Rechtliche Anforderungen an das Dokumentenmanagement

Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhbw.de, Raum 149B

Version: 1.1

Folien: [HTML] https://delors.github.io/dm-rechtliche-aspekte/folien.de.rst.html
[PDF] https://delors.github.io/dm-rechtliche-aspekte/folien.de.rst.html.pdf

Fehler melden: https://github.com/Delors/delors.github.io/issues

Dokumente

- Dokumente sind Träger von Daten, die Aufschluss über Handlungen, Abläufe und Produkte eines Unternehmens oder einen Institution geben.
- Dokumente dienen als Nachweis sowohl im Tagesgeschäft als auch bei Streitigkeiten.
- Dokumente berühren eine Reihe von gesetzlichen Regelungen, Normen und Vorschriften.

Warnung

Dieser Foliensatz dient ausschließlich einer grundlegenden Orientierung. Für eine abschließende juristische Bewertung ist ggf. juristischer Rat einzuholen.

Rechtliche Grundlagen (Deutschland - 2023)

gesetzliche Grundlagen, rechtliche Themen	AO	DSGVO	BDSG	BetrVG	BGB	GoB	GoBD	HGB	eIDAS VDG	UrhG	ZPO
Ordnungsmäßigkeit, Integrität, Authentizität	X	X	X		X	X	x	X	X		
Schutz vor Verlust (Datensicherheit)		X	X				x				
Schutz vor unberechtigtem Zugriff (Datenschutz)		X	X	X							
Ermittlung und Einhaltung der Aufbewahrungs-fristen	X				X			X			
Sicherstellung des gesetzlichen Zugriffs	X							X			
Sicherstellung der Beweiskraft vor Gericht							X		X		X
Beteiligungsrechte der Mitarbeiter				X							
Schutz vor Verletzung des Urheberrechts										X	

(Quelle: S. 30, Tab. 3-1 in *Dokumentenmanagement* von K. Götzer, Pc. Maué, U. Emmert, 2023, dpunkt.verlag)

AO: Abgabeordnung
DSGVO: Datenschutz-Grundverordnung
BDSG: Bundesdatenschutz-gesetz
BetrVG: Betriebsverfassungsgesetz
BGB: Bürgerliches Gesetzbuch
GoB: Grundsätze ordnungsgemäßer Buchführung
GoBD: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
HGB: Handelsgesetzbuch
eIDAS: Verordnung über elektronische Identitäten und Vertrauensdienste
VDG: Vertrauensdienstegesetz
UrhG: Gesetz über Urheberrecht und verwandte Schutzrechte
ZPO: Zivilprozessordnung

Allgemeine Grundsätze: Ordnungsmäßigkeit von Dokumenten

- gilt insbesondere für Dokumente, die die Buchhaltung berühren
- solche, die dem Nachweis von rechtlich relevanten Sachverhalten dienen
- die einer gesetzlichen Aufbewahrungsfrist unterliegen
- Es gibt keine branchen- und fachübergreifenden gesetzlichen Regelungen.
- Im Bereich des Handels und Steuerrechts gibt es detaillierte Vorgaben.

Allgemeine Grundsätze: Integrität von Dokumenten

- gilt als gewahrt, wenn Dokumente inhaltlich vollständig und unverändert erhalten sind.

  Mögliche formalisierte Kriterien:

  - Seitennummerierung mit Bezug zur Gesamtzahl der Seiten
  - Kordel und Siegel bei notariellen Urkunden
  - Signatur jeder einzelnen Seite
  - den Nachweis über den unverfälschten Inhalt von nicht-elektronischen Dokumenten können ggf. nur kriminaltechnische Untersuchungen erbringen
- Die Integrität von elektronischen Dokumenten kann durch Signaturen gewährleistet werden.

Allgemeine Grundsätze: Authentizität von Dokumenten

- Nachweis des Ursprungs des Dokuments.
- Bei originären Papierdokumenten, typischerweise durch handschriftliche Signatur auf dem Originaldokument.
- Die Authentizität von elektronischen Dokumenten kann durch Signaturen gewährleistet werden.

Revisionssicherheit

> *Revisionssicherheit bezieht sich rückblickend auf die Prüfbarkeit des eingesetzten Verfahrens der Aufbewahrung und somit nicht nur auf technische Komponenten, sondern auf die gesamte Lösung. Revisionssicherheit schließt sichere Abläufe, die Organisation des Unternehmens, die ordnungsgemäße Nutzung, den sicheren Betrieb und den Nachweis in einer Verfahrensdokumentation ein.*
>
> ***—Verband Organisations- und Informationssysteme e.V. (VOI)***

Grundsätze ordnungsgemäßer Buchführung (GoB)

- Ein unbestimmter Rechtsbegriff: die GOB können sich durch gutachterliche Stellungnahmen, Handelsbrauch, ständige Übung, Gewohnheitsrecht, organisatorische und technische Änderungen weiter entwickeln und sind einem Wandel unterworfen.
- bzgl. Buchführung und Rechnungsstellung ergibt sich aus dem HGB:
  - Grundsatz der Richtigkeit und Willkürfreiheit
  - Grundsatz der Klarheit und Übersichtlichkeit
  - Grundsatz der Einzelbewertung
  - Grundsatz der Vollständigkeit
  - Grundsatz der Ordnungsmäßigkeit
  - Grundsatz der Sicherheit (Revisionssichere Aufbewahrung)
  - Belegprinzip

§126a BGB: Schriftform

Die elektronische Form wird mit der Schriftform im deutschen Recht gleichgestellt. Die gesetzliche Schriftform ist erfüllt, wenn elektronische Dokumente mit einer qualifizierten elektronischen Signatur versehen sind.

Die Beweiskraft elektronisch signierter Dokumente ist in der ZPO geregelt.

Elektronische Signaturen

einfache elektronische Signatur:

Die Daten sind keiner Person zugeordnet.

fortgeschrittene elektronische Signatur:

- ausschließlich einer best. Person zugeordnet.
- ermöglicht die Identifizierung der Person.
- wird mit Mitteln erzeugt, die ausschließlich die Person unter alleiniger Kontrolle hat.
- eine nachträgliche Veränderung der Daten kann erkannt werden.

qualifizierte elektronische Signatur:

- basiert auf einem qualifizierten Zertifikat für eine natürliche Person.
- wird mit einem sicheren Signaturerstellungsgerät erzeugt.

elektronisches Siegel:

Erfolgt mithilfe eines Zertifikats, dass auf den Namen einer Organisation ausgestellt wurde.

Die einfache elektronische Signatur ist die am wenigsten sichere Form der elektronischen Signatur.

Scannen von externen Dokumenten

- Externe Dokumente dürfen ersetzend gescannt werden.
- Die Dokumente sind nach dem Stand der Technik zu scannen.
  (TR-ESOR 03125 bzw. TR-RESISCAN 03138)
- Bei gescannten öffentlichen Urkunden gilt §371b ZPO; d. h. der Beweiswert bleibt erhalten wenn der Scan von einer öffentlichen Behörde oder einer mit öffentlichen Glauben versehen Personen durchgeführt wurde.
- Relevante Vorschriften ergeben sich aus TR 3138 Resiscan des BSI.
- Durch eine verbindliche Auskunft nach Paragraph 38 AO kann eine Garantie für die Akzeptanz gescannter Dokumente durch das Finanzamt erwirkt werden.

1. Datenschutz und Datensicherheit

Datenschutz - Grundlagen

Achtung!

In Dokumentenmanagementsystem enthalten fast alle Dokumente personenbezogene Daten!

für Unternehmen in Deutschland und Bundesbehörden:

- Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutz-gesetz (BDSG)

für öffentliche Stellen der Länder:

- Datenschutz-Grundverordnung (DSGVO)
- die jeweiligen Landesdatenschutzgesetze

spezielle Regelungen:

- Sozialdatenschutz
- Telekommunikations- und Telemediendatenschutz im TTDSG
- ...

§32 DSGVO

Stellen, die mit personenbezogenen Daten umgehen, müssen technische und organisatorische Maßnahmen treffen, um die Anforderungen der DSGVO zu gewährleisten.

Zu gewährleisten ist:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten.
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit des Systems und der Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu Ihnen bei einem Zwischenfall wiederherstellen zu können.
- ein dokumentiertes Verfahren bezüglich der Wirksamkeit der technischen und organisatorischen Maßnahmen in Hinblick auf die Gewährleistung der Sicherheit der Verarbeitung.

Bemerkung
Es gilt der Grundsatz der Verhältnismäßigkeit.

Datensicherheit von Dokumentenverwaltungs- und Archivierungslösungen

in folgenden Bereichen müssen Maßnahmen ergriffen werden:

- Personal
- Gebäudesicherheit
- Organisation
- Administration
- eingesetzte Werkzeuge

Besondere Schutzmaßnahmen bei personenbezogenen Daten (§5 DSGVO)

Verarbeitungsgrundsätze

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz.
- Zweckbindung, Verarbeitung der Daten, nur für den bei Erhebung beabsichtigten Zweck.
- Datenminimierung.
- Richtigkeit und Aktualität.
- Identifizierbarkeit nur bis zur Zweckerreichung, danach Löschung oder Anonymisierung.
- Integrität und Vertraulichkeit.
- Rechenschaftspflicht für alle vorangegangenen Pflichten

Anforderung an die Revisionssicherheit gemäß GoBD

- das Verfahren zur Vergabe von Zugriffsberechtigungen muss dokumentiert und nachvollziehbar sein.
- Zugriffsberechtigungen sind Personen bezogen zu vergeben.
- Zugriffe sind zu protokollieren.
- Bild und Datenträger müssen vor fremden Zugriff sicher aufbewahrt werden.
- Sicherheitsmaßnahmen sind regelmäßig zu hinterfragen und auf einer Risikoanalyse basieren.
- das Verfahren zur Vergabe von Zugriffsberechtigungen muss dokumentiert und nachvollziehbar sein.
- die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit sowie Authentizität und Revisionssicherheit sind einzuhalten.

Rechte von Betroffenen gemäß DSGVO

- Recht auf Auskunft über gespeicherte Daten.
- Recht auf Korrektur der Daten.
- Recht auf Löschung der Daten.
- Recht auf Sperrung der Daten.
- Recht auf Gegendarstellung.

Warnung

Diese Rechte können im Widerspruch zu anderen rechtlichen Vorschriften stehen.

Beispiel

Gezielte Korrektur von gespeicherten Daten nach DSGVO; nach HGB bzw. AO soll eine Manipulation von Daten nicht möglich sein.

"privilegiertes Löschen"

- die Speicherung von Daten ist bei unrechtmäßiger Verarbeitung nicht erlaubt (BDSG).

  Dies umfasst ggf. personenbezogene Daten oder auch Daten bei denen der Besitz strafbar ist (z. B. KiPo oder verfassungsfeindliche Inhalte).

- Systeme zur revisionssicheren Aufbewahrung müssen deswegen eine Option anbieten, Daten vor Ablauf der Aufbewahrungsfristen zu löschen.

  Dies muss unter erhöhten Sicherheitsanforderungen (Vier-Augen-Prinzip, erweiterte Protokollierung) geschehen; das Vorgehen muss dokumentiert sein.

Datenschutz und Datensicherheit bei der Verwendung von Cloud-Diensten

- Die Regelungen bezüglich der Datensicherheit sind im Cloud Vertrag festzuhalten.
- Sicherheitsvereinbarungen werden häufig über Security Service Level Agreements (SSLAs) getroffen.
- Gemäß Datenschutzrecht ist diejenige Stelle, die die Entscheidungen bzgl. des Umgangs mit den personenbezogenen Daten trägt, auch rechtlich verantwortlich.
- Auch bei der Auftragsverarbeitung bleibt der Cloud Anwender als Auftraggeber verantwortlich; eine Übertragung der Verantwortlichkeit ist nicht möglich.

Datenschutz beim Vertrauen in US-amerikanische Cloud-Anbieter

[...] Microsoft gibt keine Garantie, dass EU-Daten nie an die US-Regierung weitergegeben werden: Das sagte Anton Carniaux, Chefjustiziar von Microsoft France, bei einer Anhörung vor dem französischen Senat des Parlaments aus. Konkret ging es um Daten, die Microsoft von der Union des Groupements d'Achats Publics (UGAP) erhält, der zentralen Beschaffungsstelle des öffentlichen Sektors für Schulen, Rathäuser und kommunale Verwaltungen. Auf die Frage, ob der Konzern niemals deren Informationen an die US-Regierung ohne ausdrückliche Zustimmung der französischen Behörden übermitteln würde, antwortete Carniaux, dass er das unter Eid nicht garantieren könne.

[...] Der Konzern wolle ferner die betroffenen Kunden hierüber informieren, müsse bei den US-Behörden jedoch erst um eine Erlaubnis hierzu bitten. [...]

—21.07.2025 - Heise.de: Keine Garantien: Microsoft muss EU-Daten an USA übermitteln

Datenschutz beim Austausch von Daten mit den USA

Zwischen der EU und den USA sollen Daten unkompliziert fließen - unter Einhaltung hoher Schutzstandards. Ist das dafür bestehende Abkommen ausreichend?
Ja, sagt das Gericht der EU - und sendet zugleich ein wichtiges Signal.

[...] Um regelmäßigen Datentransfer zu vereinfachen und dabei gleichzeitig einen hohen Datenschutzstandard zu gewährleisten, gibt es zwischen der Europäischen Union und den USA [...] Das Data Privacy Framework (DPF) - eine Rahmenvereinbarung [aus dem Jahr 2023], die dafür sorgen soll, dass das hohe Schutzniveau für Daten in der EU auch dann nicht verwässert wird, wenn Daten aus Europa in die USA fließen. [...]

[...] Ob dieses hohe Datenschutzniveau und diese strengen Vorgaben für die US-Behörden auch unter der Präsidentschaft von Donald Trump noch gelten, hat das Gericht in seinem Urteil nicht geklärt. Es sei aber Sache der EU-Kommission, darauf ein Auge zu haben. [...]

—03.09.2025 - Tagesschau.de: EU-Gericht weist Klage gegen Abkommen mit den USA ab

2. Aufbewahrungsfristen

Die Frist

Definition

Frist: ein bestimmter oder bestimmbarer Zeitraum.

- Die Dauer einer Aufbewahrungsfrist ist abhängig von dem Fristbeginn und dem Aufbewahrungszeitraum.
- Die Aufbewahrungsgründe und die Inhalte der Dokumente müssen dazu bekannt sein.

Fristbeginn (vgl. §187 BGB)

Häufig an ein konkretes Datum geknüpft:

- z. B. 1. Januar des Folgejahres
- an ein Ereignis
- Ablauf des Kalenderjahres in dem die letzte Änderung erfolgte
- Bei Akten/Projekten: Abschluss des Projekts

Aufbewahrungsgründe

- die Dokumente werden für betriebliche Belange benötigt (z. B. Wartung/Instandhaltung)
- historische Gründe (z. B. Unternehmensgeschichte)
- gesetzliche Gründe
- die Dokumente sind ggf. Beweismittel in einem Rechtsstreit

Gesetzliche Aufbewahrungsfristen

- Häufig nicht an konkrete Dokumententypen gebunden.
- Aussagen zur Frist leiten sich ggf. aus Nachweispflichten ab.
- Oft gibt es erhebliche Abgrenzungsschwierigkeiten zwischen den anzuwenden Vorschriften bzw. Gesetzen.

  Z.B. § 257 HGB vs. §§ 140-147 AO; d. h. Aufbewahrungspflicht 6 oder 10 Jahre.

  Vgl. IHK Konstanz - Aufbewahrungsfristen (Stand 2020)
- Werden auch gel. angepasst (2024 wurde die Aufbewahrungspflicht für Belege verkürzt).
- *Aufbewahrungspflichten werden in der Fachliteratur zusammengetragen und können dort entnommen werden.*

Aufbewahrungspflichten Ermitteln

- Einzelheiten zu der steuerrechtlichen Aufbewahrungspflicht werden in der Abgabenordnung (primär in § 147) geregelt.
- Jedoch ergeben sich steuerrechtliche Aufbewahrungspflichten auch durch „andere Gesetze“ (z. B. Steuergesetze wie das Umsatzsteuergesetz).
- Bzgl. „andere Gesetze“:

> *[... Gemeint] sind u. a. das HGB und **eine Vielzahl von Gesetzen und Verordnungen**, die für bestimmte Berufe oder Tätigkeiten Aufzeichnungs- und Buchführungspflichten vorschreiben. Beispielsweise müssen die Bewachungsbetriebe Auftragsbücher nach § 14 Abs. 2 Verordnung über das Bewachungsgewerbe i. V. m. § 34a Abs. 2 Nr. 3c Gewerbeordnung führen.*
>
> —***IHK Hamburg (Abgerufen März 2024)***

Fristfindung

dokumentenbezogen:

1. die Dokumententypen einer Einheit (z. B. Abteilung) werden ermittelt
2. die Aufbewahrungsgründe werden festgestellt
3. Feststellung der betrieblichen und der (in)direkten gesetzlichen Aufbewahrungsfristen

prozessbezogen:

1. Feststellung der Aufbewahrungsgründe pro Betrachtungseinheit
2. Zuordnung der Dokumente zu den Aufbewahrungsgründen
3. Feststellung der entsprechenden Dokumententypen

Dokumentation der Aufbewahrungsfristen

Fristenkatalog:

- Dokumententypen
- Fristbeginn
- Aufbewahrungszeitraum
- gesetzliche und/oder betriebliche Grundlage
- Aufbewahrungsform (z. B. Original)

Sicherstellung des gesetzlichen Zugriffs

- Innerhalb der Aufbewahrungsfrist muss der Zugriff auf die Dokumente innerhalb angemessener Zeit gewährleistet sein.
- Eine Speicherung in der Cloud ist nicht grundsätzliche verboten; der Zugriff (durch Behörden etc.) muss jedoch gewährleistet sein.

  (Dies kann die Verarbeitung in einem Rechenzentrum in der EU bzw. Deutschland erfordern und muss durch entsprechende Verträge abgesichert sein.)
- Für steuerlich relevante Dokumente gelten besondere Anforderungen, die sich direkt aus der GoBD ergeben.

  Dokumente, die nicht digital vorliegen, müssen nicht digitalisiert werden, um den Anforderungen der GoBD zu genügen; können jedoch digitalisiert werden, wenn eine Verfahrensdokumentation vorliegt.

"Innerhalb angemessener Zeit" bedeutet in der Regel innerhalb weniger Stunden bzw. Tage.

In den GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff) werden in Hinblick auf Datenzugriff und Prüfbarkeit von digitalen Dokumenten Vorgaben gemacht, die aber „nur“ bzgl. steuerlich relevanter Dokumente Anwendung finden.

Grundsätzlich gilt, dass steuerrechtliche Dokumente in Deutschland aufbewahrt werden müssen; Ausnahmen sind auf Antrag ggf. möglich.

Arten des Datenzugriffs

1. unmittelbarer Zugriff auf die Daten

   Dem Prüfer müssen die entsprechenden Hilfsmittel zur Verfügung gestellt werden, um die Daten zu prüfen.

2. mittelbarer Zugriff auf die Daten

   Die Finanzbehörde erstellt Vorgaben bzgl. der benötigten Auswertungen, die dann der Steuerpflichtige ausführen muss.

3. Datenträgerüberlassung

   Die Daten werden auf einem Datenträger übergeben und können dann von der Finanzbehörde geprüft werden.

Sicherstellung der Beweiskraft vor Gericht

- gem. ZPO sind insbesondere Urkunden als Beweismittel zulässig.
- Beweisführung mittels elektronischer Dokumente erfolgt nach den Regeln des Augenscheinbeweises.

  Bei E-Mails ist der Nachweis der Authentizität und Integrität ggf. problematisch.
- E-Mails mit einer qualifizierten elektronischen Signatur haben die Beweiskraft einer Urkunde.
- Bei der Verwendung von einfachen elektronischen Signaturen unterliegt die Beweiskraft der freien Beweiswürdigung durch das Gericht.

  Private elektronische Dokumente mit einer qualifizierten Signatur haben einen höheren Beweiswert als private Urkunden.
- Qualifizierte Signaturen können z. B. mit dem neuen Personalausweis und einem Kartenleser erzeugt werden.

Vor Gericht sind auch noch Zeugen, (Sachverständige Zeugen), Sachverständige, Augenschein und Parteivernehmung als Beweismittel zulässig.

Urkunden

- gemeinhin ein Originaldokument in Papierform (man unterscheidet: öffentliche und private Urkunden)
- Voraussetzung: Echtheit (Nachweis über die Echtheit der Unterschrift)
- Urkundsbeweise ist der zuverlässigste Beweis im Zivilprozess.

Zertifizierung von Systemen und Lösungen

- Prüfkriterien für Dokumentenmanagementlösungen (PK-DML) vom TÜV-IT und dem VOI.
  Bewertung erfolgt nach internationalen ISO Standards.
- Die Verwendung eines zertifizierten Dokumentenmanagementsystem entbindet den Anwender nicht von der funktionalen, technischen und betriebswirtschaftlichen Beurteilung des Produktes.
- Gesetzliche geforderte Zertifizierungen gibt es im Bereich Dokumentenmanagementsysteme nicht.

Zertifizierungen von Dokumentenmanagementsystemen

- Die (Entwicklungs-)Prozesse des Herstellers sind zertifiziert (z. B. ISO 9000).
- Die DMS Lösung wird von anderen Herstellern zertifiziert (Zweck garantierte Interoperabilität).
- Die Lösung ist Teil einer Prozesszertifizierung und dient der Qualitätsverbesserung des zu zertifizierenden Prozesses. (z. B. ISO 9000 und ISO 14001)
- Die DMS-Software bzw. Teile davon sind nach anerkannten Prüfungsgrundlagen zertifiziert.
- Die DMS-Lösung ist in der Gesamtheit (inkl. administrativer und organisatorischer Prozesse) zertifiziert.

Typische Zertifizierungsgrundlagen

- IEC/ISO 12119

  Allgemeine Anforderungen an Software in Hinblick auf

  a. die Dokumentation und
  b. die Zuverlässigkeit und Funktionalität der Software.

- IDW PS 880: „Softwaretestat“

  Orientiert sich an gesetzlichen Grundlagen - insbesondere in Hinblick auf die Rechnungslegung.

- RAL GZ 901: „Prospektprüfung“

  Leistet das Produkt das Versprochene?

IDW ≙ Institut der Wirtschaftsprüfer in Deutschland e.V.