Bundesministerium
für Wirtschaft
und Technologie

Dokumentation
Nr. 564

Dokumentation

Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente

www.bmwi.de

Text und Redaktion

Prof. Dr. jur. Alexander Roßnagel, RA Dr. rer. pol. Stefanie Fischer-Dieskau, Ass. jur. Silke Jandt
Universität Kassel

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)

Praxisbezogene Darstellung der Ergebnisse des vom Bundesministerium für Wirtschaft und Technologie geförderten Forschungsprojekts „Anforderungen und Trends der Langzeitaufbewahrung (ATLA§)“ für Hersteller und Nutzer elektronischer Archivierungssysteme

Produktion/Druck
Harzdruckerei Wernigerode GmbH

Herausgeber
Bundesministerium für
Wirtschaft und Technologie
Referat P3/Öffentlichkeitsarbeit
10115 Berlin
www.bmwi.de

Stand
August 2007

Bundesministerium
für Wirtschaft
und Technologie

Dokumentation

Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente

Vorwort

Der Übergang vom Papier zum elektronischen Dokument schreitet schnell voran. Die elektronische Abwicklung von Geschäftsprozessen resultiert vor allem in Zeit- und Kostenvorteilen. Im Verwaltungswie auch im Unternehmensbereich wird das Aufkommen elektronischer und elektronisch signierter Dokumente in den kommenden Jahren drastisch zunehmen. Nicht zu übersehen sind dabei erforderliche Lösungen für die rechtssichere Aufbewahrung solcher Dokumente, in Analogie zur Papierform. Grundlage sind gesetzliche Regelungen aber auch die eigene Nachweissicherung zur Vermeidung rechtlicher Nachteile. Neue Marktperspektiven im Bereich elektronischer Archivsysteme und Archivdienstleistungen gehören zu den damit verbundenen Chancen auf der Anbieterseite.

Mit dem Technologieprojekt „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ hatte das Bundesministerium für Wirtschaft und Technologie diese Thematik erstmals aufgegriffen. Die Ergebnisse dieser Initiative sind viel beachtet und bilden den Anker für weitergehende Entwicklungen und bereits in die Praxis eingeführte kommerzielle Lösungen.

Der vorliegende Handlungsleitfaden ist das Ergebnis einer vom BMWi im Zusammenhang mit ArchiSig und dem Folgeforschungsprojekt „TransiDoc – Rechtssichere Transformation digital signierter Dokumente“ geförderten Studie zu „Anforderungen und Trends der langfristigen Aufbewahrung (Atla§)“ von elektronischen Dokumenten, die im Jahr 2006 abgeschlossen wurde, und die eine ausführliche Übersicht und Bewertung zur rechtlichen, branchen- und anwendungsspezifischen Erfordernissen elektronischer Archivierung gibt. Der Handlungsleitfaden wurde für die Praxis entwickelt und richtet sich an Hersteller und Nutzer entsprechender Systeme.

Michael Glos
Bundesminister für Wirtschaft und Technologie

Vorwort der Verfasser

Der Umfang elektronischer Dokumente hat in den letzten Jahren in allen Bereichen sehr stark zugenommen. Unternehmen und Verwaltungen müssen die elektronischen Dokumente aufgrund rechtlicher Vorgaben zum Teil sehr lange aufbewahren, vor allem um Beweismittel zu sichern. Daneben dient die Aufbewahrung der Gedächtnisstütze und Kommunikationshilfe, der Durchführung von Kontrollen und Rechenschaften sowie dem Erhalt der Dokumente für die Nachwelt. Um diese Ziele zu erreichen, müssen elektronische Dokumente nicht nur langfristig verfügbar sowie trotz der technischen Weiterentwicklung lesbar, sondern auch nachweisbar unverändert und einem bestimmten Autor zurechenbar sein.

Der vorliegende Handlungsleitfaden geht auf die beiden Studien „ATLA§ – Anforderungen und Trends der langfristigen Aufbewahrung“ elektronischer Dokumente und „SCATE – Scannen – Anforderungen, Trends, Empfehlungen“ zurück, die im Rahmen der vom Bundesministerium für Wirtschaft und Technologie geförderten Technologieprojekte „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ und „TranisDoc – Rechtssichere Transformation digital signierter Dokumente“ entstanden sind.

Der Handlungleitfaden konzentriert sich auf die speziellen Probleme, die bei der Ausgestaltung und dem Betrieb elektronischer Archivsysteme auftreten. Dabei werden insbesondere die rechtlichen Anforderungen berücksichtigt, die sich aus der Beachtung der jeweiligen Aufbewahrungszwecke ergeben. Die gesetzlichen Vorgaben werden durch die Bewertung und Auswahl der zur Verfügung stehenden technischen Sicherungsmittel umgesetzt.

Für die anregenden Diskussionen, die zahlreichen Hinweise und die vielfältige Unterstützung bei der Erstellung des Handlungsleitfadens gilt unser herzlicher Dank den Mitgliedern des von uns gegründeten Beirats: Dr. Astrid Albrecht (Bundesamt für die Sicherheit in der Informationstechnik), Dr. Boris Baltzer (IBM), Jürgen Ewald (Datev), Dr. Dominik Gassen (Notarnet), Dr. Siegfried Hackel (Physikalisch-Technische Bundesanstalt), Dr. Christian Mrugalla (Bundesministerium des Innern), Roland Müller (Pro Dokument), Udo Polaszek (Landesversicherungsamt Nordrhein-Westfalen), Prof. Dr. Paul Schmücker (Hochschule Mannheim), Dr. Christoph Seidel (Klinikum Braunschweig), Norbert Thiel (Opentext), Dr. Wolfgang Viefhues (Oberlandesgericht Düsseldorf), Dr. Roland Wirth (Arbeitsgemeinschaft für wirtschaftliche Verwaltung – AWV).

Kassel, im August 2007

Alexander Roßnagel
Stefanie Fischer-Dieskau
Silke Jandt

Inhalt

1. Zielsetzung des Leitfadens

Darf und kann ich auf eine rein elektronische Aufbewahrung vertrauen – ist eine oft gestellte Frage.[1] Der Wechsel von einer papierbasierten zu einer elektronischen Aufbewahrung ist so grundlegend, dass gerade in den Anwendungsbereichen, in denen dem Papier eine herausragende Bedeutung zukommt, viele Unsicherheiten bestehen.

Dieser Handlungsleitfaden zur Aufbewahrung elektronischer Dokumente[2] bietet Hilfestellungen für alle Bereiche der Wirtschaft, Verwaltung und Justiz. Er bietet Hinweise für die Ausgestaltung der Aufbewahrung elektronischer Dokumente und die Wahl elektronischer Archivsysteme, bestehend aus Hard- und Software. Er enthält kein Patentrezept mit konkreten Antworten auf das Ob und das Wie der elektronischen Aufbewahrung in jedem Einzelfall. Der Leitfaden soll den Leser in die Lage versetzen, nicht nur die wesentlichen Fragen hinsichtlich der Art und Weise der elektronischen Aufbewahrung aufzuwerfen, sondern ihm auch Anhaltspunkte für das Finden geeigneter Antworten geben. Um diese Ziele zu erreichen, zeigt der Leitfaden auf, welche Rahmenbedingungen bei der elektronischen Aufbewahrung und der Wahl geeigneter Systeme für eine elektronische Aufbewahrung zu beachten und welche organisatorischen und technischen Lösungen einzusetzen sind.

Zur Info: Rechtlich ist der Begriff der Aufbewahrung von dem der Archivierung zu unterscheiden. Die Aufbewahrung umfasst jede Form der Erhaltung eines Dokuments – unabhängig davon, ob aus informationstechnischer Sicht eine Speicherung im Datenmanagementsystem oder im Datenarchiv erfolgt, ob der Gesamtvorgang, zu dem das einzelne Dokument gehört, in der Bearbeitung abgeschlossen ist oder nicht oder ob eine bestimmte Aufbewahrungsdauer festgelegt ist. Die Archivierung im juristischen Kontext betrifft allein Unterlagen der öffentlichen Verwaltung. Von „Archivgut“ wird dort erst dann gesprochen, wenn das Schriftgut bei der zuständigen Behörde ausgesondert, vom Archiv als archivwürdig eingestuft worden ist und „ewig“ verwahrt wird. Der Leitfaden betrifft allein die Aufbewahrung. Sofern allerdings Bezug auf technische Systeme genommen wird, wird am etablierten Begriff des Archivsystems festgehalten.

Der Leitfaden richtet sich an Anwender und Hersteller von elektronischen Archivsystemen. Die Anwender können anhand des Umsetzungskonzepts des Leitfadens den Bedarf und die konkrete Ausgestaltung eines elektronischen Archivsystems bestimmen. Die Hersteller der Archivsysteme können ihr Angebot unter Berücksichtigung des Leitfadens spezifizieren.

Beachte: Dieser Leitfaden setzt sich nur mit der Aufbewahrung elektronischer Dokumente auseinander. Die Frage der Transformation von Papierdokumenten in die elektronische Form bleibt in diesem Leitfaden außer Betracht.

Der Leitfaden ist nach den Schritten aufgebaut, die der Planer eines Archivsystems gehen muss, um die Frage zu beantworten, wie er ein Archiv für elektronische Dokumente auswählen und gestalten soll.

[1] Bei diesem Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente handelt es sich um eine Empfehlung ohne rechtsverbindlichen Charakter.

[2] Eine vertiefte Behandlung des Themas ist in Roßnagel/Fischer-Dieskau/Jandt/Knopp, Die langfristige Aufbeweahrung elektronischer Dokumente, Nomos Verlag, Baden-Baden 2007, zu finden. Fragen zur Zulässigkeit und Ausgestaltung des Scannens werden in der Studie „Scate – Scannen: Anforderungen, Trends, Empfehlungen“ untersucht.

2. Grundlagen zur Aufbewahrung elektronischer Dokumente

Die nationale Rechtsordnung kennt kein anwendungsübergreifendes „Aufbewahrungsgesetz“, aus dem einheitliche Fristen und Anforderungen an die Aufbewahrung entnommen werden können. Die gesetzlichen Dokumentations- und Aufbewahrungspflichten finden sich verteilt in verschiedenen Gesetzen.

Zur Info: Dokumentations- und Aufbewahrungspflichten sind immer im Zusammenhang zu sehen, denn die einen bedingen die anderen. Die Aufbewahrung ist der „verlängerte Arm“ der Dokumentation. Anforderungen an die Aufbewahrung können einen Einfluss auf die Anforderungen an die Dokumenterstellung haben. Mag das Aufbewahrungssystem noch so gut und sicher ausgestaltet sein, die Unveränderbarkeit eines Dokuments, das in einer Form erstellt worden ist, die keinen Integritätsschutz gewährleistet, kann erst ab dem Zeitpunkt eindeutig festgestellt werden, ab dem es in das Aufbewahrungssystem eingestellt worden ist. Ein Aufbewahrungssystem kann somit nicht Mängel aus der Zeit der Dokumenterstellung beheben. Insbesondere auf die Erstellung von Dokumenten durch Dritte kann grundsätzlich kein Einfluss genommen werden. Entsprechen sie nicht den eigenen Anforderungen, sollten sie – soweit möglich – mit der Bitte zurückgewiesen werden, ein neues, den Anforderungen entsprechendes Dokument zu schicken.

Pflichten zur Aufbewahrung sind anwendungs- oder gar dokumentspezifisch geregelt. Sie verweisen oft auf die allgemeine Übung in einem Bereich oder Standards einer Berufsgruppe. Paradebeispiele für anwendungsspezifische Aufbewahrungspflichten sind die Vorschriften über die Erfüllung und den Nachweis einer ordnungsgemäßen Buchführung. Welche konkreten Dokumentarten zur Erfüllung der Buchführungspflicht erstellt und aufbewahrt werden müssen, ergibt sich nur teilweise aus den handels- und steuerrechtlichen Vorschriften. Ein weiteres Beispiel enthält die Musterberufsordnung für Ärztinnen und Ärzte. Deren § 10 bezeichnet mit der Pflicht zur „ärztlichen Dokumentation“ die Zielsetzung der Dokumentation und Aufbewahrung. Die konkreten Dokumentarten ergeben sich nicht aus der Vorschrift, sondern aus einer konkretisierenden Auslegung mit Blick auf die gängige Praxis.

Ein Teil der gesetzlichen Aufbewahrungspflichten knüpft unmittelbar an eine konkrete Dokumentart an, wie zum Beispiel § 14 Abs. 4 UStG an die elektronischen Rechnungen. Daher folgt aus der Einordnung eines Dokuments in eine bestimmte Dokumentart unmittelbar, welche Dokumente verpflichtend aufzubewahren sind, um den gesetzlichen Aufbewahrungspflichten umfassend Genüge zu tun. Bereits an dieser Stelle sei darauf hingewiesen, dass Gegenstand der Aufbewahrung neben Dokumenten ebenfalls Daten (auf diese nimmt beispielsweise die Abgabenordnung Bezug) und Akten (auf die sich zum Beispiel § 298a ZPO bezieht) sein können.

Definitionen:

- Dokument: Alle Arten von Informationen, die zur Wahrnehmung durch den Menschen bestimmt sind und als Einheit zwischen Systemen oder Benutzern ausgetauscht werden können. Bei elektronischen Dokumenten sind die Informationen maschinell lesbar und verarbeitbar und werden als Daten bezeichnet.
- Daten: Oberbegriff für alle Informationen, die von elektronischen Medien verarbeitet oder gespeichert werden.
- Akte: Zusammenstellung von sachlich zusammengehörigen Dokumenten, die als Einheit behandelt und zitiert werden, in der Regel mit dem Aktenzeichen.
- Dokumentart: Abstrakte Bezeichnung eines Dokuments in Bezug auf seinen Inhalt, z.B. der Arztbrief.
- Dokumentkategorie: Anwendungsspezifische Bezeichnung einer nicht konkretisierten Anzahl und Art von Dokumenten, die zur Erfüllung einer bestimmten Funktion erforderlich sind, z.B. die ärztliche Dokumentation.

Die Dokumentkategorie erfährt eine Konkretisierung durch die Benennung der erforderlichen Dokumentarten, zum Beispiel besteht die ärztliche Dokumentation unter anderem aus dem Arztbrief, der Patientenkartei und EKG-Aufzeichnungen.

Jede Aufbewahrung verfolgt immer einen oder mehrere Zwecke. Folgende Aufbewahrungszwecke lassen sich unterscheiden:

Zweck	Erklärung
Gedächtnisstütze und Kommunikationshilfe	Informationen und Wissen über bestimmte Vorgänge werden unabhängig von dem begrenzten Erinnerungsvermögen des Menschen für die Zukunft erhalten und können einer Vielzahl von Personen zugänglich gemacht werden.
Sicherung der Beweisführung	Schriftliche Perpetuierung von Vereinbarungen, einseitigen Wissens- oder Willenserklärungen, um für die Zukunft die Gewissheit zu haben, einen Sachverhalt im Rechtsstreit nachweisen zu können.
Kontrollen und Rechenschaftslegung	Transparente und nachvollziehbare Aufzeichnung der ordnungsgemäßen Durchführung einer gesetzlich geforderten Handlung für einen Dritten. Bei der Kontrolle findet eine selbständige Überprüfung durch den Dritten statt, während bei der Rechenschaftslegung der Verpflichtete dem Dritten Auskunft erteilt.
Archivgut für die Nachwelt	Dokumente mit einem bleibenden inhaltlichen Wert werden für die Nachwelt dauerhaft erhalten.

Zur Info: Je nachdem welche Zwecke mit der Aufbewahrung und Dokumentation verfolgt werden, wird ein überwiegendes Interesse des Aufbewahrenden selbst (Eigeninteresse) oder dritter Personen (Fremdinteresse) angenommen. In manchen Anwendungsbereichen sieht der Gesetzgeber die Verfolgung der Zwecke als zwingend an und hat daher zur ihrer Durchsetzung Aufbewahrungs- und mit ihnen immer einhergehende Dokumentationspflichten normiert. Gesetzliche Aufbewahrungspflichten sind das Ergebnis einer Abwägung unterschiedlicher Interessen an dem Vorliegen und Erhalt einer Dokumentation. Die Interessen Dritter werden als so gewichtig angesehen, dass zu ihrem Schutz eine Aufbewahrungspflicht festgelegt ist.

Sofern keine gesetzlichen Aufbewahrungspflichten bestehen, kann eine Aufbewahrung aus Gründen der Beweissicherung oder zur Gedächtnisstütze, somit allein zur Wahrung eigener Interessen, sinnvoll sein.

Beachte: Die Aufbewahrung allein im eigenen Interesse ist zwar für den Aufbewahrenden freiwillig, nicht aber für die Personen, die für ihn handeln. Entscheidet etwa ein Vorstand oder eine Geschäftsführung für ein Unternehmen oder ein Behördenleiter für eine Behörde, besteht zwar weder für das Unternehmen noch für die Behörde eine Aufbewahrungspflicht. Vorstand, Geschäftsführer und Behördenleiter würden jedoch ihre Pflicht verletzen, wenn sie – trotz fehlender Rechtspflicht – auf entscheidende Gedächtnisstützen oder Beweismittel bewusst oder nachlässig verzichten, deren Fehlen dem Unternehmen oder der Behörden Nachteile bereiten können. Erleidet das Unternehmen oder die Behörde dadurch einen Schaden, haften diese Personen für diesen.

Zum Beispiel sollte der Arbeitgeber Vertraulichkeitsvereinbarungen über den Umgang mit Betriebsgeheimnissen aufheben. Bei einem Rechtsstreit über die Einhaltung dieser Pflicht, kann die Vorlage dieses Dokuments für den Ausgang des Prozesses entscheidend sein. Eine Aufbewahrung des Dokuments im eigenen Interesse ist daher zu empfehlen.

3. Prüfungsschritte

Die Auswahl eines elektronischen Aufbewahrungssystems kann strukturiert auf Basis einer „Zwei-Schritt-Analyse“ erfolgen:

- Welche Dokumente müssen aufgrund gesetzlicher Verpflichtung oder sollen aus eigenem Interesse aufbewahrt werden?
- Mit welchen Sicherungskomponenten muss oder soll das Aufbewahrungssystem ausgestattet sein?
  - Welche Anforderungen müssen bei der Aufbewahrung beachtet werden?
  - Welche Sicherungsmittel sind geeignet, die Anforderungen zu erfüllen?

3.1 Erster Prüfungsschritt – Notwendigkeit der Aufbewahrung

Bestehen gesetzliche Aufbewahrungspflichten, müssen die entsprechenden elektronischen Dokumente in dem Archivsystem aufbewahrt werden. Sofern, zum Beispiel in einer internen Arbeits- oder Dienstanweisung, bereits eine Zusammenstellung besteht, welche Dokumente zwingend in den Papierarchiven aufzubewahren waren, so kann diese weiterverwendet werden. Ansonsten ist ein Blick in die einschlägigen Gesetze erforderlich. Sind die Dokumentations- und Aufbewahrungspflichten anwendungsspezifisch, müssen die aufzubewahrenden Dokumentarten aus der Dokumentkategorie an Hand des Inhalts und der Zielsetzung der entsprechenden gesetzlichen Regelung abgeleitet werden. Sind die Dokumentations- und Aufbewahrungspflichten dokumentspezifisch ist die aufzubewahrende Dokumentart ausdrücklich in der Vorschrift bezeichnet.

In der nachfolgenden Tabelle werden – nicht abschließend! – einige Dokumentations- und Aufbewahrungspflichten, ihre rechtlichen Grundlagen und die Dokumentarten oder -kategorien aufgeführt. Sie soll einen Überblick ermöglichen und dient der Veranschaulichung der Differenzierung zwischen den Dokumentkategorien (nachfolgend in Kursivschrift) und den Dokumentarten.

Anwendungsgebiet	Aufzubewahrende Dokumentarten oder -kategorien	Rechtsgrundlage
Buchführung	- elektronische Rechungen - Handelsbücher - Handelsbriefe - Inventarverzeichnis - Eröffnungsbilanzen - Jahresabschluss - Lagebericht - Konzernabschluss - Konzernlagebericht - Arbeitsanweisungen - Organisationsunterlagen - Buchungsbelege	§§ 238 ff. HGB, §§ 140 AO, § 14b UStG
Personalsachen	- Kündigung, Auflösungsvertrag - Befristungsvereinbarung - Arbeitszeitnachweise - Lohn- und Berechnungsnachweis - Beschäftigungsverzeichnis - ärztliche Bescheinigung, Verzeichnis der Jugendlichen - Integrationsverzeichnis - Beschäftigungsverzeichnis - IOS-, EN-ISO-Normen, ASTM- Methoden - Zulassungsschein, Prüfbefunde - Wahlakten - Befristungsvereinbarung	§ 623 BGB § 2 Abs. 1 Satz 3 NachwG § 16 Abs. 2 ArbZG § 165 Abs. 4 Satz 2 SGB VII § 22 Abs. 3 LadenSchlussG, §§ 41 Abs. 1, 50 Abs. 2 JArbSchG, § 80 SGB IX, § 13 Abs. 4 Satz 1 und Satz 2 BiostoffVO, § 7 der 3. BImSchV, § 27 StrlSchVO, § 19 WO § 14 Abs. 4 TzBfG
Medizinische Dokumentation	- Ärztliche Dokumentation: z.B. Arztbrief, Patientenkartei; Medikamentenverschreibungen - Aufzeichnungen über Röntgenbehandlung: z.B. Röntgenaufzeichnungen, Röntgenbilder	Landesrechtliche Berufsordnungen für Ärzte, z.B. § 10 Abs. 3 BerufsO Ärzte Hessen § 28 Abs. 4 RöntgV
Bankunterlagen	- Vollständige Geschäftsdokumentation: vgl. HGB; z.B. Risikohandbücher - Identifizierungsunterlagen - Dokumente der Wertpapierdienstleistung: z.B. Auftrag	§ 25a Abs. 5 KWG § 9 GWG § 34 WpHG
Akten der Verwaltung	- Haushaltsplan - Haushaltsrechnung - Akten - Öffentlich-rechtliche Verträge - Öffentlich-rechtliche Verträge - Unterlagen der öffentlich-rechtlichen Verwaltungstätigkeit	§§ 33, 33a HGrG § 29 VwVfG § 57 VwVfG § 56 SGB X i.V.m. § 3a Abs. 2 VwVfG § 110a SGB IV
Gerichtsakten	- vollständige Prozessakten - Schriftgut der Bundesgerichte und der Generalstaatsanwaltschaft: z.B. Aktenregister, Namensverzeichnis, Karteien (§ 1 Abs. 2 SchrAG)	§ 298a ZPO SchriftgutaufbewahrungsG

Zur Feststellung gesetzlicher Aufbewahrungspflichten empfiehlt sich folgendes Vorgehen:

Die im Geschäfts-, Verwaltungs- oder Justizbetrieb anfallenden Dokumente sind ihrer Art und ihrer Kategorie nach zu bestimmen. Für bestimmte Dokumentarten kann unmittelbar aus der dargestellten Tabelle das Bestehen der Aufbewahrungspflicht abgelesen werden. Andere gesetzliche Aufbewahrungsvorschriften sind weniger präzise und beziehen sich lediglich auf Dokumentkategorien. In der Tabelle werden daher nur beispielhaft, aber nicht abschließend, Dokumentarten aufgeführt. Eine Aufbewahrungspflicht für weitere Dokumente ist mittelbar durch die Zuordnung in die Dokumentkategorien festzustellen. Konnten einzelne Dokumente weder einer in der Tabelle genannten Dokumentart noch -kategorie zugeordnet werden, besteht die Vermutung, dass keine gesetzliche Aufbewahrungspflicht besteht.

Wer keine dokumentspezifische Analyse vornehmen will, kann auch eine Pauschallösung wählen und grundsätzlich alle elektronischen Dokumente aufbewahren. Die Entscheidung für oder gegen eine Pauschallösung ist letztlich unter Effizienz- und Kostengesichtspunkten zu treffen. Es muss jedoch immer sichergestellt werden, dass die aufgrund gesetzlicher Pflichten oder aufgrund von Eigeninteressen aufzubewahrenden Dokumente erhalten bleiben. Zu beachten ist außerdem, dass eine Differenzierung aus anderen Gründen erforderlich sein kann: So können unterschiedliche Systeme erforderlich sein, um den Daten- und Geheimnisschutz zu wahren oder um den Zugriff Dritter auf bestimmte Daten zu ermöglichen. Die Aufbewahrung muss in einer transparenten und geordneten Struktur erfolgen, um ein Wiederauffinden der Dokumente zu gewährleisten.

Beachte: Die Verletzung von Aufbewahrungspflichten kann straf- und berufsrechtliche, aber auch prozessuale Konsequenzen haben.
Beispiele:
Die Verletzung der handelsrechtlichen Buchführungspflicht kann eine Insolvenzstraftat nach §§ 283 ff. StGB darstellen.
Gemäß § 427 ZPO gilt der Inhalt der Abschrift einer Urkunde als bewiesen, wenn der Gegner der Anordnung, die in seinen Händen befindliche Urkunde vorzulegen, nicht nachgekommen ist.

Bestehen bezüglich aller oder einzelner Dokumente keine gesetzlichen Aufbewahrungspflichten, ist für diese Dokumente zu entscheiden, ob sie dennoch im eigenen Interesse aufbewahrt werden sollen. Grundlage der Entscheidung sind wiederum Inhalt und Zielsetzung des Dokuments. Die Aufbewahrung wird empfohlen, wenn entweder der Aufbewahrungszweck Gedächtnisstütze oder Sicherung der Beweisführung eingreift.

Zur Info: Der Aufbewahrungszweck Kontroll- oder Rechenschaftslegung ist regelmäßig mit der Pflicht verbunden, Vorgänge zu dokumentieren und die Dokumente aufzubewahren. Der Aufbewahrungszweck der Archivierung für die Nachwelt wurde bei der Erstellung des Leitfadens nicht näher berücksichtigt.

Zur Feststellung eigener Aufbewahrungsinteressen empfiehlt sich folgendes Vorgehen: Die Dokumente, die nicht von einer gesetzlichen Aufbewahrungspflicht umfasst sind, sind ihrer Art nach zu bestimmen. Für jede Dokumentart ist zu prüfen, ob sie zur Beweisführung oder zur Gedächtnisstütze aufbewahrt werden soll. Ein weniger aufwändiges Verfahren ist wiederum die Zuordnung der einzelnen Dokumente in bestimmte Dokumentkategorien. Es muss nicht für jede Dokumentart, sondern nur für die übergeordneten Dokumentkategorien das Bestehen oder Nichtbestehen von Aufbewahrungszwecken festgestellt werden. Es spricht viel dafür, dass allen Dokumenten, die bisher in Papierform aufbewahrt worden sind, ein Aufbewahrungszweck zugrunde lag, so dass sie vermutlich auch in der elektronischen Fassung aufbewahrt werden sollen. Allerdings kann eine Entschlackung des Systems nur erreicht werden, wenn die bisherige Aufbewahrungspraxis in Frage gestellt und überprüft wird.

Die Notwendigkeit der Aufbewahrung von elektronischen Dokumenten sagt noch nichts darüber aus, wie die Aufbewahrung zu gestalten ist. Vielmehr ist die Frage der Ausgestaltung in einem eigenen, zweiten Schritt zu prüfen. Die Aufbewahrungspflicht und die dahinter stehenden Zwecke kommen dabei allerdings insoweit zum Tragen, als sich aus ihnen wieder bestimmte Grenzen der Ausgestaltung des Archivsystems ergeben können. So ergibt sich zum Beispiel unmittelbar für den Aufbewahrungszweck

der Beweissicherung die Anforderung der Verkehrsfähigkeit, da sie eine unabdingbare Voraussetzung für die Vorlage des Dokuments als Beweismittel beim Gericht ist.

3.2 Zweiter Prüfungsschritt – Ausgestaltung der Aufbewahrung

Der Gesetzgeber hat bei der Normierung der Dokumentations- und Aufbewahrungspflichten primär über das „Ob" der Aufbewahrung entschieden. Zur Ausgestaltung der Aufbewahrung, um der Pflicht Genüge zu tun, finden sich in den gesetzlichen Vorschriften vereinzelt sowohl konkrete, als auch recht allgemein gehaltene Aussagen. Eine konkrete Anforderung stellt zum Beispiel die Dauer der Aufbewahrung dar; recht allgemein ist hingegen die Anforderung, dass die Dokumente während der Aufbewahrung nicht verändert werden können.

Aus dem Gesetz lassen sich somit in der Regel nicht unmittelbar Vorgaben für die Ausgestaltung des Archivsystems entnehmen. Um über diese Klarheit zu erlangen, sind zunächst die Anforderungen zu bestimmen, die mit der Aufbewahrung erfüllt werden sollen. Anschließend müssen technische Sicherungsmittel ausgewählt werden, die zur Erfüllung dieser Anforderungen geeignet sind.

Beachte: Die Art und Weise der Aufbewahrung ist in einem Zwei-Stufen-Verfahren festzulegen:
- Bestimmung der Anforderungen an die aufzubewahrenden Dokumente.
- Auswahl geeigneter Sicherungsmittel.

3.2.1 Bestimmung der Anforderungen an die aufzubewahrenden Dokumente

Dokumente werden grundsätzlich mit dem Ziel aufbewahrt, sie zu erhalten, um mit ihnen für einen längeren Zeitraum ein bestimmtes Ereignis oder Nichtereignis nachweisen zu können.

Zur Info: Regelungen, die die Digitalisierung von Papierdokumenten zur Aufbewahrung erlauben, wie z.B. § 147 Abs. 2 AO, verwenden oftmals den Begriff der Daten. An ihre Aufbewahrung werden häufig ausdrücklich weitergehende Anforderungen gestellt. Da die Daten die Wahrnehmbarkeit für einen Menschen nicht implizieren, müssen sie z.B. unverzüglich lesbar gemacht werden können. Häufig muss zudem ein unmittelbarer Zugriff auf bestimmte, z.B. steuerrelevante Daten möglich sein. Die übrigen Daten müssen hingegen zur Wahrung des Daten- und Geheimnisschutzes zugriffsgeschützt sein.

Unabdingbare Voraussetzung für jede Aufbewahrung ist daher, die Lesbarkeit, Integrität und Authentizität der Dokumente zu sichern.

Definitionen:
- Integrität – Unversehrtheit der Daten.
- Authentizität – eindeutige Bestimmung der Quelle der Daten.
- Lesbarkeit – Sichtbarmachung der in den Daten enthaltenen Informationen. Ein elektronisches Dokument ist nur dann lesbar, wenn die notwendige Hard- und Software die Daten verarbeiten und ihre Informationen interpretieren und dem menschlichen Betrachter in lesbarer Weise präsentieren kann.

Daneben kann grundsätzlich die Aufbewahrungsdauer als weitere rechtliche Anforderung aus den Vorschriften zur Aufbewahrung entnommen werden. Die Aufbewahrungsfristen sind kategorien- oder dokumentspezifisch geregelt und bewegen sich im Allgemeinen zwischen 3 und 10 Jahren. In seltenen Fällen sind Dokumente bis zu 30 Jahren, bei relevanten Angaben etwa über Grundstücke oder langfristige Rechtsverhältnisse auch „ewig" aufzubewahren. Die Dauer ist bei der Auswahl der einzusetzenden Sicherungsmittel wichtig, da diese im Laufe der Zeit ihre Sicherungseignung verlieren können.

Anwendung	Rechtsgrundlage	Aufbewahrungsdauer
Verwaltungsrecht	In Abhängigkeit der Dokumentart	Im allgemeinen nicht über 30 Jahre (beachte aber eine ggf. spätere Archivierungspflicht)
Medizinrecht	§ 10 Abs. 3 MBO-Ärzte § 28 Abs. 4 RöntgVO	Grundsätzlich 10 Jahre Bis zu 30 Jahren
HGB und Steuerrecht	§ 257 Abs. 4 HGB, § 147 Abs. 3 AO	Je nach Dokumenten- oder Datenart 6 oder 10 Jahre

Beachte: Die tabellarisch dargestellten Aufbewahrungsfristen ergeben sich aus dem jeweiligen Fachrecht. Aus anderen Gründen, z.B. längere Verjährungsfristen, können sich aber längere Aufbewahrungszeiträume ergeben.

Letztlich können sich aus der Berücksichtigung des Inhalts und des Aufbewahrungszwecks der Dokumente weitere rechtliche Anforderungen ergeben. Sofern eine Aufbewahrung zum Zweck der Beweissicherung erfolgt, muss das beweiserhebliche Dokument in einem Gerichtsprozess ohne Qualitätsverlust vorgelegt werden können, muss also verkehrsfähig sein. Dies wird in der Regel durch die Verwendung von gängigen oder sogar standardisierten Datenformaten erreicht. Nach dem derzeitigen Stand der Technik sollten standardisierte Formate wie zum Beispiel pdf/A für die Aufbewahrung gewählt werden. Es ist den Gerichten zwar nicht erlaubt, nur Dokumente in bestimmten Dateiformaten als Beweismittel zuzulassen. Wird ein seltenes Format verwendet, ist allerdings häufig die Hinzuziehung eines Sachverständigen erforderlich, was hohe Kosten verursachen kann.

Sofern die Dokumentation eines Vorgangs von Bedeutung ist und daher der Gesamtzusammenhang mehrerer Dokumente erhalten bleiben muss, ist die Vollständigkeit einer Dokumentation zu gewährleisten.

Definitionen:

- Verkehrsfähigkeit – Möglichkeit, Dokumente und Akten von einem System zu einem anderen übertragen zu können, bei der die „Qualität" des Dokuments sowie seine Integrität und Authentizität nachweisbar bleiben.
- Vollständigkeit – Bezug mehrerer aufgrund eines inneren Zusammenhangs zu einer Sammlung oder auch Akte zusammengefasster Einzeldokumente ist sichergestellt.

Diese Mindestanforderungen an die Ausgestaltung der Aufbewahrung können ebenfalls als Maßstab für die Aufbewahrung im eigenen Interesse dienen.

Teilweise werden diese allgemeinen Anforderungen in außergesetzlichen Richtlinien, Standards oder weit verbreiteten Konzepten spezifiziert. Die folgende Tabelle soll einen beispielhaften Überblick ermöglichen, in welchen Bereichen und mit welchen Inhalten und Funktionen derartige Vorgaben bestehen.

Konzept, Standard, Norm	Inhalte/Funktionen
DOMEA-Konzepte der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt)	Konzept zur Hilfe von Vergabeverfahren bei der Einführung von DMS-Lösungen in der öffentlichen Verwaltung Anforderungen an Softwareprodukte
MoReq (Model Requirements for the Management of Electronic Records) Von der Europäischen Kommission beauftragte Spezifikation	Modell-Spezifikation zu funktionalen Anforderungen an Schriftgutverwaltungs-systeme
OT-Leit-ERV (Organisatorischtechnische Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften)	Von der Bund-Länder-Kommission erstellte und durch den Ländern und dem Bund zur Einführung des elektronischen Rechtsverkehrs empfohlene Leitlinien.
Open Archival Information System OAIS (ISO 14721) – Ein Referenzmodell zur Organisation und Abwicklung der Archivierung digitaler Unterlagen	Referenzmodell für ein Archiv
ISO 15 489 (Information, Documentation – Record Management)	Norm für die Verwaltung und Aufbewahrung von Unterlagen
Grundsätze der elektronischen Archivierung (Code of Practice) des Verbands Organisations- und Informationssysteme (VOI)	Leitfaden zur Einführung eines revisionssicheren Archivsystems in einer Organisation oder einem Unternehmen.
IT-Grundschutz-Kataloge des BSI	IT-Grundschutz bietet eine Methode, dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen.
PK-DML (Prüfkriterien für Dokumentenmanagement-Lösungen) vom TÜViT und VOI.	Prüfkriterien für Dokumentenmanagement-Lösungen (PK-DML),

Zur Info: Bei diesen Konzepten, Standards oder Richtlinien handelt es sich nicht um Rechtsnormen. Sie sind daher grundsätzlich nicht bindend, sondern stellen eine Orientierungshilfe für den Aufbewahrungspflichtigen bei der Bestimmung der Anforderungen dar. Eine rechtliche Bedeutung erlangen sie nur dann, wenn ein Gesetz sich ausdrücklich auf sie bezieht. Da sie allerdings im Allgemeinen von Experten erstellt worden sind, kommt Ihnen eine Indizfunktion zu, so dass ihre Berücksichtigung zu empfehlen ist.

Von diesen Konzepten und Normen sind Anforderungskataloge zu unterscheiden, die entweder von Aufsichts- und Kontrollinstanzen zur Prüfung des ordnungsgemäßen Handelns bestimmter Personen herangezogen werden oder diese zu einem entsprechenden Handeln verpflichten.

Anforderungskataloge	Funktionen
GoBS (Grundsätze ordnungsgemäßer DV-stützter Buchführungssysteme)	Wurden durch Schreiben des Bundesministeriums der Finanzen (BMF) an die obersten Finanzbehörden der Länder vom 7.11.1995 intern für verbindlich erklärt. Die Schreiben des Bundesministeriums für Finanzen sind Verwaltungsanweisungen ohne Rechtsnormcharakter. Sie binden zwar die Verwaltung aber nicht die Gerichte. die sich aber aufgrund der als Willensbekundung des BMF hohen Bedeutung maßgeblich auf sie stützen werden. Sie sind Leitlinien für die Hersteller und Betreiber von Buchführungs- und technischen Aufbewahrungssystemen, da die Finanzbehörden sich bei der Prüfung grundsätzlich an diesen orientieren.
GDPdU (Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)	Wurden durch BMF-Schreiben vom 16. Juli 2001 ebenfalls intern, d.h. für die Finanzbehörden, für verbindlich erklärt. Vom Charakter her entsprechen sie der GoBS.

Zur Info: Auch diese Regelungen sind kein allgemein geltendes Recht. So führt eine Buchführung, die entsprechend der Grundsätze ordnungsgemäßer Speicherbuchführung geführt ist, zwar dazu, dass sie vom Finanzamt als Grundlage für die Besteuerung herangezogen wird. Abgesehen von einer Indizfunktion für das Erbringen bestimmter Nachweise kommt ihr jedoch keine weitere juristische Funktion zu.

Betreffen die dargestellten Anforderungen alle die Aufbewahrung, so ist bei dieser ebenfalls immer die Sicherung der Vertraulichkeit im Auge zu behalten.

Definition:
Vertraulichkeit: Schutz vor unbefugter Kenntnisnahme zur Sicherung der Geheimhaltung personenbezogener Daten und betriebs- oder berufsbezogener Geheimnisse.

Sofern die aufzubewahrenden Dokumente personenbezogene Daten oder Geheimnisse beinhalten, stehen der Daten- und Geheimnisschutz immer in einem Spannungsverhältnis zur Aufbewahrung. Zur Auflösung dieses Konflikts sind im Rahmen der Ausgestaltung der Aufbewahrungssysteme Maßnahmen zu ergreifen (zum Beispiel Verschlüsselung der Daten), die die Vertraulichkeit sicherstellen. Außerdem muss die Möglichkeit bestehen, einzelne Dokumente aus dem Archiv zu löschen, sofern eine weitere Aufbewahrung aus datenschutzrechtlichen Gründen verboten ist.

Zur Info: Die Vertraulichkeit ist die einzige bei der Aufbewahrung zu berücksichtigende Anforderung, die sich nicht aus den Aufbewahrungszwekken, sondern aus anderen zu schützende Rechtsgütern ableiten lässt. Bezüglich bestimmter Arten von Dokumenten wie z.B. Personalunterlagen ergibt sich die Pflicht zur Wahrung der Vertraulichkeit aus gesetzlichen Vorschriften, die auf den Daten- und Geheimnisschutz zurückzuführen sind. Die Sicherung der Vertraulichkeit ist als rechtliche Anforderung während der Aufbewahrung zu berücksichtigen. Regelmäßig bestehen für vertrauliche Daten zudem Löschungspflichten ab einem bestimmten Zeitpunkt.

3.2.2 Geeignete Sicherungsmittel

Die Entscheidung für den Einsatz bestimmter Sicherungsmittel zur Erfüllung der Anforderungen an die Aufbewahrung setzt nicht nur die Kenntnis voraus, welche Sicherungsmittel überhaupt am Markt zur Verfügung stehen, sondern verlangt auch eine Bewertung ihrer Eignung, um die mit der Aufbewahrung verfolgten Zwecke erreichen zu können.

a. Sicherungsmittel

Die gesetzlichen Vorschriften zur Aufbewahrung von elektronischen Dokumenten benennen in der Regel keine Sicherungsmittel, die zur Erfüllung der Anforderungen einzusetzen sind.

Zur Info: Der Gesetzgeber verfolgt grundsätzlich einen technikneutralen Ansatz, indem er nicht den Einsatz bestimmter technischer Sicherungsmittel vorschreibt. Diese Technikneutralität hat Vor- und Nachteile. Einerseits gewährt sie dem aufbewahrungspflichtigen Anwender ein großes Maß an Entscheidungsfreiheit und die Möglichkeit, unternehmensspezifische und wirtschaftliche Aspekte bei der Auswahl der Sicherungsmittel zu berücksichtigen. Andererseits ist sie mit einer gewissen Mehrarbeit verbunden, weil der Anwender selbst die Auswahl der geeigneten Sicherungsmittel leisten muss und das Risiko trägt, dass die von ihm getroffenen Maßnahmen nicht ausreichend sind.

Einige Ausnahmen bestätigen die Regel: So kennt das Gesetz die Benennung technisch-organisatorischer Maßnahmen zur Wahrung des Datenschutzes (s. dazu zum Beispiel Anhang zu § 9 BDSG). Eine weitere Ausnahme sind elektronische Signaturen, die als Grundtechnologie in einer Reihe von Form- und Beweisvorschriften ihren Niederschlag gefunden haben. Erfolgt somit eine Aufbewahrung auch zum Zwecke der Beweissicherung, empfiehlt sich der Einsatz qualifizierter elektronischer Signaturen, da elektronische Dokumente, die qualifiziert signiert sind, beweisrechtlich privilegiert werden und damit eine höhere Beweissicherheit erreichen.

Zur Info: Die (Papier-)Urkunde ist im System des Beweisrechts das sicherste Beweismittel, da das Gericht, sofern die Echtheit der Unterschrift feststeht, hinsichtlich der Bestimmung des Beweiswerts des Dokuments Beweisregeln unterliegt. Sofern elektronische Dokumente qualifiziert signiert sind, sind sie von ihrer Beweiswirkung Urkunden gleichgestellt. Zu beachten ist allerdings, dass selbst nicht signierte elektronische Dokumente nicht beweisrechtlich wertlos sind. Sie können ebenfalls in einen Prozess als Beweismittel eingeführt werden; das Gericht ist allerdings in seiner Beweiswürdigung frei. Sofern die Echtheit des Dokuments strittig ist, muss der Beweispflichtige weiterführende Nachweise erbringen. Ob er dies kann, hängt von den konkreten Umständen ab und dürfte bei ungesicherten Dokumenten – soweit nicht weitere Beweismittel zugezogen werden können – im Regelfall schwierig, muss aber nicht unmöglich sein.

Eine konkrete und umfassende Umsetzung der Anforderungen, in der die geeigneten technischen Sicherungsmittel und organisatorischen Maßnahmen beschrieben werden, finden sich auch nicht in den bereits dargestellten Konzepten, Standards, Richtlinien und Anforderungskatalogen.

Beachte: Die nachfolgend vorgenommene Konkretisierung der einzusetzenden Sicherungsmittel will diese Lücke aufgreifen. Sie orientiert sich am derzeitigen Stand der Technik; technische Weiterentwicklungen können in Zukunft zu anderen Bewertungen führen.

Ausgehend von der Zielsetzung des Einsatzes von Sicherungsmitteln, nämlich eine langfristige und unveränderbare Aufbewahrung der im Archiv befindlichen Dokumente sicherzustellen, können unterschiedliche Sicherungsmittel zum Einsatz kommen. Dies können – einzeln oder in Kombination – system-, datenträger- und dokumentspezifische Sicherungsmittel sein.

Definition Sicherungsmittel:
- Systembezogene Sicherungsmittel beschränken durch eine individuelle Konfiguration des Archivsystems oder der auf dieses zugreifenden Komponenten den Zugriff auf die Daten, z.B. durch Berechtigungssysteme.
- Datenträgerbezogene Sicherungsmittel sind Speichermedien, die ein Überschreiben oder Verändern der auf ihnen abgelegten Informationen ausschließen, z.B. CD-ROM, DVD, WORM.
- Dokumentenbezogene Sicherungsmittel sind solche, die die elektronischen Dokumente selbst gegen die unbemerkte Veränderungen und unberechtigte Kenntnisnahme schützen, z.B. Verschlüsselungstechnologien.

b. Eignung der Sicherungsmittel

Die Auswahl der Sicherungsmittel muss sich an den Anforderungen orientieren. Nicht jedes Sicherungsmittel ist geeignet, jede beliebige Anforderung zu erfüllen. Daneben können die Sicherungsmittel für eine Anforderung eine eher geringe oder recht hohe Effektivität gewährleisten. Die Art und Weise der Aufbewahrung und die technischen Sicherungsmittel sind daher so auszuwählen und zu gestalten, dass die verfolgten Ziele und Interessen erfüllt werden.

Zur Info: Die Eignung der Sicherungsmittel ist immer in Bezug auf das jeweilige Schutzziel hin zu überprüfen. Die nachfolgenden Überlegungen beziehen sich primär auf die Eignung zur Erfüllung der Aufbewahrungszwecke. Sofern Vertraulichkeit zu gewährleisten ist, sind gegebenenfalls weitere Sicherungsmittel zum Schutz der Dokumente einzusetzen.

Für die verschiedenen Sicherungsmittel ergibt sich im Hinblick auf ihre Eignung zur Erfüllung der unterschiedlichen Anforderungen eine differenzierte Bewertung. Zielsetzung der Matrix auf Seite 167 ist eine möglichst einfache Bestimmbarkeit, mit welchen technischen Sicherungsmitteln welche Aufbewahrungszwecke bestmöglich erreicht werden können.[3] Als Bewertungsmaßstab wurde ein dreistufiges Verfahren gewählt, aus dem folgt, ob ein Mittel ungeeignet (= 0), ausreichend (= 1) oder gut (= 2) die Anforderung erfüllt. Die Tabelle verdeutlicht, dass in der Regel durch ein Sicherungsmittel verschiedene Anforderungen erfüllt werden. Der Faktor Zeit, der Einfluss auf die dauerhafte Eignung der Sicherungsmittel hat, wird in der Matrix nicht behandelt, sondern findet nachfolgend unter c) seine Berücksichtigung.

Schreibschutzmechanismen sind ein systembezogenes Sicherungsmittel. Indem das System keine Änderungen an dem Dokument zulässt, sondern die Dokumente im „Nur-Lesemodus“ anzeigt, ist ihre Integrität und Authentizität mittelbar, nämlich durch das Aufbewahrungssystem, ausreichend geschützt. Gleiches gilt in Bezug auf die Vollständigkeit, da Schreibschutzmechanismen ebenfalls vor dem Löschen der Dokumente schützen. Da jedoch die Möglichkeit von Manipulationen bleibt, zum Beispiel durch Umgehen des „Nur-Lesemodus“, kann dem Sicherungsmittel keine uneingeschränkt gute Bewertung gegeben werden. Sofern die Dokumente aus dem System genommen und Dritten zur Verfügung gestellt werden sollen, verlieren die Dokumente allerdings ihren Schutz. Dritte haben in diesem Fall keine Anhaltspunkte, um die Authentizität zu überprüfen. Zur Wahrung der Verkehrsfähigkeit sind sie daher ungeeignet.

Zu einer entsprechenden Bewertung führt die Prüfung der Eignung von Bearbeitungs- und Zugriffsprotokollen sowie Zugriffs- und Zutrittsbeschränkungen. Diese Mechanismen schützen wie auch Schreibschutzmechanismen das Dokument nur durch das Aufbewahrungssystem, indem Änderungen am Dokument protokollarisch verfolgt oder auf diese gar nicht erst zugegriffen werden darf. Ein Entnehmen der Dokumente aus dem System führt zu einem Verlust des Schutzes. Ihnen fehlt daher die Verkehrsfähigkeit.

Der Einsatz wiederbeschreibbarer Speichermedien ist ungeeignet, um die Anforderungen zu erfüllen. Anders verhält es sich jedoch bei nichtwie-

[3] Es sei nochmals darauf hingewiesen, dass die hier herangezogenen Anforderungen nicht abschließend sind. Außerdem hat eine Kombination von Sicherungsmitteln ebenfalls Auswirkungen auf die Bewertung.

derbeschreibbaren Medien. Die Eignung ergibt sich aus ihrer Eigenschaft, dass keine Änderungen an den auf den Datenträgern gespeicherten Dokumenten vorgenommen werden können. Sofern die Speichermedien portabel und die zum Lesen des Mediums erforderliche Hard- und Software verfügbar sind, sind die darauf gespeicherten Dokumente auch ausreichend verkehrsfähig.

Der Sicherheitsmechanismus elektronischer Signaturen setzt hingegen unmittelbar beim Dokument an, indem die Daten über den Hashwert Grundlage und Teil der Signatur sind. Der Einsatz elektronischer Signaturen schützt zwar nicht vor Veränderungen der Daten, doch kann bei Verwendung geeigneter Verfahren der mathematische Beweis geführt werden, dass die Daten nicht verändert wurden. Bei der Verwendung fortgeschrittener Signaturen kann eine allgemeine Aussage zu ihrer Eignung zur Integritäts- und Authentizitätssicherung nicht getroffen werden. Diese hängt vielmehr von der Qualität der eingesetzten Verfahren ab, weshalb für ihre Eignung ein „von – bis“ Wert angegeben ist. Gleiches gilt für die Bewertung ihrer Eignung für die Vollständigkeit und Verkehrsfähigkeit der Dokumente.

Anders verhält es sich beim Einsatz qualifizierter elektronischer Signaturen. Die an sie gestellten rechtlichen Voraussetzungen sind so hoch, dass die Integrität, Authentizität und Vollständigkeit sichergestellt sind. Aufgrund ihres Dokumentbezugs ist ebenfalls die Verkehrsfähigkeit gewährleistet, da das Dokument nicht lediglich über das Aufbewahrungssystem und einen Datenträger gesichert wird. Der Schutz greift auch dann, wenn das elektronisch signierte Dokument nach außen gegeben werden muss. Darüber hinaus ist der Schutzmechanismus einer qualifizierten elektronischen Signatur für einen Dritten transparent. Er muss nicht auf die Verlässlichkeit eingesetzter Systeme und Datenträger vertrauen, sondern kann sie selbst prüfen. Die Überprüfung der Signatur kann durch jede beliebige Person durchgeführt werden, ohne dass es der Mitwirkung des Signierenden bedarf.

System- oder datenträgerspezifische Maßnahmen, die die Authentizität der Dokumente sichern, erfordern immer das Vertrauen des Dritten in das System und dessen Administratoren; eine Möglichkeit, beides selbst zu überprüfen, besteht nicht. Dies kann zwar durch Dokumentations- und Protokollierungsmaßnahmen sowie durch Erstellung einer Signatur bei Herausnahme eines Dokuments aus dem Archiv erreicht werden. Neben dem dadurch entstehenden hohen Dokumentationsaufwand zur Darstellung der Abgeschlossenheit des Archivsystems, ist damit allerdings immer auch die Notwendigkeit verbunden, im Einzelfall diese Sicherheit nachweisen zu müssen.

Anforderungen		Technische Maßnahmen Bewertungsskala: 0 = ungeeignet, 1 = ausreichend, 2 = gut						
		Systemspezifisch			Datenträgerspezifisch		Dokumentspezifisch	
		Schreibschutz	Bearbeitungs- und Zugriffsprotokolle	Zugriffs- und Zutrittsbeschränkungen	Wiederbeschreibbare Speichermedien	Nicht wiederbeschreibbare Speichermedien	Fortgeschrittene Signaturen	Qualifizierte Signaturen
Grundanforderung	Integrität	1	1	1	0	2	0–2	2
	Authentizität	1	1	1	0	2	0–2	2
	Lesbarkeit	0	0	0	0	0	0	0
	Vollständigkeit	0	1	1	0	2	0–2	2
	Verkehrsfähigkeit	0	0	0	0	1	0–2	2

Durch den kumulativen Einsatz mehrerer Sicherheitsmittel kann ein insgesamt höheres Sicherheitsniveau erreicht werden.

Beachte:
- Der Einsatz elektronischer Signaturen ermöglicht einen Integritäts- und Authentizitätsschutz, schützt jedoch NICHT vor Veränderungen am Dokument. Es müssen daher weitere Mechanismen, wie z.B. Zugriffsschutzmechanismen eingesetzt werden.
- Eine durchgängige Verkehrsfähigkeit des Dokuments lässt sich nur über den Einsatz elektronischer Signaturen erreichen, da nur diese für Dritte überprüfbare und transparente Sicherungsmittel sind.
- Beweiserleichterungen werden nur beim Einsatz qualifizierter Signaturen gewährt.
- Allen Sicherungsmitteln kommt für die Sicherung der Lesbarkeit keine Relevanz zu.

c. Dauerhaftigkeit

Die eingesetzten Sicherungsmittel unterliegen alle dem durch die Weiterentwicklung bedingten „technischen Verfall“. Die zum Einsatz kommenden Archivsysteme, Datenträger (Hardware) sowie Datenformate und Programme (Software) müssen, um weiterhin dem Stand der Technik zu entsprechen, ausgewechselt werden. Der Verlust der Sicherheitseignung der eingesetzten Schlüssel- und Hashverfahren kann die Sicherheit elektronischer Signaturen bedrohen. Darüber hinaus ist eine langfristige Prüfung der Signaturen nicht gewährleistet.

Beachte: Alle eingesetzten Sicherungsmittel sind im Allgemeinen nicht langzeittauglich und bedürfen daher grundsätzlich einer Aktualisierung.

Die Sicherheit eines Aufbewahrungssystems muss deshalb im Zeitraum der Aufbewahrungsdauer immer wieder kritisch überprüft werden. Gegebenenfalls müssen Maßnahmen getroffen werden, um den Sicherheitsstatus zu erhalten.

Zur Überbrückung dieser bestehenden Risiken bietet es sich an, folgende Sicherungsmaßnahmen zu ergreifen:

Bei jedem Datenträger- und Systemwechsel ist zu beachten, dass die Sicherung der Integrität und Authentizität der Daten gewährleistet bleibt. Sofern die zu übertragenden Dokumente nicht signiert sind und somit keinen dokumentenspezifischen Integritätsschutz haben, ist insbesondere über technisch-organisatorische Maßnahmen (zum Beispiel ein Zugriffsschutz) zu gewährleisten, dass Änderungen ausgeschlossen werden. Dies gilt es umfassend zu dokumentieren, um nachträglichen Einwänden hinsichtlich der Unversehrtheit der Dokumente etwas entgegenhalten zu können.

Sofern ein Formatwechsel zur Sicherung der Lesbarkeit erforderlich ist, gilt Vorstehendes ebenfalls. Darüber hinaus ist bei elektronisch signierten Dokumenten zu beachten, dass die elektronische Signatur als Sicherungsmittel ihren Wert verliert, da sie hinsichtlich des neuen Dokuments nicht mehr prüfbar ist. Daher sind geeignete Verfahren einzusetzen, die sicherstellen, dass die Integrität des Dokuments vor diesem Transformationsprozess festgestellt wird und im Rahmen der Transformation keine Änderungen möglich sind. Schließlich ist das neu entstandene Dokument entsprechend zu schützen und daher ebenfalls mit einer Signatur gleicher Güte zu signieren.

Beachte: Die Gefahr einer erforderlichen Transformation zur Sicherung der Lesbarkeit kann durch den Einsatz geeigneter Formate bereits bei der Dokument- und Signaturerstellung reduziert werden. Als geeignete Formate sind insbesondere standardisierte Formate anzusehen.

Dem drohenden Verlust der Sicherheitseignung der eingesetzten Schlüssel- und Hashverfahren bei elektronischen Signaturen ist durch eine rechtzeitige Neusignierung, die den Anforderungen des § 17 SigV entspricht, entgegenzuwirken.

Zur Info:
- Die Notwendigkeit einer Neusignierung kann zeitlich nicht eindeutig festgelegt werden. Es kann nicht ausgeschlossen werden, dass die verwendeten Hash- und Signaturverfahren schneller als vom BSI prognostiziert ihre Sicherheitseignung verlieren (s. zur Algorithmeneignung www.bnetza.de -> elektronische Signatur -> Veröffentlichungen -> amtliche Veröffentlichungen -> geeignete Algorithmen).
- Der Ablauf der Gültigkeit eines Zertifikats hat KEINE Auswirkung auf die Sicherheitseignung der verwendeten Hash- und Signaturverfahren und zieht daher keine Neusignierung nach sich.

Bei der Wahl eines Archivsystems ist daher zu beachten, dass dieses ein Verfahren zur Neusignierung erlaubt, das entsprechend kostengünstig und in einem automatisierten Prozess durchzuführen ist.

Beachte: Sofern eine Neusignierung entsprechend dem ArchiSig-Konzept[4] über die Bildung von Hashwertbäumen erfolgt, sollten die für die Prüfung der Ursprungssignatur erforderlichen Hashwerte und Verifikationsdaten unter Verwendung eines standardisierten Formats dem signierten Dokument beigefügt werden können, um dadurch eine Verkehrsfähigkeit des maßgeblichen Dokuments unter Einbeziehung der Signaturen zu erreichen. Ein entsprechendes Format wird derzeit unter der Bezeichnung ERS (Evidence Record Syntax) auf internationaler Ebene bei der IETF standardisiert.

Um die Echtheit elektronischer Signaturen jederzeit unabhängig von Dritten überprüfen zu können, sind deren erforderliche Verifikationsdaten einzuholen und zu speichern.

Zur Info: Die erforderlichen Verifikationsdaten zur Prüfung einer Signatur sollten so früh wie möglich eingeholt werden. Erfolgt eine frühe Aufbewahrung parallel zur weiteren Bearbeitung des Dokuments im Vorgangsbearbeitungssystem, kann dieser Vorgang im Archivsystem erfolgen. Werden die Dokumente dagegen erst im Archivsystem abgelegt, wenn sie für die Vorgangsbearbeitung nicht mehr benötigt werden (so genannte späte Aufbewahrung), sollten die Verifikationsdaten bereits vom Vorgangsbearbeitungssystem beschafft werden.

In den meisten Fällen reicht es bei Vorliegen qualifizierter elektronischer Signaturen aus, folgende Verifikationsdaten einzuholen:
- User-Zertifikate (Signatur, Attribut) mit Zertifikatskette bis zur Wurzelinstanz,
- Akkreditierter Zeitstempel (als Referenzzeitpunkt) bzgl. Signaturwert mit Zertifikatskette bis zur Wurzelinstanz,
- Gültigkeitsabfragen (OCSP-Responses, akkreditiert signiert) auf Nutzerzertifikate mit Zertifikatskette bis zur Wurzelinstanz.

Es bietet sich an, diese Daten vor der ersten Neusignierung einzuholen, da auch Verifikationsdaten mit Signaturen versehen sind, deren Algorithmen „gepflegt“ werden müssen.

Beachte:
- Nur eine rechtzeitige Neusignierung sichert dauerhaft die Verkehrsfähigkeit eines elektronisch signierten Dokuments.
- Die Sicherung der prozessualen Beweiserleichterung setzt eine rechtzeitige Neusignierung voraus.
- Die Erfüllung der Anforderungen an die Aufbewahrung elektronischer Dokumente lässt sich ebenfalls durch system- und datenträgerbezogene Sicherungsmittel erreichen, doch setzt dies umfassende Dokumentationsmaßnahmen voraus.

[4] Beim diesem handelt es sich um eine Methode, an Hand der automatisiert und kostensparend Neusignaturen vorgenommen werden können. Umfassend dazu s. Roßnagel/Schmücker (Hrsg.), Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente, Heidelberg 2005.

In die Abwägung bei der Wahl des Sicherungsmittels können noch weitere Kriterien, wie zum Beispiel die Wirtschaftlichkeit oder die Nutzerfreundlichkeit einfließen. Erst aus der Gesamtschau und der Bewertung der zu berücksichtigenden Anforderungen kann das geeignete Sicherungsmittel gefunden werden. Aus diesem Grund ist es nicht ausgeschlossen, dass der Einsatz eines „nur“ mit ausreichend bewerteten Sicherungsmittels in Bezug auf die rechtlichen Anforderungen gerechtfertigt sein kann. Insofern ist im Rahmen des rechtlich Zulässigen eine Risikoabwägung zu treffen.

Diese Überlegungen zur Ausgestaltung der Aufbewahrung können auch als Maßstab für die Aufbewahrung im eigenen Interesse dienen. Allerdings steht es dem Anwender frei, ein niedrigeres Sicherheitsniveau umzusetzen, sofern dadurch keine Sorgfaltspflichtverletzung der Verantwortungsträger droht.

Beachte: Dies ist nur dann zu empfehlen, wenn eine zuvor durchgeführte Risikoeinschätzung zu dem Ergebnis kommt, dass der mit der Umsetzung der Sicherungsanforderungen verbundene Aufwand (technisch, organisatorisch und finanziell) gegenüber dem potentiellen Vorteil der sicheren Aufbewahrung unverhältnismäßig hoch ist.

4. Besondere Bedeutung von Archivzeitstempeln

Das Aufbewahrungssystem ist so zu gestalten, dass die allgemein oder für unterschiedliche Dokumente und Aufbewahrungszwecke ermittelten Anforderungen optimal gewährleistet werden.

Sind für jede aufzubewahrende Dokumentart die Anforderungen festgestellt, bieten sich für die Gestaltung des Aufbewahrungssystems zwei Alternativen an. Es wird ein einheitliches Aufbewahrungssystem zur Aufbewahrung aller Dokumente konzipiert. Dieses muss dann gebündelt alle Anforderungen erfüllen, die bei der dokumentspezifischen Bestimmung der Anforderungen festgestellt worden sind. Die zweite Möglichkeit ist, ein abgestuftes Aufbewahrungssystem zu gestalten. Entsprechend der jeweils umzusetzenden Anforderungen sind unterschiedliche Sicherungsmittel einzusetzen.

Sofern in das Archiv signierte wie auch nicht signierte Dokumente gelangen, bietet sich allerdings auf alle Fälle der Einsatz von initialen Archivzeitstempeln bei Aufnahme in das Archiv an. Hierunter sind Zeitstempel zu verstehen, die in Verbindung mit einer elektronischen Signatur bestätigen, dass bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben. In diesem Fall muss nicht jedes Dokument zeitgestempelt werden, Vielmehr genügt es, nach dem ArchiSig-Konzept Hashwertbäume, die viele Dokumente repräsentieren, mit einer Signatur oder einem Zeitstempel zu versehen.

Wenn ein unsigniertes Dokument bei der Aufnahme in ein Archivsystem mit einem solchen Zeitstempel versehen und beide untrennbar miteinander verbunden werden, kann die Integrität des Dokuments zumindest ab dem Zeitpunkt der Zeitstempelung mit ausreichender Sicherheit nachgewiesen werden. Der Zeitraum für mögliche Veränderungen kann dadurch wesentlich verkürzt werden. Die Beweisaussichten verbessern sich zudem durch die Erfahrung, dass sich ein Veränderungsmotiv häufig erst nach einiger Zeit und daher unter Umständen erst nach der Erstellung des Archiveingangszeitstempels ergibt. Für diesen Zeitraum gewährleistet der Zeitstempel aber gerade den Nachweis der Integrität. Darüber hinaus stellen erst diese Maßnahmen eine für Dritte transparente und nachvollziehbare Sicherung der Authentizität des Dokuments dar.

Beachte: Die Verwendung eines Archivzeitstempels auch für ursprünglich unsignierte Dokumente führt zwar nicht dazu, dass für dieses Dokument die Beweisregelung des § 371a ZPO eingreift, führt aber im Beweisverfahren zu faktischen Vorteilen, da der Zeitraum möglicher Veränderungen nachvollziehbar und transparent eingegrenzt werden kann. Der Zeitstempel und die Signatur erfüllen ihre Funktionen daher nicht nur im Zusammenhang mit der Erstellung eines Dokuments, sondern auch noch, wenn sie zu einem späteren Zeitpunkt zum Einsatz kommen.

Letztlich ist die Entscheidung, welche Sicherungsmittel eingesetzt werden sollen, aber immer im Rahmen einer Risikoabwägung zu treffen.

Checkliste

Erster Prüfungsschritt – Notwendigkeit der Aufbewahrung:

- Bestimmung des Dokumentenbestands
- Qualifizierung der Dokumente in Kategorien und/oder Arten
- Bestimmung gesetzlicher Dokumentations- und Aufbewahrungspflichten für die Dokumentkategorien und/oder -arten
- Bestimmung von Aufbewahrungszwecken im eigenen Interesse für die Dokumentkategorien und/oder -arten

Zweiter Prüfungsschritt – Ausgestaltung der Aufbewahrung:

- Beachtung der Grundanforderungen der Aufbewahrung: Integrität, Authentizität, Lesbarkeit
- Bestimmung weiterer Anforderungen für die Dokumentkategorien und/oder –arten
  - Aufbewahrungsdauer
  - Verkehrsfähigkeit
  - Vollständigkeit
  - Vertraulichkeit
- Eignungsbestimmung der bestehenden system-, datenträger- und dokumentbezogenen Sicherungsmittel in Bezug auf die zu erfüllenden Anforderungen
- Auswahl der konkret einzusetzenden Sicherungsmittel
  - Beachte die Qualitätsunterschiede elektronisch signierter und elektronisch unsignierter Dokumente
  - Entscheidung über den Einsatz von Archiveingangszeitstempeln
- Beachte die Notwendigkeit der Pflege der eingesetzten Sicherungsmittel für die dauerhafte Sicherung der Anforderungen
  - Notwendigkeit der Transformation
  - Notwendigkeit der Verifikationsdatenbeschaffung
  - Notwendigkeit der Neusignierung
- Auswahl der entsprechenden Komponenten des elektronischen Archivssystems

Abkürzungsverzeichnis

Abs.	Absatz
AO	Abgabenordnung
ArbZG	Arbeitszeitgesetz
ArchiSig	Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente, Forschungsprojekt
ASTM	American Society for Testing and Materials
BDSG	Bundesdatenschutzgesetz
BerufsO	Berufsordnung
BGB	Bürgerliches Gesetzbuch
BImSchVO	Bundesimmissionsschutzverordnung
BiostoffVO	Biostoffverordnung
BMF	Bundesministerium der Finanzen
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CD-ROM	Compact Disk-Read Only Memory
DMS	Dokumenten-Management-System
DOMEA	Dokumenten-Management und elektronische Archivierung
DV-	Datenverarbeitung-
DVD	Digital Versatile Disk
EN-ISO-	Europäische Norm - International Standardisation Organisation
ERS	Evidence Record Syntax
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoBS	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
GWG	Geldwäschegesetz
HGB	Handelsgesetzbuch
HGrG	Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder
IETF	Internet Engineering Task Force
IOS	International Organisation of Standardization
JArbSchG	Jugendarbeitsschutzgesetz
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KWG	Kreditwesengesetz
LadenSchlussG	Ladenschlussgesetz
MBO-Ärzte	Musterberufsordnung für die deutschen Ärztinnen und Ärzte
MoReq	Model Requirements fort he Management of Electronic Records
NachwG	Gesetz über den Nachweis der für ein Arbeitsverhältnis geltenden wesentlichen Bedingungen
OASIS	Open Archival Information System
OSCP	Online Certificate Service Protocoll
OT-Leit-ERV	Organisatorisch-technische Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften
PDF/A	Portable Document Format zur Langzeitarchivierung
PK-DML	Prüfkriterien für Dokumentenmanagement-Lösungen
UStG	Umsatzsteuergesetz
RöntgV	Röntgenverordnung
s.	siehe
SchrAG	Schriftgutaufbewahrungsgesetz
SGB	Sozialgesetzbuch
SigV	Signaturverordnung
StGB	Strafgesetzbuch
StrlSchV	Strahlenschutzverordnung
TIFF	Tagged Image File Format
TÜViT	Technischer Überwachungsverein Informationstechnik
TzBfG	Gesetz über Teilzeitarbeit und befristete Arbeitsverträge
VOI	Verband Organisations- und Informationssystem
VwVfG	Verwaltungsverfahrensgesetz

WO	Wahlordnung
WORM	Write Once, Read Multiple Times
WpHG	Wertpapierhandelsgesetz
z.B.	zum Beispiel
ZPO	Zivilprozessordnung

Glosar

Akte
: Zusammenstellung von sachlich zusammengehörigen Dokumenten, die als Einheit behandelt und zitiert werden, in der Regel mit dem Aktenzeichen.

Archivierung
: Die Archivierung im juristischen Kontext betrifft allein Unterlagen der öffentlichen Verwaltung. Von „Archivgut“ wird dort erst dann gesprochen, wenn das Schriftgut bei der zuständigen Behörde ausgesondert, vom Archiv als archivwürdig eingestuft worden ist und „ewig“ verwahrt wird.

Aufbewahrung
: Die Aufbewahrung umfasst jede Form der Erhaltung eines Dokuments – unabhängig davon, ob aus informationstechnischer Sicht eine Speicherung im Datenmanagementsystem oder im Datenarchiv erfolgt, ob der Gesamtvorgang, zu dem das einzelne Dokument gehört, in der Bearbeitung abgeschlossen ist oder nicht oder ob eine bestimmte Aufbewahrungsdauer festgelegt ist.

Authentizität
: Die Authentizität elektronischer Dokumente erfordert, dass die eindeutige Bestimmung der Quelle der Daten.

Daten
: Oberbegriff für alle Informationen, die von elektronischen Medien verarbeitet oder gespeichert werden.

Dokument
: Alle Arten von Informationen, die zur Wahrnehmung durch den Menschen bestimmt sind und als Einheit zwischen Systemen oder Benutzern ausgetauscht werden können. Bei elektronischen Dokumenten sind die Informationen maschinell lesbar und verarbeitbar.

Dokumentart
: Abstrakte Bezeichnung eines Dokuments in Bezug auf seinen Inhalt, z.B. der Arztbrief.

Dokumentkategorie
: Anwendungsspezifische Bezeichnung einer nicht konkretisierten Anzahl und Art von Dokumenten, die zur Erfüllung einer bestimmten Funktion erforderlich sind, z.B. die ärztliche Dokumentation.

Elektronische Signatur
: Nach § 2 Nr. 1 SigG sind elektronische Signaturen: „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Der Begriff der elektronischen Signatur wird auch synonym zu „digitale Signatur“ verwendet. Die elektronische Signatur kann in der Sicherheitsstufen „einfache“ (§ 2 Nr. 1 SigG), „fortgeschrittene“ (§ 2 Nr. 1 SigG), „qualifizierte“ (§ 2 Nr. 1 SigG) und „akkreditierte“ Signatur (§ 15 Abs. 1 SigG) erzeugt werden.

Integrität
: Die Intregrität elektronischer Dokumente erfordert die Unversehrtheit der Daten, in dem Sinne, dass an dem Dokument keine Ergänzungen oder Löschungen vorgenommen worden sind.

Lesbarkeit
: Ist die Sichtbarmachung der in den Daten enthaltenen Informationen. Ein elektronisches Dokument ist nur dann lesbar, wenn die notwendige Hard- und Software die Daten verarbeiten und ihre Informationen interpretieren und dem menschlichen Betrachter in lesbarer Weise präsentieren kann.

Sicherungsmittel
: Systembezogene Sicherungsmittel beschränken durch eine individuelle Konfiguration des Archivsystems oder der auf dieses zugreifenden Komponenten den Zugriff auf die Daten, z.B. durch Berechtigungssysteme. Datenträgerbezogene Sicherungsmittel sind Speichermedien, die ein Überschreiben oder Verändern der auf ihnen abgelegten Informationen ausschließen, z.B. CD-ROM, DVD, WORM. Dokumentenbezogene Sicherungsmittel sind solche, die die elektronischen Dokumente selbst gegen die unbemerkte Veränderungen und unberechtigte Kenntnisnahme schützen, z.B. Verschlüsselungstechnologien.

Urkunde
: Eine Urkunde im Sinne der Zivilprozessordnung ist die Verkörperung einer Gedankenerklärung (als Material wird regelmäßig Papier verwendet) durch Schriftzeichen, die allgemein bekannt oder dem Gericht verständlich sind.

Verkehrsfähigkeit
: Die Verkehrsfähigkeit elektronischer Dokumente bezeichnet die Möglichkeit, Dokumente und Akten von einem System zu einem anderen übertragen zu können, bei der die „Qualität" des Dokuments sowie seine Integrität und Authentizität nachweisbar bleiben.

Vertraulichkeit
: Der Schutz vor unbefugter Kenntnisnahme zur Sicherung der Geheimhaltung personenbezogener Daten und betriebs- oder berufsbezogener Geheimnisse.

Vollständigkeit
: Erfordert die Sicherstellung des Bezugs mehrerer aufgrund eines inneren Zusammenhangs zu einer Sammlung oder auch Akte zusammengefasster Einzeldokumente.

Zeitstempel
: Authentische und unfälschbare Verknüpfung von Daten mit einem Datum. Ein Zeitstempel ist eine mit einer elektronischen Signatur versehene elektronische Bescheinigung eines Zeitstempeldienstes, dass ihm bestimmte elektronische Daten zum entsprechenden Zeitpunkt vorgelegen haben. Ein Zeitstempel kann in einfacher oder in „qualifizierter" Form (§ 2 Nr. 14 SigG) vorliegen.