten, als wären die Daten und Dokumente noch im alten System. Hierfür sind entsprechende Prüfprozesse, die die gleichwertige Auswertbarkeit zwischen Alt- und Neusystem gewährleisten, »aufzusetzen«. ▪ Sofern noch nicht mit der Außenprüfung begonnen wurde, ist es im Falle eines Systemwechsels oder einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem ausreichend, wenn nach Ablauf des 5. Kalenderjahres, das auf die Umstellung folgt, nur noch der Z3-Zugriff zur Verfügung gestellt wird.
(151)	Reports und sonstige Auswertungsmöglichkeiten	▪ Vorhandene Systemreports mit steuerlichem Bezug (z. B. Übersicht Rechnungen sortiert nach Zahlungsziel) müssen auch im Zielsystem vorhanden sein.
(152)	Volltext-Index	▪ Ist ein Volltext-Index vorhanden, sollte ein Nachweis über die Übernahme oder ggf. den Neuaufbau der Indexstrukturen erfolgen.
(153)	Mapping-Regeln (bei Datenbeständen)	▪ Es ist sicherzustellen, dass für die Migration der Datenbestände das Mapping vom Quelldatenbanksystem zum Zielsystem dokumentiert ist. ▪ Gegebenenfalls erforderliche Änderungen, Aufteilungen oder Zusammenfassungen von Indexstrukturen sollten nachvollzogen werden können. ▪ Es darf zu keinen Einschränkungen von vorhandenen Suchmöglichkeiten kommen.

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(154)	Konvertierungen	▪ Bei Formatkonvertierungen im Rahmen der Migration sind die Anforderungen an die maschinelle Auswertbarkeit (vgl. ↗ Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff) und die Vorgaben im Rahmen von Konvertierungen (vgl. ↗ Kapitel 5.2 Konvertierung) zu beachten.
(155)	Verlinkungen	▪ Verlinkungen wie z. B. Buchungen zu Dokumenten oder Referenzen zwischen Anwendungen müssen im Rahmen der Migration erhalten bleiben (vgl. ↗ 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. ▪ Hinweis: Wenn ein externes ERP Referenzen auf die Doc-IDs enthält, so sind diese Doc-IDs im Neusystem als recherchierbare Indexfelder anzulegen, damit das ERP die Dokumente finden kann.
(156)	Abbildung von Notizen und grafischen Annotationen	▪ Da Notizen und grafische Annotationen oft herstellerspezifisch umgesetzt sind, sollte festgelegt werden, wie hiermit im Rahmen der Migration umgegangen 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).

5.4 Outsourcing / Auslagerung von DMS-Funktionen

a) Grundsatz und Kontrollziel

Die in ↗ Kapitel 3.2 Rechenzentrum und Cloud Computing dargestellten Grundsätze haben auch aus steuerlicher Sicht ihre Gültigkeit. Entsprechend wird im Folgenden auf ausgewählte Besonderheiten im steuerlichen Kontext eingegangen.

Besonderheiten aus steuerlicher Sicht gilt es insbesondere 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 GoBD und damit einhergehend die Vorgaben zum Datenzugriff in vollem Umfang eingehalten werden. Für Rechnungen existiert eine Sonderregelung (§ 14b UStG). 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 sowie deren Herunterladen und Verwendung gewährleistet ist. Zum bildlichen Erfassen im Ausland vgl. ↗ Kapitel 4.3 Bildliche Erfassung von Papierdokumenten.

b) DMS-Kontext

Anforderungen an das Outsourcing sind nur indirekt in den GoBD enthalten. Die Verantwortung für die Ordnungsmäßigkeit elektronischer Bücher und sonstiger erforderlicher elektronischer Aufzeichnungen einschließlich der Verfahren trägt – auch bei einer teilweisen oder vollständigen organisatorischen und / oder technischen Auslagerung von Buchführungs- und Aufzeichnungspflichten auf Dritte (Outsourcing) – allein der Steuerpflichtige.

Soweit das DMS im Ausland betrieben wird, müssen die angeforderten Unterlagen und Daten unverzüglich zur Verfügung gestellt, die angeforderten Auskünfte zeitnah erteilt und Datenzugriffsmöglichkeiten in vollem Umfang gewährleistet werden können. Dazu ist regelmäßig ein Antrag nach § 146 Abs. 2a AO zu stellen.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(157)	Maschinelle Auswertbarkeit / Datenzugriff	▪ Die in ↗ Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff definierten Anforderungen müssen auch bei der Auslagerung von Funktionen uneingeschränkt gegeben sein und erhalten bleiben. ▪ Zu den allgemeinen Anforderungen an einen ordnungsgemäßen IT-Betrieb vgl. ↗ Kapitel 3 Anforderungen an den ordnungsgemäßen IT-Betrieb.
(158)	Verfahrensdokumentation	▪ Sicherstellung der Dokumentation der Verfahren und des IKS seitens des Dienstleistungsunternehmens sowie des auslagernden Unternehmens. 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. ▪ Zur Verfahrensdokumentation vgl. ausführlich ↗ Kapitel 6 Verfahrensdokumentation.
(159)	Auslagerung ins Ausland	▪ Bei einer Auslagerung ins Ausland sind besondere steuerliche Vorgaben zu beachten. ▪ Es ist ein schriftlicher Antrag beim zuständigen Finanzamt zu stellen. ▪ Der schriftliche Antrag muss insbesondere eine detaillierte Beschreibung der für die Verlagerung vorgesehenen elektronischen Bücher und sonstigen erforderlichen elektronischen Aufzeichnungen enthalten. ▪ Sicherstellung des Rechts auf Datenzugriff (vgl. ↗ Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff). ▪ Sonderfall Rechnungen: Eine elektronische Aufbewahrung von Rechnungen im übrigen Gemeinschaftsgebiet setzt voraus, dass eine vollständige Fernabfrage (Online-Zugriff) der betreffenden Daten gewährleistet ist. ▪ Zum bildlichen Erfassen im Rahmen einer genehmigten Verlagerung der elektronischen Buchführung vgl. ↗ Kapitel 4.3 Bildliche Erfassung von Papierdokumenten.

6 Verfahrens-dokumentation

6 Verfahrensdokumentation

6.1 Erstellung und Umgang mit der Verfahrensdokumentation

a) Grundsatz und Kontrollziel

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 stets eine ordnungsgemäße Verfahrensdokumentation, welche die Beschreibung aller zum Verständnis der Buchführung erforderlichen Verfahrensbestandteile, Daten und Dokumentbestände enthalten muss. Dabei hat die Dokumentation stets den in der Praxis eingesetzten Komponenten und Prozessen des DV-Systems zu entsprechen, umgekehrt müssen die Inhalte einer Verfahrensdokumentation auch so »gelebt werden«. Die Verfahrensdokumentation hat sowohl die aktuellen als auch die historischen Verfahrensinhalte für die Dauer der Aufbewahrungsfrist nachzuweisen und den in der Praxis eingesetzten Versionen des DV-Systems zu entsprechen.

b) DMS-Kontext

Entsprechend dem Kontrollziel muss 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 vgl. ↗ Kapitel 6.2 Inhalte einer Verfahrensdokumentation.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(160)	Gegenstand einer Verfahrensdokumentation	▪ Die Verfahrensdokumentation hat den »End-to-End«-Prozess von der Entstehung bzw. dem Eingang originär elektronischer Daten bzw. digitalisierter Dokumente bis zur Bereitstellung im Rahmen des Datenzugriffs der Finanzverwaltung zu beschreiben.
(161)	Erstellen der Verfahrensdokumentation allgemein	▪ Häufig erfolgt die Erstellung mit den bereits im Unternehmen im Einsatz befindlichen Office-Anwendungen (z. B. Textverarbeitungs- und Tabellenkalkulationsprogramme) nebst Ablage im Dateisystem oder in der eigenen DMS-Umgebung. ▪ Ist eine »Wiki-Umgebung« oder Intranet-Lösung im Einsatz, entscheiden sich Unternehmen häufig für die Pflege der Dokumentation in dieser Umgebung. ▪ Das zu verwendende Tool wird häufig auch danach ausgewählt, wie erforderliche bzw. bereits vorhandene Dokumentationen erstellt und gepflegt werden (z. B. IT-Betriebskonzept, Arbeitsanweisungen).
(162)	Vorhandene Dokumentationen, mitgeltende Unterlagen	▪ Bei der Erstellung und Pflege einer Verfahrensdokumentation hat es sich bewährt, die wesentlichen Prozesse in einem sog. »Masterdokument« niederzulegen. ▪ Die den Prozessen zugehörigen Sekundärinformationen (Arbeitsanweisungen, technische Dokumentationen, Beschreibung IKS etc.) sollten als Anlagen (Sekundärdokumente oder mitgeltende Unterlagen) dem Masterdokument beigefügt sein. ▪ Vorhandene Dokumentationen, auf die als Sekundärdokumente oder mitgeltende Unterlagen verwiesen werden kann, sind typischerweise Fachkonzepte, IT-Konzepte, Arbeitsanweisungen oder auch Organisationshandbücher. ▪ Nutzung einfacher Verlinkungsmöglichkeiten zum Verweis auf vorhandene Beschreibungen. ▪ Es ist sicherzustellen, dass bei einem Verweis die Anforderungen an die Versionierung mit Änderungsprotokoll erfüllt werden.

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

(163)	Zuständigkeiten für Erstellung und Pflegeregeln	▪ Beispiele für Themen, die beim Hersteller angesiedelt sind:
		  ▪ Beschreibung von Standardfunktionen
		  ▪ Beschreibung der internen technischen Prozesse etc.
		  ▪ Möglichkeit der Systemmigration
		  ▪ Zurverfügungstellung einer Mustervorlage durch den Hersteller
		▪ Beispiele für Themen, die beim Integrator / Systemhaus angesiedelt sind:
		  ▪ Beschreibung der Einrichtung des Systems (z. B. Dokumentarten, Indexfelder, Gruppen und Rechte, technische Einstellungen etc.)
		▪ Beispiele für Themen, die beim Betreiber angesiedelt sind:
		  ▪ Allgemeine Beschreibung des Unternehmens und des Einsatzzwecks
		  ▪ Vorhalten von Arbeitsanweisungen
		  ▪ Beschreibung des Vorgehens bei Test und Abnahme
		  ▪ Sicherstellung der Betriebssicherheit sowie der Betriebsbereitschaft
		  ▪ Individuelle Umsetzung der sachlogischen Prozesse
		  ▪ Umfang und Vorgehensweise bei Schulungen
		▪ Hinweis: Vor allem für die Erstellung, aber auch die anschließende Pflege und Freigabe der Verfahrensdokumentation empfiehlt es sich, beim Betreiber sowohl einen technischen als auch einen fachlichen System- bzw. Anwendungsverantwortlichen zu bestimmen.

(164)	Unveränderbarkeit und Pflege der Verfahrensdokumentation	▪ Sicherstellung einer korrekten und permanenten Versionierung / Historisierung der Dokumentation. ▪ Dazu sollte es Regeln geben, bei welchen Änderungen eine Anpassung der Verfahrensdokumentation erforderlich ist und wann nur referenzierte Daten und Dokumente fortgeschrieben werden. ▪ 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). ▪ Anbringen eines Zeitstempels bei Versionierung der Verfahrensdokumentation und Archivierung mit / in einem DMS- bzw. Archivsystem (alternativ gesonderter Ausdruck). ▪ Bei geringfügigen Änderungen bietet sich ggf. eine jährliche Aktualisierung (z. B. zum Ende des Geschäftsjahres) an.

(165)	Übereinstimmung von Verfahrensdokumentation und realem Systembetrieb	▪ Vorhandensein eines regelmäßigen Review-Prozesses der Verfahrensdokumentation zur Sicherstellung der
		  ▪ Vollständigkeit und Aktualität (Nachweisprotokolle),
		  ▪ tatsächlichen Identität von Prozessen und Dokumentation.
		▪ Vorhandensein eines Prozesses, durch den die Aufbewahrung der jeweils gültigen Verfahrensdokumentation über die Dauer der gesetzlichen Aufbewahrungsfrist sichergestellt wird.
		▪ Bei lediglich trivialen Änderungen ist eine Dokumentation ggf. entbehrlich. Hier sollten jedoch klare Regeln existieren, welche Änderungen als »relevant« angesehen werden und von wem diese zu dokumentieren sind.
		▪ Relevante Änderungen am DMS werden nur nach einer expliziten Freigabe vorgenommen.
		▪ Die Zuständigkeiten für die Freigabe sind vom Unternehmen zu definieren.

(166)	Aufbewahrung der Verfahrensdokumentation	▪ Die Verfahrensdokumentation gehört zu den Arbeitsanweisungen sowie 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.

6.2 Inhalte einer Verfahrensdokumentation

a) Grundsatz und Kontrollziel

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. Aus der Verfahrensdokumentation muss sich ergeben, wie die in den GoBD enthaltenen Anforderungen und Ordnungsvorschriften Beachtung finden (»Steuerliche Verfahrensdokumentation«). Insbesondere müssen daraus Inhalt, Aufbau und Ergebnisse des DV-Verfahrens vollständig und schlüssig ersichtlich sein.

Über die formale Gestaltung und technische Ausführung kann der Buchführungspflichtige individuell entscheiden. Eine konkrete Definition der Inhalte einer Verfahrensdokumentation enthält die GoBD nicht. Es existiert lediglich der 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, wie bspw. auf die Anwenderdokumentation, auf Testdokumentationen oder grundsätzliche Steuerungs- und Kontrollkonzepte (IT-Risikomanagement und allgemeines Sicherheitskonzept, Bedrohungen und Maßnahmen, IT-Strategie, IT-Sicherheitsrichtlinie etc.) verweisen. Die Gesamtheit der Dokumente stellt die Verfahrensdokumentation i. S. d. GoBD dar. 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) DMS-Kontext

Entsprechend dem Kontrollziel ist der organisatorisch und technisch gewollte Prozess zu beschreiben. In Bezug auf elektronische Dokumente betrifft dies den End-to-End-Prozess von der Entstehung der Informationen über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, der Absicherung gegen Verlust und Verfälschung bis hin zur Reproduktion.

c) Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten
(167)	Gliederung und Pflichtbestandteile	▪ Die Gliederung in die Bestandteile Allgemeine Beschreibung, Anwenderdokumentation, Technische Systemdokumentation sowie Betriebsdokumentation ist nicht zwingend vorgeschrieben. Eine Gliederung entlang der sachlogischen Prozesse vereinfacht die Zuordnung von Bearbeitern und Verantwortlichkeiten sowie den korrespondierenden Kontrollzielen und Kontrollen je Teilprozess. Dabei können sich die erforderlichen Inhalte sowohl aus einem Masterdokument als auch aus mitgeltenden Unterlagen ergeben. Die Gesamtheit aller erstellten und referenzierten Dokumente stellt die Verfahrensdokumentation i. S. d. GoBD dar.
(168)	Allgemeine Beschreibung, Compliance-Rahmen	▪ Zur allgemeinen Beschreibung rechnen Ausführungen zu Rahmenbedingungen, Aufgabenstellung und Einsatzgebiet. ▪ Beschreibung aller durch die Systemlösung einzuhaltenden Richtlinien, wie Gesetze, Verordnungen, Auflagen und Vereinbarungen.
(169)	Aufbau- und Ablauforganisation	▪ Darstellung des Unternehmens bzw. der Organisation sowie der organisationsspezifischen Schwerpunkte. ▪ Vorhalten von Organisationsbeschreibungen der betroffenen Bereiche. ▪ Beschreibung des genauen Standorts des Systems. ▪ Verständliche Darstellung der Aufbauorganisation sowohl in Textform als auch grafisch.
(170)	Anwenderdokumentation	▪ Gegenstand der Anwenderdokumentation ist eine Beschreibung der fachlichen Prozesse. ▪ Die Anwenderdokumentation muss alle Informationen enthalten, die für eine sachgerechte Anwendung einer IT-Anwendung erforderlich sind.
(171)	Technische Systemdokumentation	▪ Die technische Systemdokumentation beinhaltet im Wesentlichen eine Darstellung der eingesetzten IT-Anwendungen. ▪ Die technische Systemdokumentation enthält eine technische Darstellung der IT-Anwendung. Sie ist Grundlage für die Einrichtung eines sicheren und geordneten IT-Betriebs sowie für die Wartung der IT-Anwendung durch den Programmersteller. Art und Umfang der technischen Dokumentation sind abhängig von der Komplexität der IT-Anwendung. Die Dokumentationstechnik und formale Gestaltung der technischen Dokumentation liegen im Ermessen des Programmerstellers.
(172)	Betriebsdokumentation	▪ Die Betriebsdokumentation untergliedert sich typischerweise in die Bereiche der Anweisungen und Dokumentationen zum IT-Betrieb und zur IT-Sicherheit sowie der Kontrollgrundsätze und Kontrollen zur Einrichtung und Änderung sowohl der eingesetzten Verfahren als auch Systeme. ▪ Die Betriebsdokumentation dient der Dokumentation der ordnungsgemäßen Anwendung des Verfahrens.
(173)	GoBD-Bezug, steuerliches IKS	▪ Bei der Beschreibung der sachlogischen Prozesse ist sicherzustellen, dass hervorgeht, wie die Ordnungsmäßigkeitsgrundsätze der GoBD (vgl. insbesondere ↗ Kapitel 2 Allgemeine Anforderungen an DMS-Produkte und Lösungen) eingehalten werden. ▪ Beschreibung der automatischen und manuellen Kontrollfunktionen in der Verfahrensdokumentation. ▪ Im Speziellen ist zu beschreiben, wie das Recht auf Datenzugriff (vgl. ↗ Kapitel 5.1 Maschinelle Auswertbarkeit und Datenzugriff) gewährleistet wird. ▪ Ergänzende Beschreibung des steuerlichen IKS.

Nr.	Bereich	Empfehlungen, Hinweise und Umsetzungsmöglichkeiten

(174)	IT-Infrastruktur, IT-Umfeld	▪ Übersichtliche Systemdarstellung mit allen Komponenten inkl. der Darstellung von Beziehungen zu vorgelagerten Systemen (IT-Komponenten).
		▪ 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 technischen Verarbeitungsregeln (z. B. Datenflüsse, Protokollierungen, Ablaufpläne etc.).
		▪ Beschreibung der IT General Controls:
		  ▪ Beschreibung der Maßnahmen betreffend Sicherheitskonzept
		  ▪ Beschreibung der Maßnahmen betreffend physische Sicherungsmaßnahmen und Zutrittskontrollen
		  ▪ Beschreibung der Maßnahmen betreffend logische Zugriffskontrollen und Zugriffsschutz
		  ▪ Beschreibung der Maßnahmen betreffend Backup & Recovery bzw. Datensicherungs- und Auslagerungsverfahren
		  ▪ Beschreibung der Maßnahmen betreffend Monitoring
		  ▪ Beschreibung der Maßnahmen betreffend Betriebsbereitschaft und Incident- / Problem-Management
		  ▪ Beschreibung der Maßnahmen betreffend Notfallmanagement (Business Continuity Management, Disaster Recovery Planning)
		  ▪ Beschreibung der Maßnahmen betreffend Change-Management

(175)	Sonstige relevante Dokumentationen und Inhalte	▪ Darstellung der vorhandenen Mitarbeiterqualifikation (z. B. Rollen, erforderliche Kenntnisse, durchgeführte Qualifizierungsmaßnahmen), Kompetenzen und Verantwortlichkeiten für den Betrieb. ▪ Organisationsanweisungen für die fachlichen Prozesse / Arbeitsanweisungen für den Standardbetrieb (z. B. bildliche Erfassung (scannen / fotografieren), 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 (z. B. Verantwortlichkeiten, Eskalationswege, präventive Wartung, Störungsbehebung, Dokumentation). ▪ Verfahren zur Sicherstellung der Programmidentität (Identität von technischer Umgebung zur Dokumentation).

Anhang

Anhang

Abkürzungsverzeichnis

Abkürzung	Definition
AO	Abgabenordnung
BMF	Bundesministerium der Finanzen
BStBl	Bundessteuerblatt
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
HGB	Handelsgesetzbuch
IDW	Institut der Wirtschaftsprüfer
IKS	Internes Kontrollsystem
OCR	Optical Character Recognition
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

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). »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.

Bildliche Erfassung

Der Begriff beinhaltet sowohl das Scannen von Dokumenten als auch das Fotografieren.

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. 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

Dokumenten Management 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,
- Anhängen.

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 usw.) 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 die steuerlichen 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«. Neufassung vom 28. November 2019. Die GoBD ersetzt die bisher geltenden GoBS sowie die GDPdU.

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 auf die 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.

Hashwert

Ein Hashwert ist ein eindeutiger Zahlenwert, der durch einen mathematischen Algorithmus aus dem Inhalt einer Information gebildet wird. Somit ist die 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 sowohl 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. Die Aufbewahrungsvorschriften im 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.

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 Zeichencodes (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. Hierzu 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

Beim Scannen oder bildlichen Erfassen wird mit einer Hardware (dem Scanner) durch rasterförmiges Auflösen eines Bildes in Bildpunkte und Umwandlung der im Bild enthaltenen schwarzen, weißen, grauen oder farbigen Werte 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.

XRechnung

Nationale Möglichkeit der Spezifizierung der europäischen Norm für die elektronische Rechnungsstellung (»CEN-Norm«).

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 und am 11. März 2019 die Version 2.0 der Spezifikation veröffentlicht.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

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