3 Rechtliche Anforderungen an das Dokumenten-Management

Das Thema Dokumenten-Management ist von einer Vielzahl von rechtlichen Vorschriften abhängig und wird durch sie maßgeblich beeinflusst. In diesem Kapitel werden die wichtigsten rechtlichen Anforderungen im deutschen und Schweizer Recht dargestellt.

Dabei geht es um sehr viele unterschiedliche Rechtsgebiete: um allgemeines Zivilrecht und Zivilprozessrecht im Bereich der Formvorschriften, um Handels-, Verwaltungs- und Steuerrecht im Bereich von Aufbewahrung und Rechnungsstellung, um Datenschutzrecht sowie um Urheberrecht.

In den letzten 6 Jahren seit dem Erscheinen der 5. Auflage haben sich erhebliche Änderungen in quasi allen hier behandelten Rechtsgebieten ergeben, sodass eine umfassende Überarbeitung dieses Kapitels notwendig war.

Das bisherige Datenschutzrecht wurde durch die Datenschutz-Grundverordnung (DSGVO) der EU abgelöst, das Signaturgesetz durch die EU-Verordnung über elektronische Identitäten und Vertrauensdienste, die GDPdU durch schon die zweite Fassung der GoBD usw.

Auch auf die Schweiz haben die Entwicklungen Einfluss genommen: Das neue Datenschutzgesetz wurde schon auf Druck der EU an die DSGVO angepasst, soll aber erst 2023 in Kraft treten. Auf der anderen Seite wurden auch hier Bürokratiehürden abgebaut, z. B. durch die Streichung der EIDI-V.

3.1 Das Kapitel »Rechtliche Aspekte«

Dieses Kapitel wurde von Praktikern für Praktiker nach rechtlichen Themen systematisiert, die für den Einsatz von Dokumenten-Management- und Archivlösungen relevant sind. Auf die berührten gesetzlichen Regelungen und anderweitige Richtlinien wird themenspezifisch eingegangen. In den Unterkapiteln wird zwischen deutschem und Schweizer Recht unterschieden. In den Ausführungen zum Schweizer Recht sind die relevanten Bundesgesetze und Verordnungen berücksichtigt. Im konkreten Anwendungsfall kann aber auch die Einbeziehung kantonalen Rechts vonnöten sein, auf das in dieser Veröffentlichung nicht weiter eingegangen werden soll.

Dokumente sind Träger von Daten, die Aufschluss über Handlungen, Abläufe und Produkte eines Unternehmens oder einer Institution geben. Häufig dienen sie als Nachweis sowohl im Tagesgeschäft als auch bei Streitigkeiten. Allein die Tatsache, dass Dokumente erzeugt, verwaltet und aufbewahrt werden, berührt eine Reihe von gesetzlichen Regelungen, Normen und Vorschriften, die zu beachten sind (siehe Tab. 3–1). Darüber hinaus entscheidet der Dokumenteninhalt über die Notwendigkeit, weitere rechtliche Anforderungen zu berücksichtigen.

Die Autoren möchten ausdrücklich darauf hinweisen, dass eine abschließende rechtliche Bewertung nur an konkret vorliegenden Sachverhalten vorgenommen werden kann und zu diesem Zweck professioneller juristischer Rat eingeholt werden sollte.

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 Aufbewahrungsfristen	X				X			X			
Sicherstellung des gesetzlichen Zugriffs	X						X	X			
Sicherstellung der Beweiskraft vor Gericht							X		X		X
Beteiligungsrechte der Mitarbeiter				X							
Schutz vor Verletzung des Urheberrechts										X	

AO – Abgabeordnung; DSGVO – Datenschutz-Grundverordnung; BDSG – Bundesdatenschutzgesetz; 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

Tab. 3–1 *Gesetzliche Grundlagen und Themen – Bundesrepublik Deutschland*

Tab. 3–1 und Tab. 3–2 dienen Ihnen als Orientierung. Aus ihnen gehen die gesetzlichen Grundlagen hervor, die durch die jeweiligen rechtlichen Themen berührt werden. Diese wiederum spiegeln sich in den Überschriften der Unterkapitel wider.

Gesetzliche Grundlagen/ rechtliche Themen	DSG, VDSG	GeBüV	MWSTG, MWSTGV	OR	UrhG	ZertES, VZertES
Ordnungsmäßigkeit, Integrität, Authentizität		X	X	X		X
Schutz vor Verlust (Datensicherung)		X				
Schutz vor unberechtigtem Zugriff (Datenschutz)	X					
Ermittlung und Einhaltung der Aufbewahrungsfristen				X		X
Sicherstellung des gesetzlichen Zugriffs		X	X	X		
Sicherstellung der Beweiskraft vor Gericht						

DSG – Bundesgesetz über den Datenschutz; VDSG – Verordnung zum Bundesgesetz über den Datenschutz; GeBüV – Geschäftsbücherverordnung; MWSTG – Mehrwertsteuergesetz, MWSTGV – Verordnung zum Mehrwertsteuergesetz; OR – Obligationsrecht; UrhG – Gesetz über Urheberrecht und verwandte Schutzrechte; ZertES – Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, VZertES – Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur

Tab. 3–2 *Rechtliche Grundlagen und Themen – Schweiz*

3.1.1 Allgemeine Grundsätze

Die **Ordnungsmäßigkeit** bei der Erstellung, Verwaltung und Archivierung ist eine wesentliche Basis zur Erlangung von Rechtssicherheit. Der Begriff der Ordnungsmäßigkeit wird im Folgenden, soweit nicht anders beschrieben, stellvertretend für die Nachvollziehbarkeit von Vorgängen und Dokumenteninhalten, für die systematische Gliederung von Dokumentenstrukturen sowie für die Wahrung der Integrität und Authentizität verwendet. Grundsätzlich sollte die Ordnungsmäßigkeit für alle Dokumenttypen gelten, die in einer Organisationseinheit erstellt, verwaltet und archiviert werden. Aufgrund gesetzlicher Regelungen gilt sie aber insbesondere für Dokumente, die die Buchhaltung berühren, Dokumente, die als Nachweis von rechtlich relevanten Sachverhalten genutzt werden sollen, sowie für Dokumente, die einer gesetzlichen Aufbewahrungsfrist unterliegen. Für die Einhaltung der Ordnungsmäßigkeit gibt es keine branchen- und fachübergreifenden gesetzlichen Regelungen. Allerdings wurden im Bereich des Handels- und

Steuerrechts detaillierte Vorgaben erlassen, die wegen fehlender fachspezifischer Regelungen sinngemäß auf andere Bereiche übertragen werden sollten.

Die **Integrität** eines Dokuments ist gewahrt, wenn dieses inhaltlich vollständig und unveränderlich erhalten ist. Häufig werden formale Kriterien angesetzt, um die Vollständigkeit der Inhalte zu wahren, z.B. Seitennummerierung mit Bezug auf die Gesamtseitenanzahl, Signatur jeder einzelnen Seite bzw. Kordel und Siegel bei notariellen Urkunden. Der unverfälschte Inhalt kann hingegen häufig nur mit kriminaltechnischen Mitteln bestätigt werden.

Die **Authentizität** eines Dokuments, d.h. der Nachweis seines Ursprungs, ist rechtlich relevant, wenn ein Dokument Urkundencharakter trägt und/oder als Nachweis verwendet werden soll (siehe auch Kapitel 3.6). Bisher war der Nachweis des Ursprungs an die Vorlage des Originaldokuments in Papierform geknüpft. Als wesentliches Merkmal zum Nachweis der Authentizität bei originären Papierdokumenten wird die handschriftliche Signatur betrachtet (siehe Abbildung 3–1).

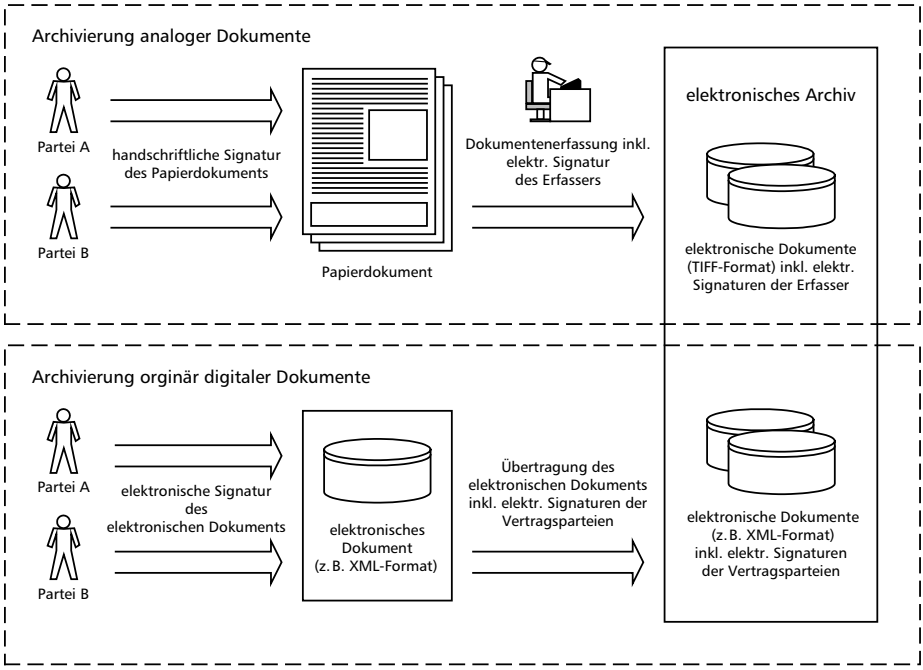

Abb. 3–1 *Originär digitale Dokumente versus analoge Dokumente*

Bereits seit den 1970er-Jahren bestehen die technischen Voraussetzungen, um Integrität und Authentizität elektronischer Dokumente auch mithilfe elektronischer Signaturen sicherzustellen.[1]

1. Durch die Entwicklung des Public-Key-Ansatzes seit 1970 und die Patentierung des RSA-Verfahrens im Jahre 1977 (RSA: nach seinen Entwicklern Rivest, Shamir und Adleman)

An dieser Stelle muss auf die bereits beschriebenen Erscheinungsformen elektronischer Dokumente hingewiesen werden. Aus rechtlicher Sicht muss die Erscheinungsform »analoge Dokumente« von »originär digitalen Dokumenten« unterschieden werden. Bei der Umwandlung der Papierform in elektronische Dokumente muss damit umgegangen werden, dass ein solcher Medienbruch rechtliche Folgen für die Beweiswirkung von Dokumenten hat (siehe auch Kapitel 3.6).

Die durchgängige Sicherstellung der Integrität und Authentizität eines elektronischen Dokuments mithilfe der elektronischen Signatur ist nur bei originär digitalen Dokumenten möglich. Wird hingegen ein analoges Dokument z. B. unmittelbar nach dem Scannen signiert, so kann die elektronische Signatur zwar zur Identifikation der Person dienen, die das Dokument erfasst hat, und die Integrität für die Folgebearbeitung abgesichert werden; aber ein Nachweis für die Authentizität und ein Nachweis für die Wahrung der Integrität, bevor das Dokument gescannt worden ist, kann somit nicht technisch aus dem elektronisch signierten Dokument abgeleitet werden.

Die Sicherstellung und die Erhaltung von Integrität und Authentizität bei einem Wechsel der Informationsträger (Medienbruch) ist ein grundsätzliches Problem, das sowohl in Deutschland als auch in der Schweiz über rechtliche Bestimmungen gelöst wird.

Für öffentliche elektronische Dokumente, also Dokumente einer Behörde oder einer mit öffentlichem Glauben versehenen Person, bleibt nach § 371b ZPO beim ersetzenden Scannen der Beweiswert erhalten, wenn die Dokumente von einer öffentlichen Behörde oder einer mit öffentlichem Glauben versehenen Person nach dem Stand der Technik gescannt werden.

»Stand der Technik« ist in Deutschland nach dem Minikommentar des Bundesinnenministeriums zum E-Government-Gesetz[2] die Einhaltung der Technischen Richtlinien TR-ESOR 03125[3] zur Beweiswerterhaltung[4] bzw. TR-RESISCAN 03138[5] zum Ersetzenden Scannen[6] des Bundesamts für Sicherheit in der Informationstechnik.

Ohne die Verwendung qualifizierter elektronischer Signaturen gibt es keine zwingende Beweisregel für das ersetzende Scannen; es verbleibt hier beim Augenscheinbeweis, d. h., der Richter kann selbst entscheiden, ob das verwendete Verfahren in seinen Augen revisionssicher ist.

---

2. *https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/e-government-gesetz-minikommentar.pdf;jsessionid=198A80010B78C77A520BC997490071C7.1_cid364?__blob=publicationFile&v=2*
3. *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html*
4. BMI-Minikommentar zu § 6 EGovG
5. *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138.pdf?__blob=publicationFile&v=5*
6. BMI-Minikommentar zu § 7 EGovG

In jedem Fall wird man davon ausgehen können, dass die Einhaltung der TR-RESISCAN geeignet ist, die Revisionssicherheit nachzuweisen. Der Begriff *Revisionssicherheit* wurde 1992 durch den *Verband Organisations- und Informationssysteme (VOI) e. V.* geprägt, dessen stellvertretender Vorstandsvorsitzender der Mitautor ist, und er bedeutet:

> *»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 Anwenderunternehmens, die ordnungsgemäße Nutzung, den sicheren Betrieb und den Nachweis in einer Verfahrensdokumentation ein. Wesentliches Merkmal revisionssicherer Archivsysteme ist, dass die Informationen wieder auffindbar, nachvollziehbar, unveränderbar und verfälschungssicher archiviert sind. Revisionssichere Archivierung ist ein wesentlicher Bestandteil für die Compliance von Informationssystemen.«*[7]

Daneben sind für die Anforderungen der Finanzverwaltung die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)[8] vom 28.11.2019 zu beachten, die aufgrund der Vorgaben von Handelsgesetzbuch und Abgabenordnung als Nachfolger von GoBS und GdPdU zum 1.1.2015 in Kraft getreten sind und seit 1.1.2020 in einer neuen, digitalisierungsfreundlicheren Version gelten.

Wichtige Rechtsgrundlagen im handels- und steuerrechtlichen Bereich in Deutschland sind das Handelsgesetzbuch (HGB), die Abgabenordnung (AO) sowie die Grundsätze ordnungsmäßiger Buchführung (GoB), die sich aus den Kommentierungen zu den Gesetzen und aus der betrieblichen Praxis entwickelt haben und ein Regelwerk darstellen, das die gesamte Rechnungslegung berührt.

Definiert wird das Wesen der GoB in Abschnitt 1.10 der GoBD vom 28.11.2019[9] wie folgt: »Die GoB sind ein unbestimmter Rechtsbegriff, der insbesondere durch Rechtsnormen und Rechtsprechung geprägt ist und von der Rechtsprechung und Verwaltung jeweils im Einzelnen auszulegen und anzuwenden ist.« (BFH-Urteil vom 12. Mai 1966, BStBl III S. 371; BVerfG-Beschluss vom 10. Oktober 1961, 2 BvL 1/59, BVerfGE 13 S. 153). Die GoB können sich durch gutachterliche Stellungnahmen, Handelsbrauch, ständige Übung, Gewohnheitsrecht, organisatorische und technische Änderungen weiterentwickeln und sind einem Wandel unterworfen.

---

7. *https://de.wikipedia.org/wiki/Revisionssicherheit*
8. *https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf?__blob=publicationFile&v=13*
9. GoBD, Seite 7, Tz 17 ff.

Grundsätze der GOB für die Buchführung und Rechnungsstellung sind:

- Grundsatz der Richtigkeit und Willkürfreiheit: Der Jahresabschluss ist nach gültigen Regeln erstellt und lässt sich objektiv aus den Büchern herleiten (§ 239 Abs. 2 HGB).
- Grundsatz der Klarheit und Übersichtlichkeit: Die äußere Gestaltung der Unterlagen muss es sachverständigen Dritten ermöglichen, die Buchführung nachzuvollziehen (§ 238 Abs. 1 S. 2 HGB, § 243 Abs. 2 HGB).
- Grundsatz der Einzelbewertung: Sämtliche Vermögensgegenstände sind einzeln zu bewerten, in bestimmten Fällen sind Gruppenbewertungen zulässig (§ 252 Abs. 1 Nr. 3 HGB).
- Grundsatz der Vollständigkeit: Eine lückenlose Buchführung wird erwartet (§ 239 Abs. 2 HGB, § 246 Abs. 1 HGB).
- Grundsatz der Ordnungsmäßigkeit: Geschäftsvorfälle sind zeitnah und chronologisch zu erfassen (239 Abs. 2 HGB).
- Grundsatz der Sicherheit: Unterlagen sind revisionssicher für die Dauer der gesetzlichen Aufbewahrungspflicht zu archivieren (§ 147 AO, § 257 Abs. 1 und 4 HGB, § 14b UStG, § 239 Abs. 3 HGB).
- Belegprinzip: Jedem einzelnen Geschäftsfall muss ein Beleg zugrunde liegen (§ 238 Abs. 1 und 2 HGB).

»Der Zusammenhang zwischen dem zugrundeliegenden Geschäftsvorfall und dessen Buchung bzw. dessen DV-Verarbeitung muss durch eine aussagekräftige Verfahrensdokumentation – ergänzend durch den Nachweis ihrer ordnungsmäßigen Anwendung – dargestellt werden«.[10] Der Verfahrensdokumentation und dem Nachweis ihrer Anwendung kommen somit Schlüsselfunktionen zu, um die Ordnungsmäßigkeit der Erstellung, Verwaltung und Archivierung von Dokumenten sicherzustellen. Die Erstellung und Pflege der Verfahrensdokumentation liegen in der Verantwortung des Buchführungspflichtigen.[11] Umfang und Aufbau sind nicht vorgeschrieben. Die GoBD legt nur den Mindestinhalt fest. Eine bereits bestehende Verfahrensdokumentation, z. B. für eine Buchhaltungslösung, kann auf die Dokumenten-Management- und Archivierungslösung ausgedehnt werden.

Im Grundsatz sind von den GoBD handelsrechtlich und steuerrechtlich relevante Organisations- und Informatiklösungen betroffen. Jedoch gibt es in der Praxis bereits Fälle, bei denen mangels anderweitiger Regelungen auf die GoBD verwiesen wird. Dies führt dazu, dass die Verfahrensdokumentation nach GoBD immer öfter zum Standard auch für andere Fachgebiete erklärt wird.

Die Neufassung der GoBD im Jahr 2019 hat zu einer Anpassung an moderne IT-Verfahren geführt. So ist es nicht mehr unzulässig, unterwegs, sogar im Aus-

10. GoBD, Seite 36, Tz. 10.1
11. vgl. Tz. 10.1 GoBD

land, Belege mit der Smartphone-Kamera zu erfassen und dann an das Unternehmen zu schicken, um diese Kopie dann revisionssicher zu speichern. Ebenso ist die Führung der Buchhaltung in der Cloud explizit erlaubt, wenn die übrigen Rahmenbedingungen der GoBD und der Gesetze, insbesondere des HGB und der DSGVO, eingehalten werden.

Die konkrete Struktur und die Inhalte für eine Verfahrensdokumentation nach den GoBD sind im Kapitel 3.10 beschrieben.

Wie bereits weiter oben erwähnt, kann eine elektronische Signatur die Grundlage für die Sicherung der Integrität und Authentizität von elektronischen Dokumenten bilden. Das erste deutsche Signaturgesetz (SigG) wurde im Jahr 1997 als Teil des Gesetzes des Bundes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) erlassen.[12] 2001 und 2005 gab es Änderungen des Signaturgesetzes und der zugehörigen Signaturverordnung mit den spezifischen technischen Voraussetzungen. Seit dem 28.08.2014 gilt in der ganzen Europäischen Union die eIDAS-Verordnung über elektronische Identitäten und Vertrauensdienste (EU 910/2014)[13], die im Unterschied zur vorherigen EU-Signaturrichtlinie 1999/93/EG[14] nicht mehr nur einen Rechtsrahmen für die Mitgliedsstaaten bietet, sondern direkt in der ganzen EU anwendbar ist. Seit 2016 sind auch die wesentlichen Durchführungsverordnungen mit den technischen Normen der Vertrauensdienste in Kraft.

Neben der elektronischen Signatur gibt es seitdem weitere Vertrauensdienste:

- Erstellung, Überprüfung und Validierung von
  - elektronischen Signaturen
  - elektronischen Siegeln
  - elektronischen Zeitstempeln
- Zustellung elektronischer Einschreiben
- Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung
- Bewahrungsdienste von Dokumenten mit elektronischen Signaturen, Siegeln oder Zertifikaten

In Folge des Formanpassungsgesetzes[15] wurde § 126a in das BGB aufgenommen. Durch ihn wird die elektronische Form mit der Schriftform im deutschen Recht gleichgestellt, wie es nun auch in Art. 25 der eIDAS-Verordnung vorgesehen ist. Generell gilt nun, dass die gesetzliche Schriftform erfüllt ist, wenn elektronische

12. vgl. Art. 3 IuKDG
13. *https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910*
14. *https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31999L0093&from=ES*
15. Gesetz zur Anpassung der Formvorschriften im Privatrecht und anderer Vorschriften an den modernen Rechtsverkehr vom 01.08.2001

Dokumente mit einer qualifizierten elektronischen Signatur versehen sind. Es sei denn, die elektronische Form ist explizit ausgeschlossen, wie z.B. bei privaten Bürgschaften oder Schuldanerkenntnissen. Die Beweiskraft elektronisch signierter Dokumente ist in den §§ 371a ff. und 415 ff. ZPO geregelt.

In der **Schweiz** stellen das Obligationenrecht (OR)[16] und das Mehrwertsteuergesetz (MWSTG)[17] sowie die Geschäftsbücherverordnung von 2002[18] und das Bundesgesetz über die elektronische Signatur (ZertES)[19] die wichtigsten rechtlichen Grundlagen für eine ordnungsgemäße Verwaltung und Archivierung von Dokumenten dar. So kann sinngemäß das OR als Rechtsgrundlage für die handelsrechtlichen Aspekte angesehen werden und das MWSTG als stellvertretende Grundlage für die steuerliche Seite dienen.

Die Möglichkeit, Bücher, Buchungsbelege und Geschäftskorrespondenz in elektronischer Form zu verwahren, ist im Grundsatz durch das OR gesetzlich geklärt.[20] Ausnahmen bilden lediglich Betriebsrechnung und Bilanz; diese sind grundsätzlich schriftlich und unterzeichnet aufzubewahren.[21] Unter bestimmten Voraussetzungen besitzen elektronische Dokumente und Dokumente in Papierform die gleiche Beweiskraft.[22]

Im Obligationenrecht heißt es zur Frage der Grundsätze ordnungsmäßiger Buchführung und zur Möglichkeit elektronischer Belege:

»Die Buchführung bildet die Grundlage der Rechnungslegung. Sie erfasst diejenigen Geschäftsvorfälle und Sachverhalte, die für die Darstellung der Vermögens-, Finanzierungs- und Ertragslage des Unternehmens (wirtschaftliche Lage) notwendig sind.

Sie folgt den Grundsätzen ordnungsmässiger Buchführung. Namentlich sind zu beachten:

1. die vollständige, wahrheitsgetreue und systematische Erfassung der Geschäftsvorfälle und Sachverhalte;
2. der Belegnachweis für die einzelnen Buchungsvorgänge;
3. die Klarheit;
4. die Zweckmässigkeit mit Blick auf die Art und Grösse des Unternehmens;
5. die Nachprüfbarkeit.

Als Buchungsbeleg gelten alle schriftlichen Aufzeichnungen auf Papier oder in elektronischer oder vergleichbarer Form, die notwendig sind, um den einer Bu-

16. *https://www.fedlex.admin.ch/eli/cc/27/317_321_377/de*
17. *https://www.fedlex.admin.ch/eli/fga/2016/1634/de*
18. *https://www.fedlex.admin.ch/eli/cc/2002/216/de*
19. *https://www.fedlex.admin.ch/eli/cc/2016/752/de*
20. vgl. Art. 957 Abs. 2 OR
21. vgl. Art. 957 Abs. 3 OR
22. vgl. Art. 957a Abs. 1 und 2 OR

chung zugrunde liegenden Geschäftsvorfall oder Sachverhalt nachvollziehen zu können.«

Die erforderlichen Voraussetzungen, die elektronische Dokumente bzw. das Verfahren ihrer Erzeugung und Aufbewahrung im Steuerrecht erfüllen müssen, um mit Papierdokumenten gleichgestellt zu werden, sind in der Geschäftsbücherverordnung (GeBüV)[23] beschrieben. Die GeBüV ist als eine direkte Umsetzung des OR zu verstehen. Sie beschreibt die zulässigen Informationsträger und benennt die Bedingungen zur Wahrung der Integrität, der Verfügbarkeit der Dokumente und der ordnungsgemäßen Organisation.

Die auf Grundlage des MWSTG und der Verordnung vom 29.03.2000 zum Bundesgesetz über die Mehrwertsteuer (MWSTGV) erlassene Verordnung über elektronisch übermittelte Daten und Informationen (EIDI-V) hat das Eidgenössische Finanzdepartement zum 1.1.2018 abgeschafft. Damit sind ähnlich wie in der EU die Anforderungen der qualifizierten Signatur von Belegen weggefallen; es gelten nur noch OR und GeBüV.

Die Wahrung der Integrität und Authentizität bei einem Datenträgerwechsel von Dokumenten, die der GeBüV zuzuordnen sind, ist im 4. Abschn. GeBüV, i. B. im Art. 10 GeBüV geregelt. Danach können Daten in andere Formate oder auf andere Informationsträger übertragen werden, wenn sichergestellt wird, dass die Vollständigkeit und Richtigkeit der Informationen gewährleistet bleiben und die Verfügbarkeit und Lesbarkeit den gesetzlichen Anforderungen weiterhin genügen.[24]

Auch in der Schweiz werden zur umfänglichen Erfüllung der GeBüV Dokumentationen gefordert.[25] Dabei konzentrieren sich die Forderungen gemäß GeBüV schwerpunktmäßig auf die Dokumentation der Arbeitsorganisation. Eine gesetzliche Vorgabe zur Struktur der Verfahrensdokumentation ist nicht gegeben. Jedoch wird empfohlen, die Strukturvorgabe (siehe Kapitel 3.10) gemäß den deutschen GoBD als Grundlage auch in der Schweiz zu verwenden. Diese dürften vollumfänglich den Dokumentationsanforderungen gemäß GeBüV genügen.

Seit 01.01.2005 ist das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) in Kraft, das die seit dem Jahr 2000 bestehende Zertifizierungsdiensteverordnung (ZertDV) ablöste. Es regelt die Voraussetzungen, unter denen die Anbieter von Zertifizierungsdiensten im Bereich der elektronischen Signatur anerkannt werden, sowie die Rechte und Pflichten der Anbieter. Die detaillierte Umsetzung des ZertES erfolgte zeitgleich mit der Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES).

Mit Erlass des ZertES wurde der Artikel 14 OR wie folgend ergänzt: »Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signa-

23. Verordnung über die Führung und Aufbewahrung von Geschäftsbüchern vom 24.04.2002
24. vgl. Art. 10 Abs. 2 GeBüV
25. vgl. Art. 4 GeBüV V

tur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003 über die elektronische Signatur beruht. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten.«[26] Wie in der EU wird dies oft als Hindernis für die Digitalisierung betrachtet, da in vielen Fällen auch eine fortgeschrittene elektronische Signatur dem Sicherheitsbedürfnis Rechnung tragen würde oder eine Rückstufung der Formerfordernisse zu niedrigeren Formvorschriften sinnvoll wäre.[27]

Es gibt nach ZertES folgende Stufen von elektronischen Signaturen:

- **(einfache) elektronische Signatur**
  Diese Daten sind keiner Person zugeordnet und ermöglichen daher keine Identifizierung von Personen.
- **fortgeschrittene elektronische Signatur (Art. 2 Bst. b ZertES)**
  Dies ist eine elektronische Signatur, die folgende Anforderungen erfüllt:
  1. Sie ist ausschließlich der Inhaberin oder dem Inhaber zugeordnet,
  2. sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers,
  3. sie wird mit Mitteln erzeugt, die die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann,
  4. sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

  Wenn die fortgeschrittene Signatur unter Verwendung einer sicheren Signaturerstellungseinheit erstellt wurde und auf einem gültigen Zertifikat beruht, wird diese als geregelte elektronische Signatur (Art. 2 Bst. c ZertES) bezeichnet.
- **qualifizierte elektronische Signatur (Art. 2 Bst. e ZertES)**
  Ein qualifiziertes Zertifikat darf nur auf eine natürliche Person ausgestellt werden und muss einen Eintrag enthalten, wonach es nur für die elektronische Signatur bestimmt ist (Art. 8 Abs. 1 und 2 ZertES). Zudem ist der Hinweis ins Zertifikat aufzunehmen, dass es sich um ein qualifiziertes Zertifikat handelt (Art. 8 Abs. 3 ZertES). Die qualifizierte elektronische Signatur hat im Grundsatz dieselben Eigenschaften wie die fortgeschrittene elektronische Signatur nach Art. 2 Bst. b ZertES, muss jedoch unter Verwendung einer sicheren Signaturerstellungseinheit nach Art. 6 ZertES erstellt werden und beruht auf einem qualifizierten Zertifikat.
- **geregeltes elektronisches Siegel (Art. 2 Bst. d ZertES)**
  Das entsprechende Zertifikat wird nicht auf den Namen einer Person, sondern auf den Namen einer Organisation (Behörde, Unternehmen usw.) ausgestellt.

---

26. Art. 14 Abs. 2bis OR
27. Simon Roth, Die Schriftlichkeit im Privatrecht: Ein Hindernis zur Digitalisierung, *https://www.lexfutura.ch/was-uns-gerade-beschaeftigt/artikel/die-schriftlichkeit-im-privatrecht-ein-hindernis-zur-digitalisierung/*

Diese Regelungen entsprechen fast vollständig den Regelungen der eIDAS-Verordnung der EU.

3.1.2 Konkretes Beispiel: Elektronische Rechnung

In Deutschland wurden diese allgemeinen Grundsätze ganz aktuell am Beispiel der elektronischen Rechnung durch die »Vereinfachung der elektronischen Rechnungsstellung zum 1. Juli 2011 durch das Steuervereinfachungsgesetz 2011« wie folgt konkretisiert:

Durch die Neufassung des § 14 Abs. 1 und 3 UStG durch den Art. 5 Nr. 1 des Steuervereinfachungsgesetzes 2011 vom 01. November 2011 sind die umsatzsteuerrechtlichen Regelungen für elektronische Rechnungen zum 01. Juli 2011 neu gefasst worden. Eine elektronische Rechnung ist nach § 14 Abs. 1 Satz 8 UStG n.F. eine Rechnung, die in einem elektronischen Format ausgestellt und empfangen wird. Die Anforderungen an die Übermittlung elektronischer Rechnungen sind gegenüber der bisherigen Rechtslage deutlich reduziert. Nunmehr können u.a. auch Rechnungen, die per E-Mail (ggf. mit Bilddatei- oder Textdokumentanhang) übermittelt werden, zum Vorsteuerabzug berechtigen.

Bisher wurden auf elektronischem Wege übermittelte Rechnungen umsatzsteuerrechtlich nur anerkannt, wenn eine qualifizierte elektronische Signatur (§ 14 Abs. 3 Nr. 1 UStG a.F.) oder ein EDI-Verfahren (§ 14 Abs. 3 Nr. 2 UStG a.F.) verwendet wurden. Dies entsprach den europarechtlichen Regelungen nach Art. 233 Abs. 1 Satz 1 Buchstabe a und b und Abs. 2 MwStSystRL. Der Gesetzgeber hat nunmehr von der Option nach Art. 233 Abs. 1 Satz 2 MwStSystRL Gebrauch gemacht, die es den Mitgliedsstaaten freistellt, auch Rechnungen anzuerkennen, die auf andere Weise elektronisch übermittelt oder bereitgestellt werden.

In Anlehnung an Art. 233 MwStSystRL in der ab dem 01. Januar 2013 geltenden Fassung (Änderung durch die Richtlinie 2010/45/EU des Rates zu den Rechnungsstellungsvorschriften vom 13. Juli 2010, AB1. EU 2010 L 189 Seite 1) sind Papier- und elektronische Rechnungen ab dem 01. Juli 2011 umsatzsteuerrechtlich gleich zu behandeln (§ 14 Abs. 1 UStG n.F.). Die Gleichstellung führt zu keiner Erhöhung der Anforderungen an die Ordnungsmäßigkeit einer Papierrechnung.

Sowohl bei Papier- als auch bei elektronischen Rechnungen müssen nach § 14 Abs. 1 UStG n.F. die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet werden. Dies kann durch jegliche innerbetriebliche Kontrollverfahren erreicht werden, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung herstellen können. § 14 Abs. 3 Nr. 1 und 2 UStG n.F. nennt deshalb die qualifizierte elektronische Signatur oder die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung nach dem Signaturgesetz und den elektronischen Datenaustausch (EDI) nach Artikel 2 der Empfehlung 94/820/EG der Kommission vom 19. Oktober 1994 über die rechtlichen

Aspekte des elektronischen Datenaustauschs (AB1. EG 1994 L 338 Seite 98) nur noch als Beispiele für Technologien, die die Echtheit der Herkunft und die Unversehrtheit des Inhalts einer elektronischen Rechnung gewährleisten. Der Vorteil seit der Abschaffung der Signaturpflicht ist, dass bei Verwendung dieser Technologien nach § 14 Abs. 3 UStG ein Anscheinsbeweis für die Echtheit und Unversehrtheit des Dokuments spricht, aber gleichzeitig die Anforderungen der ehemaligen GdPdU auf Empfängerseite weggefallen sind. Dies entspricht Art. 233 Abs. 2 MwStSystRL in der Fassung der Richtlinie 2010/45/EU des Rates zu den Rechnungsstellungsvorschriften vom 13. Juli 2010, a.a.O.

Das innerbetriebliche Kontrollverfahren im Sinne des § 14 Abs. 1 UStG n.F. dient nicht dazu, die materiell-rechtlichen Voraussetzungen des Vorsteuerabzugs nach § 15 UStG zu überprüfen. Ebenso wenig soll die inhaltliche Ordnungsmäßigkeit der Rechnung hinsichtlich der nach §§ 14 Abs. 4, 14a UStG erforderlichen Angaben gewährleistet werden. Mit dem innerbetrieblichen Kontrollverfahren soll lediglich die korrekte Übermittlung der Rechnungen sichergestellt werden. Eine inhaltlich richtige Rechnung (gemeint: richtige Leistung, richtiger Leistender, richtiges Entgelt, richtiger Zahlungsempfänger) rechtfertigt die Annahme, dass bei der Übermittlung keine die Echtheit der Herkunft oder die Unversehrtheit des Inhalts beeinträchtigenden Fehler vorgekommen sind. Das heißt, die Rechnung wurde weder ge- noch verfälscht oder auf andere Weise verändert; die Rechnung entspricht der erbrachten Leistung. Die Anforderungen an das innerbetriebliche Kontrollverfahren haben sich an dieser Zielrichtung zu orientieren.

In der Praxis werden sich die Durchführung des Kontrollverfahrens und die Prüfung der Voraussetzungen des Vorsteuerabzuges in Teilen überschneiden. Ist der Nachweis erbracht, dass die Voraussetzungen des Vorsteuerabzuges nach § 15 UStG gegeben sind, kommt der Frage der Durchführung des innerbetrieblichen Kontrollverfahrens in dem konkreten Einzelfall keine eigenständige Bedeutung mehr zu und kann insbesondere nicht mehr zur Versagung des Vorsteuerabzuges führen.

Unter innerbetrieblichen Kontrollverfahren im Sinne des § 14 Abs. 1 UStG n.F. sind Verfahren zu verstehen, die der Unternehmer zum Abgleich der Rechnung mit seinen Zahlungsverpflichtungen einsetzt. Der Unternehmer ist in der Wahl des Verfahrens frei. Er wird im eigenen Interesse insbesondere überprüfen, ob

- die Rechnung in der Substanz korrekt ist, d.h. ob die in Rechnung gestellte Leistung tatsächlich in dargestellter Qualität und Quantität erbracht wurde,
- der Rechnungsaussteller also tatsächlich den behaupteten Zahlungsanspruch hat,
- die vom Rechnungssteller angegebene Kontoverbindung korrekt ist und Ähnliches,

um zu gewährleisten, dass er tatsächlich nur die Rechnungen begleicht, zu deren Begleichung er auch verpflichtet ist.

Ein innerbetriebliches Kontrollverfahren erfüllt die Anforderungen des § 14 Abs. 1 UStG n.F., wenn es einen verlässlichen Prüfpfad gibt, durch den ein Zusammenhang zwischen der Rechnung und der zugrunde liegenden Leistung hergestellt werden kann. Dies kann im Rahmen eines entsprechend eingerichteten Rechnungswesens erfolgen, aber z.B. auch durch einen manuellen Abgleich der Rechnung mit vorhandenen geschäftlichen Unterlagen (z.B. Kopie der Bestellung, Auftrag, Kaufvertrag, Lieferschein, Überweisungs- oder Zahlungsbeleg). Es werden keine technischen Verfahren vorgegeben, die die Unternehmen verwenden müssen. Das innerbetriebliche Kontrollverfahren unterliegt keiner gesonderten Dokumentationspflicht. Allerdings ist der Steuerpflichtige nach wie vor verpflichtet, die Voraussetzungen des geltend gemachten Vorsteuerabzuges nachzuweisen.

Papier- und elektronische Rechnungen sind nach § 14 UStG zehn Jahre aufzubewahren. Während des gesamten Aufbewahrungszeitraums müssen die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet werden (§ 14 Abs. 1 Satz 2 UStG n.F.).

Die beweisrechtlichen Anforderungen an elektronische Rechnungen waren in den letzten Jahrzehnten erheblichen Schwankungen ausgesetzt, wie Abbildung 3–2 verdeutlichen soll:

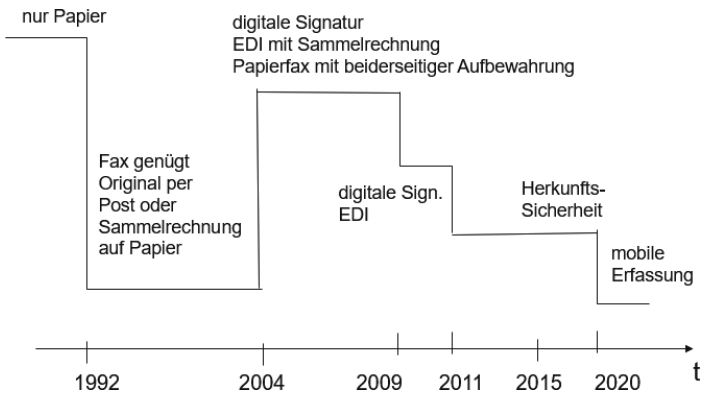

Abb. 3–2 *Beweisrechtliche Anforderungen an Rechnungen*

Für die Bewertung der Anforderungen sind die GoBD in der Fassung seit 1.1.2020 maßgebend.

Für den Austausch von elektronischen Rechnungen wurden verschiedene Dokumentformate entwickelt.

Die EU hat bereits 2014 die E-Rechnungsrichtlinie[28] erlassen, die in den Mitgliedsstaaten die Akzeptanz von elektronischen Rechnungen durch öffentliche Auftraggeber verlangt. Dabei sind zwei verschiedene XML-Standards erlaubt:

28. Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen, *https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32014L0055*

- der von der UN-Organisation UN-CEFACT entwickelte *Cross Industry Invoice Standard* (standardisiert als EN 16931) und
- der von der Organization for the Advancement of Structured Information Standards entwickelte Standard *Universal Business Language*, ISO/IEC 19845:2015.

In Deutschland wurde die Richtlinie durch das E-Rechnungsgesetz[29] umgesetzt. Hier wurde der Standard *XRechnung* durch die zugehörige E-Rechnungsverordnung für Rechnungen an öffentliche Auftraggeber über einem Betrag von 1000 Euro festgelegt.

Die elektronische Rechnung hat neben den umsatzsteuerrechtlichen Rechnungsbestandteilen nach § 5 E-Rechnungsverordnung mindestens folgende Angaben zu enthalten:

1. eine Leitweg-Identifikationsnummer,
2. die Bankverbindungsdaten,
3. die Zahlungsbedingungen und
4. die De-Mail-Adresse oder eine E-Mail-Adresse des Rechnungsstellers.

Die elektronische Rechnung hat zusätzlich zu den Angaben nach Absatz 1 folgende Angaben zu enthalten, wenn diese dem Rechnungssteller bereits bei Beauftragung übermittelt wurden:

1. die Lieferantennummer,
2. eine Bestellnummer.

Das *Forum elektronische Rechnung Deutschland* (FeRD) wurde von der *Arbeitsgemeinschaft für wirtschaftliche Verwaltung* unter Beteiligung zahlreicher Institutionen aus Ministerien, Verwaltungen, Hochschulen, Verbänden und Firmen gegründet. Dieses Forum hat ein Hybridformat namens ZUGFerD (*Zentraler User Guide des Forums elektronische Rechnung Deutschland*) entwickelt, das aus einem maschinenlesbaren Teil im XML-Format und einem menschenfreundlichen Teil im PDF-Format besteht. Nach Inkrafttreten der E-Rechnungsrichtlinie wurde dieses Format überarbeitet. Jetzt gibt es insgesamt vier Profile dieses Formats:

- ZUGFeRD 2.0 – Teil 1: Profil EN 16931 (RL-compliant)
- ZUGFeRD 2.0 – Teil 2: Profil Extended
- ZUGFeRD 2.0 – Teil 3: Profil Basic
- ZUGFeRD 2.0 – Teil 4: Profil Buchungshilfe

29. *https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s0770.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s0770.pdf%27%5D__1670424102407*

Seit Version 2.0 entspricht der Teil 1 der Spezifikation der E-Rechnungsrichtlinie und dem deutschen E-Rechnungsgesetz. Dieser wird in Frankreich als *FACTURX*-Standard bezeichnet. Bei Verwendung des Hybridformats ist es erforderlich, dass der Steuerpflichtige entweder das XML-[30] oder das PDF-Format[31] als steuerrechtlich relevant festlegt.

3.2 Datenschutz und Datensicherheit

Daten und Dokumente sind wichtige Ressourcen eines Unternehmens. In vielen Fällen sind sie die einzigen Nachweise für die Erfüllung der Pflichten, die sich aus den Handlungen, Abläufen und Produkten eines Unternehmens oder einer Institution ergeben. Datenschutz und Datensicherheit gehören eng zusammen, da Datenschutz nur mit technischen Sicherheitsmaßnahmen gewährleistet werden kann.

Die Datenschutzrichtlinie 95/46/EG von 1995 unternahm erstmals den Versuch, das Datenschutzrecht in der Europäischen Union zu harmonisieren, und seit dem 25. Mai 2018 gibt es mit der Datenschutz-Grundverordnung (DSGVO)[32] ein einheitliches Datenschutzrecht in der ganzen Europäischen Union. Daneben gibt es lediglich in Deutschland und Österreich noch nationale Datenschutzgesetze, in denen aber lediglich Ausnahmen zur DSGVO bzw. der parallel erlassenen Datenschutz-Richtlinie für Justiz und Inneres[33] enthalten sind.

Grundlage des Datenschutzes sind für Unternehmen mit Sitz in Deutschland und öffentliche Stellen des Bundes die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz (BDSG), für öffentliche Stellen der Länder die Datenschutz-Grundverordnung und das jeweilige Landesdatenschutzgesetz. Darüber hinaus gibt es in einzelnen Rechtsgebieten weitere Datenschutzregelungen, wie z.B. den Sozialdatenschutz nach den §§ 67 bis 85a SGB X oder den Telekommunikations- und Telemediendatenschutz im TTDSG.

Daten sind **personenbezogen**, wenn Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, d.h. einem betreffenden Menschen, zugeordnet werden können. Dies gilt nach einem Urteil des Europäischen Gerichtshofes[34] nur dann, wenn der Empfänger der Daten aus eigener Kraft diese Personenzuordnung vornehmen kann, d.h. entweder selbst oder mithilfe eines Gerichtes. Weiter gehören dazu auch technische Daten, z.B. IP-Adressen, Accountnamen oder MAC-Adressen, wenn eine Zuordnung dieser Daten zu einer Person gegeben ist. Bei dynamisch vergebenen IP-Adressen gilt dies nur so lange, wie die Zuordnungsdaten noch vorhanden sind (z.B. DHCP-Tabellen).

30. EN 16937
31. Version PDF-A/3, ISO 19005-3
32. EU-Verordnung 2016/679, Amtsblatt L 119/1 der EU vom 4.5.2016
33. EU-Richtlinie 2016/680, Amtsblatt L 119/89 der EU vom 4.5.2016
34. EuGH, C-582/14 vom 19.10.2016