ARTEC®
IT Solutions

WHITEPAPER

EMA® und Compliance – Whitepaper zur rechtskonformen Archivierung: Alle rechtlichen Aspekte im Überblick

INHALTSVERZEICHNIS

EDITORIAL

Prinzipiell ist es jedem irgendwie klar – so ganz genau kann es dann aber doch keiner sagen: Nicht nur Akten und Unterlagen, sondern auch elektronische und gescannte Dokumente, geschäftliche E-Mails und sogar aufgezeichnete Telefongespräche unterliegen in Deutschland gesetzlichen Aufbewahrungsfristen. Doch für welche Daten gilt das? Wie lange sind diese Fristen? Und was passiert zum Beispiel mit privaten E-Mails oder Spam?

Hierzu gibt es im Handelsgesetzbuch, der Abgabenordnung, der Europäischen Datenschutzgrundverordnung (DSGVO), aber auch in branchenspezifischen Leitlinien sowie in internationalen und EU-Richtlinien verschiedenste Regeln und Normen unterschiedlichster Konkretheit – vor allem gibt es aber auch viele Grauzonen.

Um in dieser Vielfalt den Überblick zu behalten und eine tatsächlich rechtskonforme Archivierung zu gewährleisten, finden Sie in diesem Whitepaper die wichtigsten rechtlichen Aspekte im Überblick und eine Einordnung unserer Lösung EMA für die ganzheitliche Archivierung aller geschäftlich relevanten Daten, Dokumente und Kommunikation.

IN WELCHEN GESETZEN UND VORSCHRIFTEN WIRD DIE ARCHIVIERUNG GEREGELT?

Soviel vorab: Den einen Paragraphen, der alle Fragen zur Archivierung klar beantwortet, gibt es leider nicht. Dafür finden sich aber in vielen nationalen und internationalen Gesetzen und Leitlinien Regeln, die es je nach Unternehmensstruktur und Branche zu beachten gilt, darunter zum Beispiel:

Gesetze und Richtlinien in der DACH-Region

Deutschland

- HGB: Handelsgesetzbuch § 257
- AO: Abgabenordnung § 147
- GoBD: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (als Ablösung von GDPdU und GoBS)
- SigG: Signaturgesetz
- UStG: Umsatzsteuergesetz
- KonTraG: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- WPHG: Wertpapierhandelsgesetz § 16 sowie § 34
- BDSG: Bundesdatenschutzgesetz
- TKG: Telekommunikationsgesetz
- BME: Bundesverband Materialwirtschaft, Einkauf und Logistik
- VOI: Verband Organisations- und Informationssysteme e.V.
- und weitere…

Österreich

- BAO: Bundesabgabenordnung §§ 131, 132
- UGB: Unternehmergesetzbuch § 190
- UStG: Umsatzsteuergesetz (§ 11)
- 516. Verordnung des Bundesministeriums für Finanzen (vom 28.12.2012)
- und weitere….

Schweiz

- OR: Obligationsrecht, Art. 957 ff.
- GeBüV: Geschäftsbücherverordnung Art. 2 Abs. 2
- HaREGV: Handelsregisterverordnung Art. 52 ff.
- MWStGV: Mehrwertsteuerverordnung Art. 43-45, 47 und 49
- StHG: Bundesgesetz über die Harmonisierung der direkten Steuern der Kantone und Gemeinden Art. 42
- StG: Bundesgesetz über die Stempelabgaben Art. 35
- Verordnung zur papierlosen Übermittlung und Aufbewahrung von elektronisch übermittelten Daten und Informationen (EIDI-V) vom 1.3.2002
- ZertES; Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur
- und weitere….

EU-Richtlinien

- GDPR: EU-Datenschutz-Grundverordnung (DSGVO)
- Basel II (bzw. Basel III)
- MiFID (bzw. MiFID II): EU-Richtlinie über Märkte für Finanzinstrumente
- Euro-SOX
- und weitere….

Internationale Richtlinien

- SOX: Sarbanes-Oxley Act
- USA: Patriot Act
- FRCP: Federal Rules of Civil Procedure
- GLGBA: Gramm-Leach-Bliley Act
- Dodd Frank Act: Dodd–Frank Wall Street Reform and Consumer Protection Act
- AML/CFT: Anti-Money Laundering/Combating the Financing of Terrorism
- FSMA 2000: Financial Services and Markets Act 2000
- HIPAA: Health Insurance Portability & Accountability Act
- SEC: Securities and Exchange Commission
- und weitere….

WAS MUSS ARCHIVIERT WERDEN?

Grundsätzlich wichtig zu wissen: Dokumente mit geschäftlichen Inhalten werden im kaufmännischen Verkehr als Handelsbriefe eingestuft und unterliegen damit exakt den gleichen Aufbewahrungspflichten wie normale Geschäftsbriefe. Laut §257 Handelsgesetzbuch müssen demnach nach deutschem Recht folgende Unterlagen geordnet aufbewahrt werden:

- Handelsbücher und Aufzeichnungen, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse, Lageberichte, Konzernabschlüsse und Konzernlageberichte; sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen
- Empfangene Handelsbriefe
- Wiedergaben der abgesandten Handelsbriefe
- Buchungsbelege

Doch das ist noch nicht alles: Zur Dokumentation und Nachvollziehbarkeit muss zudem auch jeglicher Schriftwechsel, durch den ein Geschäft vorbereitet, durchgeführt, abgeschlossen oder gegebenenfalls wieder rückgängig gemacht wird, entsprechend aufbewahrt werden. Dabei handelt es sich beispielsweise um Verträge, Vereinbarungen, Angebote, Rechnungen, Aufträge, Reklamationen oder Zahlungsbelege, die heutzutage in der Praxis meist elektronisch kommuniziert werden.

WIE LANGE MÜSSEN DOKUMENTE ARCHIVIERT WERDEN?

Als schnelle Faustregel kann man sagen, dass steuerlich und buchhalterisch relevante Dokumente bis zu zehn Jahre lang, Mails mit anderen geschäftlich bedeutsamen Inhalten bis zu sechs Jahre lang geordnet und revisionssicher (siehe unten) aufzubewahren sind. Die spezifischen, rechtssicheren Formulierungen zu dem Thema finden sich im Handelsgesetzbuch (§ 257 HGB) und in der Abgabenordnung (§ 147 AO):

- Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen, die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen sowie Buchungsbelege müssen **zehn Jahre** lang aufbewahrt werden.
- Empfangene Handels- oder Geschäftsbriefe, Wiedergaben der abgesandten Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind, müssen **sechs Jahre** lang aufbewahrt werden.

Die Fristen beginnen mit Schluss des Kalenderjahres, indem die Handels- oder Geschäftsbriefe versendet oder empfangen wurden oder die sonstigen Unterlagen entstanden sind. In der Praxis geht man daher faktisch von einer Aufbewahrungsfrist von **elf Jahren** aus.

Exkurs Österreich/Schweiz

In Österreich liegt die Regelaufbewahrungsfrist für Handelsbriefe zwischen drei und sieben Jahren und für Geschäftsbücher und Steuerbelege bei sieben Jahren. In der Schweiz werden zehn Jahre angesetzt.

Ausnahmen der Regel

Die Aufbewahrungsfrist läuft jedoch jeweils nicht ab, wenn die Unterlagen für Steuern von Bedeutung sind, für welche die Festsetzungsfrist noch nicht abgelaufen ist. Dasselbe gilt bei laufenden Prüfungen oder strafrechtlichen Ermittlungen.

Zudem können je nach **Branchenzugehörigkeit** oder **Dokumentenart** eigene Archivierungs-Regeln und -Fristen gelten: beispielsweise in der Pharma- oder Automobilindustrie mit Fristen bis zu 30 Jahren oder deutlich länger.

Auch für spezielle Dokumente wie zum Beispiel Versicherungspolicen, Gerichtsurteile oder Baupläne gelten eigene Gesetze: mit über 100 Jahren bzw. in den letzten beiden Fällen sogar mit dauerhaften Aufbewahrungspflichten.

Herausforderung Zukunftssicherheit

Unternehmen stehen daher laut Bundesamt für Sicherheit in der Informationstechnik (BSI) neben der Aufgabe der rechtlich korrekten Archivierung als solche vor weiteren großen technischen Herausforderungen. Für immer mehr elektronisch erzeugte, verarbeitete und gespeicherte Dokumente und Daten muss auch in ferner Zukunft die Lesbarkeit, Verfügbarkeit sowie Integrität und Authentizität gewährleistet bleiben[1].

→ 1 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

WELCHE KRITERIEN GIBT ES FÜR EINE RECHTSKONFORME ARCHIVIERUNG?

Die Frage, ob die im Unternehmen vorgenommene Archivierung auch tatsächlich den rechtlichen Vorgaben entspricht und somit „revisionssicher" ist, beschäftigt viele IT-Verantwortliche. Antworten finden sich in den Ordnungsvorschriften für die Buchführung und für Aufzeichnungen (§ 146 AO)[2] sowie den Vorgaben zur Führung der Handelsbücher (§ 239 HGB)[3]. Demnach geht es bei der Führung der Handelsbücher und sonstiger erforderlicher Aufzeichnungen primär um:

- Vollständigkeit
- Richtigkeit
- Zeitgerechtigkeit
- Ordnung
- Unveränderbarkeit
- Nachvollziehbarkeit

Mehr Rechtsklarheit durch die GoBD

Um dies zu konkretisieren und für die Unternehmen etwas mehr Rechtsklarheit zu schaffen, hat das Bundesfinanzministerium zudem die ab Januar 2015 geltenden „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff", kurz GoBD, veröffentlicht[4]. Diese lösen die vorherigen Grundsätze „GDPdU" und „GoBS" ab und fassen die Anforderungen der Finanzverwaltung an eine IT-gestützte Buchführung praxisgerecht zusammen. Betriebsprüfungen richten sich generell an den GoBD aus – im Falle einer festgestellten Nichteinhaltung kann unter Umständen die Buchführung verworfen werden.

Für die rechtssichere Archivierung ergeben sich daraus folgende Aspekte: Wie auch in den bereits oben aufgeführten Gesetzestexten gefordert, sollen alle relevanten Dokumente, E-Mails und Daten grundsätzlich **zeitgerecht**, **vollständig**, **manipulationssicher** und **jederzeit verfügbar** aufbewahrt werden. Zudem müssen die Daten und ihre Aufbewahrung jedoch auch jederzeit **nachvollziehbar** und **maschinell auswertbar** sein. Eine einfache Aufbewahrung in Form von Papier oder per Mikrofilm ist demnach also nicht ausreichend. Auch eine Langzeitarchivierung im eingesetzten ECM, DMS oder E-Mail-System stellt nach den GoBD keine passende Alternative dar, da die Anforderungen an die Unveränderbarkeit und Nachvollziehbarkeit hierbei in der Regel nicht zufriedenstellend erfüllt werden können.

Der Grundsatz der Unveränderbarkeit schränkt zudem auch eine **Umwandlung in ein anderes Format** für Archivierungszwecke extrem ein. Denn diese ist nur zulässig, wenn die maschinelle Auswertbarkeit weiterhin ermöglicht und keine inhaltliche Veränderung vorgenommen wird. Vor diesem Hintergrund verlangen die Finanzbehörden eine sichere Aufbewahrung aller Dokumente im **elektronischen Original**. Das gilt auch für alle aufzeichnungs- und aufbewahrungspflichtigen Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen, die im Unternehmen entstanden oder dort eingegangen sind: Sie alle sind im elektronischen Original aufzubewahren und dürfen nicht vor Ablauf der Aufbewahrungsfrist gelöscht werden. Eine alleinige Archivierung in **ausgedruckter Form** ist daher also nicht mehr zulässig. (Elektronisch erstellte Handels- und Geschäftsbriefe, die jedoch in Papierform verschickt wurden, dürfen wiederum (auch ausschließlich) in Papierform aufbewahrt werden.) Aus Gründen der Nachvollziehbarkeit fordern die GoBD zudem eine **Verfahrensdokumentation**, welche alle Maßnahmen zur Sicherung der Vollständigkeit, Nachvollziehbarkeit, Unveränderbarkeit und maschinellen Auswertbarkeit etc. genau beschreibt.

Architektur des Archivsystems

Bei der Konzeption des Archivsystems stellt sich vielen IT-Verantwortlichen im Auswahlprozess die Frage, ob es bestimmte Anforderungen an die Architektur des künftigen Systems zur Revisionssicherheit gibt. Beispielsweise, ob gegebenenfalls nur einmal beschreibbare Speicher eingesetzt werden dürften. Hierzu finden sich jedoch keine Einschränkungen oder Hinweise in den aktuellen Gesetzen. Demnach eignen sich auch gängige Festplatten oder andere Speichermedien, sofern die sonstigen Voraussetzungen erfüllt sind.

IDW RS FAIT 3

Mit der Stellungnahme „Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren" (IDW RS FAIT 3)[5] hat das Institut der Wirtschaftsprüfer in Deutschland e.V. eine Abhandlung über wichtige, grundlegende Kriterien zur ordnungsgemäßen elektronischen Archivierung zusammengestellt. Darin sind eine Reihe von Vorgaben und Anforderungen gebündelt. Sie betreffen die Grundsätze ordnungsgemäßer Buchführung beim Einsatz elektronischer Archivierungsverfahren beziehungsweise den vorschriftsmäßigen Betrieb einer IT-Lösung im Bereich Dokumentenmanagement.

→ 2 https://www.gesetze-im-internet.de/ao_1977/__146.html
→ 3 https://www.gesetze-im-internet.de/hgb/__239.html
→ 4 https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html
→ 5 IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3). Stand: 11.09.2015. ISBN: 978-3-8021-2254-5

Besondere Bedeutung hat IDW RS FAIT 3 somit auch für die elektronische Archivierung von Geschäftsbriefen wie beispielsweise E-Mails, Rechnungen, etc. In dem Dokument werden verschiedene Aspekte behandelt, darunter rechtliche, technische, organisatorische Belange, die zugrunde liegenden juristischen Grundlagen sowie Sicherheitsanforderungen und Risiko-Faktoren. Darüber hinaus werden konkrete Anregungen und Hinweise für die Gestaltung der IT-Infrastruktur gegeben. Die Anforderungen von IDW RS FAIT 3 basieren auf den Regeln des Handelsgesetzbuchs (HGB), Vorschriften der Abgabenordnung und GoBD und ergänzen diese. IDW RS FAIT 3 leitet aus der GoBD Sicherheits- und Betriebsanforderungen ab und spezifiziert diese für den DMS/ECM-Bereich. Als wichtige Kriterien für den Betrieb einer ECM-Lösung werden hier beispielsweise die Richtigkeit, Verfügbarkeit, Unveränderbarkeit, Nachvollziehbarkeit, Vertraulichkeit und Authentizität der Daten genannt und konkretisiert.

WER IST FÜR DIE RECHTSKONFORME ARCHIVIERUNG VERANTWORTLICH?

Im Sinne der „Geschäftsführerhaftung“ wurde auch die ordnungsgemäße Archivierung gesetzesseitig zur „Chefsache“ erklärt: die Verantwortung für die ordnungsgemäße Umsetzung aller rechtlichen Anforderungen zur Archivierung von E-Mails unterliegt der **Geschäftsführung** eines Unternehmens. Das bedeutet für Geschäftsführer von GmbHs bzw. Vorstände von Aktiengesellschaften eine persönliche Haftung bei Missachtung der Sorgfaltspflichten mit etwaigen zivilrechtlichen und strafrechtlichen Folgen:

- Steuerliche Konsequenzen, wie Strafzahlungen an das Finanzamt nach § 162 AO[6]
- eine Freiheitsstrafe von bis zu 5 Jahren bei Verletzung der Buchführungspflicht nach § 283 StGB[7]
- Schadensersatzansprüche nach § 280ff. BGB[8] und § 241 Abs. 2 BGB

Viele weitere Akteure sind für rechtssichere Datenaufbewahrung, IT-Sicherheit und den Datenschutz mitverantwortlich und ebenfalls mit ernsthaften rechtlichen Konsequenzen bedroht. Auch der Compliance-Officer, IT-Security-Officer und der Datenschutzbeauftragte müssen ggfs. in einem Rechtsstreit schlüssig darlegen können, alle erforderlichen und gebotenen Präventiv- und Notfallmaßnahmen ergriffen zu haben[9].

WAS GILT FÜR DIE VERSCHLÜSSELUNG ARCHIVIERTER DATEN?

Bei verschlüsselten Daten wird insbesondere ein Augenmerk auf die Prüfbarkeit gelegt: Denn auch hier muss nach den GoBD (Abs. 176) sichergestellt sein, dass der Prüfer bei einer Datenträgerüberlassung auf die Daten zugreifen kann und die maschinelle Auswertbarkeit weiterhin gewährleistet ist. Die tatsächliche Entschlüsselung der übergebenen Daten muss spätestens bei der Datenübernahme auf Systeme der Finanzverwaltung erfolgen. Die eingesetzten Schlüssel müssen folglich für denselben Zeitraum sicher aufbewahrt werden.

WAS GIBT ES HINSICHTLICH DER DATENSICHERHEIT ZU BEACHTEN?

Das Thema Datensicherheit spielt auch gemäß den GoBD (Pkt. 7 bzw. Abs. 103) eine wichtige Rolle, um die formelle Ordnungsmäßigkeit der Buchführung zu gewährleisten. Daten, Datensätze, elektronische Dokumente und Unterlagen sind demzufolge ausreichend zu schützen und gegen Verlust (zum Beispiel Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) und unberechtigte Eingaben und Veränderungen (beispielsweise durch Zugangs- und Zugriffskontrollen) zu sichern. Die Beschreibung der genauen Vorgehensweise zur Datensicherung ist Bestandteil der Verfahrensdokumentation und abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems.

LÖSCHEN - DATENSCHUTZ VS. ARCHIVIERUNG

Solange es nicht der gesetzlich geforderten Vollständigkeit und den entsprechenden Aufbewahrungsfristen widerspricht, dürfen Daten prinzipiell aus dem Archiv gelöscht werden. Das gilt zum Beispiel bei E-Mails für Spam oder private Mails. Allerdings ist es in der Praxis sehr schwer, konsistent und zuverlässig zwischen archivierungspflichtigen und nicht-archivierungspflichtigen Dokumenten zu unterscheiden. Um dem Grundsatz der Vollständigkeit zu entsprechen, entscheiden sich die meisten Unternehmen dazu, zum Beispiel prinzipiell alle E-Mails und alle erzeugten elektronischen Dokumente (unter anderem auch Scans und

→ 6 https://www.gesetze-im-internet.de/ao_1977/__162.html
→ 7 https://www.gesetze-im-internet.de/stgb/__283.html
→ 8 https://www.gesetze-im-internet.de/bgb/__280.html
→ 9 https://www.iitr.de/blog/datenschutzbeauftragte-und-strafrecht-verschaerfte-haftung-wie-compliance-officer/2765/

Printstreams) automatisiert zu archivieren. Auf diese Weise wird auch die Manipulationssicherheit gewährleistet, da die Mitarbeiter die Mails vor der Archivierung nicht mehr verändern oder gar löschen können. Dabei entsteht allerdings ein Spannungsfeld mit den Rechten der Mitarbeiter und den Kommunikationspartnern eines Unternehmens.

Berücksichtigung der DSGVO

Die Einführung der DSGVO im Jahr 2018 hat viele Anforderungen des Datenschutzes dringend gemacht. Somit ist das genannte Vorgehen vor dem Hintergrund des modernen Datenschutzes ebenfalls nicht haltbar. Daten sind danach grundsätzlich zu löschen, wenn der Zweck ihrer Verarbeitung erfüllt ist oder entfällt. Die DSGVO erlaubt (Art. 6) die Verarbeitung – und dazu zählt letztlich auch die systematische Speicherung grundsätzlich nur ausnahmsweise. Dementsprechend sind Daten nach dem Prinzip der Datensparsamkeit (Art. 5c) zu löschen, wenn kein entsprechender Ausnahmetatbestand (mehr) besteht. Durch die DSGVO werden die Rechte der von Datenverarbeitungsvorgängen Betroffenen gestärkt und sind nun gegenüber dem Verantwortlichen direkt durchsetzbar. Die Ausnahmen der DSGVO sind aber umfassend weit gefasst um es Unternehmen, Behörden und anderen Institutionen unter allen Umständen zu erlauben, ihren legitimen Zwecken nachkommen, dabei rechtliche Anforderungen erfüllen und ihre berechtigten Interessen wahren zu können.

Erstellung eines Löschkonzepts

Mit der Einhaltung aller gesetzlichen Anforderungen im Rahmen der Archivierung ist man bei Revisionen und gerichtlichen Auseinandersetzungen erst einmal auf der sicheren Seite. Vor rechtlichen Konflikten ist man jedoch leider dennoch nicht gefeit, da es in einigen Fällen bei konsequenter Umsetzung zu Differenzen mit anderen Gesetzen kommen kann, wie wir gesehen haben zum Beispiel dem Datenschutz. In praktisch allen Ratgebern zum Datenschutz in Unternehmen wird die Erstellung eines „Löschkonzeptes“ als integraler Bestandteil genannt. Damit ist die konkrete Festlegung von Aufbewahrungs- und Löschfristen für spezifizierte Datenarten in sogenannten Löschregeln gemeint[10]. Rechtskonforme Archivierung und Löschung müssen also zusammen gedacht werden[11].

Hinsichtlich der Priorisierung und Interessenabwägung zwischen Archivierungspflicht und Datenschutz stellen IT-Rechtler übrigens meistens die Archivierung an erste Stelle. Begründet wird dies zum Beispiel im Falle des Arbeitgeber-Arbeitnehmer Verhältnisses mit dem Begriff der „Erforderlichkeit“ der Datenaufbewahrung nach Art. 9 DSGVO. Allerdings muss der Arbeitgeber in solchen Fällen unbedingt seiner Informationspflicht über die Archivierung gemäß Art. 12 – 14 DSGVO nachkommen und alle Mitarbeiter vor der Einführung eines solchen Systems informieren.

Eine Archivierungslösung muss also umfangreiche Features besitzen, um Datenschutzkonform nach den neuesten Standards zu sein. Das betrifft natürlich zuallererst den Zugriffschutz und die Verschlüsselung, die durchgängig gewährleistet sein müssen, sowie die Datenminimierung zum Beispiel durch Vermeidung der Generierung von Duplikaten persönlicher Daten. Ein Archiv, das dem Datenschutz Rechnung trägt, muss aber zum Beispiel auch den Anwender in die Lage versetzen, gegebenenfalls persönliche Daten und Dokumente oder E-Mails, die sie enthalten, wieder aufzufinden und gegebenenfalls kontrolliert – d.h. insbesondere protokolliert – zu löschen. Nur so können die umfangreichen Rechte der Betroffenen aus Artikel 15 – 22 DSGVO zum Beispiel auf Auskunft und Löschung sicher berücksichtigt werden.

→ 10 DIN Norm 66389 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“

→ 11 Dieses Thema würde den Rahmen dieses Papers sprengen. Als weiterführende Literatur siehe zum Beispiel Durmus, Selzer, und Pordesch, „Das Löschen nach der DSGVO“, Datenschutz und Datensicherheit 43 (12) 2019; Macit und Selzer, „DATENSCHUTZKONFORMES LÖSCHEN PERSONENBEZOGENER DATEN IN KUNDEN- BEZIEHUNGSMANAGEMENTSYSTEMEN“. BvD News 1/2020

BESONDERHEITEN VON E-MAILS

Unter den vielfältigen modernen Kommunikationsformen in Unternehmen ist und bleibt die E-Mail eine der wichtigsten, wenn es darum geht, Dinge verbindlich zu machen. E-Mails mit ihren Anhängen sind daher in vielen Fällen als Geschäftsbriefe in Aufbewahrungspflichten einbezogen. E-Mails sind im Geschäftsbetrieb allgegenwärtig und stellen besondere Anforderungen an die Aufbewahrung. Ihre umfangreiche, leistungsfähige Struktur bestehend aus Headern (Metadaten), Body – heutzutage häufig formatiert als HTML – und (kodierten) Anhängen erfordert besondere Sorgfalt bei der Überführung in das Archiv und auch bei der Reproduktion. Würde eine E-Mail also beispielsweise (etwa um Langzeitsicherheit zu erreichen) als PDF-A-Datei gespeichert, so könnten dabei unter Umständen wichtige Informationen über den Absender, den Betreff, das Zustelldatum, etc. aus den Metadaten verloren gehen, was wiederum Auswirkungen auf die Nachvollziehbarkeit hätte. Auch zugehörige Dateianhänge müssen archiviert werden, sollte die E-Mail ohne diese Anlagen unklar oder unvollständig sein.

E-Mails sind aber zuvorderst auch ein Kommunikations- und nicht nur ein Dokumentationsmedium. Bedenkt man die Vielzahl an ein- und ausgehenden E-Mails jedes einzelnen Mitarbeiters innerhalb eines Unternehmens pro Tag, wird schnell klar, dass eine einfache und vor allem eindeutige Zuordnung in archivierungspflichtige und nicht-archivierungspflichtige E-Mails nahezu unmöglich ist. Daher entscheiden sich viele Unternehmen dazu, einfach alle **E-Mails** zu archivieren. Der Umgang mit Spam und privaten E-Mails stellt uns dabei vor besondere Herausforderungen.

Exkurs: Müssen eigentlich auch Messages archiviert werden?

Neben der E-Mail-Kommunikation nimmt auch im geschäftlichen Bereich das Instant Messaging immer mehr zu. Vor diesem Hintergrund stellt sich natürlich die Frage, ob auch diese Nachrichten archiviert werden müssten. Nach aktueller Meinung werden diese „Messages“ jedoch wie Telefonate eingestuft und müssen daher aktuell nicht aufbewahrt werden, wenn dies nicht explizit für einen Vorgang, zum Beispiel einen Vertragsabschluss vorgesehen und angekündigt ist. Findet eine wichtige, unternehmensrelevante Kommunikation statt, empfiehlt es sich dennoch, diese in Form einer Notiz zu dokumentieren und entsprechend zu archivieren.

Werden E-Mails als Beweismittel anerkannt?

Bei gerichtlichen Auseinandersetzungen werden zunehmend auch E-Mails zur Klärung der Sachverhalte hinzugezogen. Ob diese als Beweis anerkannt werden, hängt jedoch u.a. davon ab, ob es sich um elektronisch signierte E-Mails handelt. Denn elektronische Dokumente genießen in der freien richterlichen Beweiswürdigung nicht per se den gleichen Status wie eine Urkunde, gelten aber grundsätzlich als Augenscheinbeweis nach § 371 Abs. 1 Satz 2 der Zivilprozessordnung[12].

Elektronische Signaturen

Auf der sicheren Seite ist man bei der Archivierung mit qualifizierten elektronischen Signaturen. Denn diese können gemäß § 126a BGB[13] eine per Gesetz geforderte Schriftform auf Papier ersetzen. Somit können die Inhalte qualifiziert elektronisch signierter E-Mails vor Gericht entsprechend als Beweis gewertet werden. In Übereinstimmung mit der europäischen eIDAS-Richtlinie[14] ist eine qualifizierte elektronische Signatur eine fortgeschrittene elektronische Signatur, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurde[15]. Aber ob mit oder ohne Signatur: Neben den generellen Archivierungspflichten empfiehlt sich eine entsprechende Aufbewahrung des E-Mail-Verkehrs auf jeden Fall, da Mails heutzutage oftmals der einzige Nachweis für getroffene Absprachen und zeitliche Zusammenhänge im Streitfall sind.

Spannungsfeld Spam-Filter vs. Vollständigkeit

Der Umgang mit Spam-E-Mails wirft ebenfalls einige Fragen auf. Einerseits möchte man natürlich nicht die komplette Masse täglicher Spam-Mails jahrzehntelang mit archivieren. Denn dies führt nicht nur zu einem deutlich höheren Speicherbedarf, sondern wirkt sich mit der Zeit auch auf die Qualität der Suchergebnisse aus. Andererseits dürfen ja aus Gründen der Vollständigkeit und vor allem der Manipulationssicherheit auch keine geschäftsrelevanten empfangenen E-Mails aus dem Archiv gelöscht werden.

→ 12 https://dejure.org/gesetze/ZPO/371.html
→ 13 https://www.gesetze-im-internet.de/bgb/__126a.html
→ 14 Die eIDAS Richtlinie über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ersetzt seit Juli 2014 die Signaturrichtlinie aus dem Jahr 1999. Siehe https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910
→ 15 https://de.wikipedia.org/wiki/Qualifizierte_elektronische_Signatur

Bei einer Spam-Filterung vor der Archivierung bliebe schließlich das Risiko, dass archivierungspflichtige E-Mails versehentlich im Spam-Filter hängen bleiben und somit nicht im Archiv ankommen. Das Archivierungsverfahren wäre somit nicht mehr rechtskonform. Unternehmen müssen daher im Vorfeld entscheiden, welche Konsequenzen sie am ehesten tragen möchten. Eine auch rechtlich gesehen mögliche Alternative wäre es in diesem Kontext beispielsweise, als Spam identifizierte E-Mails direkt vor der Annahme vom eigenen E-Mail-Server abweisen zu lassen. Denn solange die Nachrichten nicht angenommen werden, gelten sie auch nicht als zugestellt und es besteht somit auch keine Pflicht zur Archivierung.

Umgang mit privaten E-Mails

Ist den Arbeitnehmern die private E-Mail-Nutzung gestattet, kann es zu Konflikten mit den Datenschutzrichtlinien kommen, da der Arbeitgeber in diesem Falle rechtlich als Telekommunikationsanbieter betrachtet wird und somit der DSGVO, dem Bundesdatenschutzgesetz[16] (BDSG) und dem Telekommunikationsgesetz[17] (TKG) unterliegt.

Um diese datenschutzrechtlichen Konflikte zu umgehen, wird manchmal geraten, die private E-Mail-Nutzung im Unternehmen komplett zu verbieten oder die ausschließliche Verwendung externer E-Mail-Dienste vorzuschreiben. Doch selbst wenn die private Nutzung der geschäftlichen E-Mail-Accounts untersagt ist, sind noch nicht alle datenschutzrechtlichen Aspekte berücksichtigt: Denn auch dienstliche E-Mails können persönliche, vertrauliche und somit „schützenswerte“ Inhalte enthalten, beispielsweise bei einer Kommunikation mit dem **Betriebsarzt** oder dem **Betriebsrat**. In jedem Fall empfiehlt es sich, Regelungen zur privaten E-Mail Nutzung schriftlich zu fixieren und auch entsprechend konsequent zu kontrollieren, da juristisch gesehen eine Duldung der privaten Nutzung bereits als stillschweigende Erlaubnis bewertet werden kann. Private E-Mails können aber grundsätzlich archiviert werden wenn die private E-Mail Nutzung erlaubt ist. In der Orientierungshilfe der Konferenz der Datenschutzbehörden aus 2016[18] heißt es dazu:

„Haben Beschäftigte im Zusammenhang mit der betrieblichen E-Mail-Nutzung in die Regelungen zur privaten Mailnutzung eingewilligt, sind sie darauf hinzuweisen, dass im Zusammenhang mit einer Archivierung (z.B. gem. § 257 HGB, § 147 AO) auch eine Archivierung ihrer privaten E-Mails erfolgen kann. Den Beschäftigten sollte jedoch Gelegenheit gegeben werden, private Mails zu löschen oder an ihren privaten Account weiterzuleiten.“

Es ist klar, dass eine zu simple Archivierungslösung nicht geeignet sein kann, mit privaten E-Mails von Mitarbeitern in Firmen umzugehen. Ein intelligentes Archiv, mit vielfältigen Sicherheitsfunktionalitäten und Möglichkeiten Zugriffe feingranular zu kontrollieren und zu protokollieren, kann dies aber durchaus ermöglichen, wenn einige einfache Grundsätze beachtet werden. Ausgangspunkt ist, dass private Kommunikation natürlich grundsätzlich nicht in das Archiv der Firma gehört und dort nur ausnahmsweise gespeichert sein kann. Den Mitarbeitern muss wie beschrieben ermöglicht werden, E-Mails als privat zu klassifizieren und gegebenenfalls zu löschen. Dazu sollte auch ein Filtern von Mails, bevor sie in das Archiv gelangen, unterstützt werden. Vielfältige Möglichkeiten, wie spezielle Attribute, separate Ordner oder nutzerdefinierte Filter bieten sich hier an.

Es wird in der Regel vorkommen, dass private E-Mails gelegentlich mit archiviert werden. Für diesen Fall sollte eine kontrollierte Löschmöglichkeit vorgesehen werden, die zum Beispiel regelt, dass E-Mails, die ein Nutzer als privat erkennt, nach einer gewissen Zeit nur unter Zuhilfenahme des 4-Augen-Prinzips und der gleichzeitigen Einsichtnahme durch eine vertrauenswürdige Instanz wie dem Betriebsrat oder dem Datenschutzbeauftragten gelöscht werden können.

RECHTSSICHERE ARCHIVIERUNG MIT EMA - REVISIONSSICHERHEIT

Bei der Entwicklung und der kontinuierlichen Weiterentwicklung von EMA wurde und wird rechtlichen Regelungen laufend Rechnung getragen, um alle Vorgaben abzubilden. Wie zuvor gezeigt wurde, sind relevante Regeln vielfältig und kommen aus verschiedenen Rechts- und Verwaltungsbereichen. Einige praktische Systematiken von Anforderungen haben den Anspruch, eine Synthese der vielen Anforderungen für Eigenschaften, Aufbau, Organisation und Betrieb von elektronischen Archiven zu bilden. Dazu zählt zum Beispiel die schon beschriebene IDW RS FAIT 3. An solch konkreten Katalogen lassen sich technisch-organisatorische Maßnahmen und Komponenten wie die Archivierungslösung EMA bezüglich ihrer Geeignetheit zur Umsetzung rechtssicherer Archivierung messen. Im Folgenden skizzieren wir eine entsprechende Evaluation von EMA am besonders prägnanten und häufig verwendeten Begriff der **Revisionssicherheit**.

→ 16 http://www.gesetze-im-internet.de/bdsg_2018/index.html
→ 17 http://www.gesetze-im-internet.de/tkg_2004/index.html
→ 18 Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz. https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf

Der Begriff der Revisionssicherheit beschreibt die Dokumentenaufbewahrung und Datenhaltung einer Organisation aus der Perspektive eines Prüfers. Dies fokussiert den Blick auf Kriterien, deren Einhaltung es (Wirtschafts-) Prüfern erlaubt ihre inhaltlichen Prüfungen vertrauensvoll durchzuführen. Das heißt konkret, dass sie sich bei ihrer Arbeit darauf verlassen können, dass die ihnen vorgelegten Daten und Dokumente authentisch, unverändert und vollständig sind und das für alle diese Eigenschaften auch Nachweise vorgelegt werden können.

Eine umfassende Anforderung wie Revisionssicherheit bezieht sich naturgemäß auf alle organisationsweiten Maßnahmen und eingesetzten Mittel zur Aufbewahrung von Dokumenten, E-Mails und allen anderen Daten. Ein Archivsystem ist dabei – neben beispielsweise dokumentierten Prozeduren und Verfahren – nur ein, wenn auch zentraler, Baustein. Häufig taucht das Thema Zertifizierung im Zusammenhang mit Revisionssicherheit auf. Hierzu ist zweierlei festzuhalten: Der Begriff ‚Revisionssicherheit' als solcher ist weder durch Rechtsvorschriften festgelegt noch technisch-organisatorisch normiert. Weiterhin kann es keine Zertifizierungen der ‚Revisionssicherheit' einzelner technischer Komponenten oder auch ganzer Archivierungslösungen geben – die Spezifika der Gesamtorganisation können niemals außen vor bleiben. Daraus folgt, dass die Prüfung der Revisionssicherheit der Dokumentenaufbewahrung einer Organisation ein anspruchsvolles Unterfangen ist. Solche Prüfungen werden zum Beispiel vom TÜViT[19] durchgeführt und entsprechende Testate ausgestellt.

Die Anforderungen für Revisionssicherheit leiten sich ebenfalls aus verschiedenen rechtlichen Vorschriften wie HGB, AO und GoBD ab. In diesen Rechtsregeln treten die Anforderungen aber eher sporadisch auf, sind noch immer recht allgemein formuliert und lassen viele konkrete Fragen aus der Praxis unbeantwortet. Aus diesem Grund hat der VOI (Verband Organisations- und Informationssysteme e.V.) bereits 1996 erste Merksätze zur revisionssicheren elektronischen Archivierung verfasst, die im Laufe der Zeit noch weiter ergänzt wurden. Die zehn aktuellen Grundsätze des VOI zur Revisionssicherheit decken vielfältige Eigenschaften ab, die eine klassische oder elektronische Aufbewahrung erfüllen muss. Sie lassen sich in vier funktionale Anforderungsbereiche gruppieren, die den Funktionen eines Archivsystems entsprechen[20]. Damit lässt sich konkret bewerten, ob ein Archivsystem im Rahmen einer umfassenden Aufbewahrungsstrategie geeignet ist, um Revisionssicherheit bis zum erforderlichen Grad zu erreichen. Die vier Funktionsgruppen sind:

A. Sichere Übernahme

Dokumente und Daten sollen vollständig und unverändert in das Archiv übernommen werden. Dies hat vielfältige Implikationen. Formatumwandlungen sollten ebenso unterbleiben wie eine Zwischenablage in ungeschützten Speicherorten. Bei der Übertragung dürfen keine Verluste auftreten.

B. Geschützte Aufbewahrung

Dies ist die Kernfunktion jedes Archivs. Sie bedingt etliche Teilfunktionen wie Zugriffsschutz und –kontrolle, dauerhafte Integritätssicherung digitaler Daten (analog zur regelmäßigen Überprüfung der Leserlichkeit von Papierdokumenten) und Protokollierung aller Vorgänge.

C. Korrektes Auffinden

Jedes zu einer inhaltlichen Prüfung einer Organisation nötige Dokument muss zeitnah und ohne großen Aufwand gefunden werden können. Dies muss auch bei einer sehr großen Dokumenten- oder Datenmenge gelten. Bestehende Zugangsbeschränkungen sind dabei zu beachten. Ob Daten strukturiert abgelegt sind und anhand dieser Struktur gefunden werden, oder ob das Archivsystem Dokumente unstrukturiert vorhält mittels Indizes oder Metadaten durchsucht, ist dabei unerheblich.

D. Getreue Wiedergabe

Dokumente sind originalgetreu wiederzugeben. Dazu kann das Archivsystem zum Beispiel eigene Anzeige- und Ausgabemethoden umfassen. Anhand des gefundenen Dokuments und beigefügter Protokolle über die Aufbewahrung muss sich die Einhaltung aller vorgenannten Anforderungen nachprüfen lassen.

→ 19 Liste: ‚Revisionssichere Archivierung von Dokumentenmanagement-Lösungen'. https://www.tuvit.de/de/leistungen/zertifizierung/revisionssichere-archivierung-von-dokumentenmanagement-loesungen/
→ 20 Vergleiche hierzu unser Whitepaper ‚Backup vs. Archive' in dem Grundkonzepte der Archivierung erläutert werden.

GRUNDSÄTZE VS. TECHNISCH/ORGANISATORISCHE ANFORDERUNGEN

EMA deckt alle Anforderungsbereiche vollumfänglich ab und ist damit prädestiniert, ein Kernelement der revisionssicheren Aufbewahrung im Unternehmen zu sein. Organisatorische Prozesse für die Revisionssicherheit lassen sich einfach und effektiv rund um EMA als Archiv für alle Arten von Unternehmensdaten gestalten.

VOI-GRUNDSÄTZE

1. Jedes Dokument muss nach Maßgabe der rechtlichen und organisationsinternen Anforderungen ordnungsgemäß aufbewahrt werden.
2. Die Archivierung hat vollständig zu erfolgen – kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
3. Jedes Dokument ist zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren.
4. Jedes Dokument muss mit seinem Original übereinstimmen und unveränderbar archiviert werden.
5. Jedes Dokument darf nur von entsprechend berechtigten Benutzern eingesehen werden.
6. Jedes Dokument muss in angemessener Zeit wiedergefunden und reproduziert werden können.
7. Jedes Dokument darf frühestens nach Ablauf seiner Aufbewahrungsfrist vernichtet, d.h. aus dem Archiv gelöscht werden.
8. Jede ändernde Aktion im elektronischen Archivsystem muss für Berechtigte nachvollziehbar protokolliert werden.
9. Das gesamte organisatorische und technische Verfahren der Archivierung kann von einem sachverständigen Dritten jederzeit geprüft werden.
10. Bei allen Migrationen und Änderungen am Archivsystem muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein.

ANFORDERUNGSBEREICHE

SICHERE ÜBERNAHME

GESCHÜTZTE AUFBEWAHRUNG

KORREKTES AUFFINDEN

GETREUE WIEDERGABE

→ In der Abbildung ist die Zuordnung der VOI-Grundsätze zu den Anforderungsbereichen dargestellt.

SICHERE ÜBERNAHME

Für die sichere Übernahme sorgt bei EMA die direkte Anbindung an alle Datenquellen für die eine Vielzahl an Möglichkeiten bestehen. EMA macht sich dabei nicht abhängig vom Integritätszustand externer Systeme und Datenbanken, sondern übernimmt Daten in dem Moment in dem sie am Ein-/Ausgabegerät, Speicherort oder im Netzwerk entstehen. Dabei gibt es keine Zwischenspeicherung wie bei manch anderen Systemen, die zum Beispiel Daten zunächst in Archivcontainern sammeln. Alle Daten und Dokumente, egal ob E-Mails, Dateien, Druckausgaben, Scans, Telefonie- & Sprachdateien, Daten aus ECM, DMS oder anderen Systemen und Fachanwendungen werden direkt und ohne irgendeine Transformation in EMA übernommen. Quelle und Ursprung jedes eingehenden Datensatzes werden protokolliert und mit archiviert. Die Originaldaten werden mit Eingangszeitstempeln versehen und kryptographisch nach höchsten Standards mit fortgeschrittenen elektronischen Signaturen dauerhaft gegen Veränderung gesichert und sodann verschlüsselt abgelegt. Weitere Metadaten werden nach Bedarf (zum Beispiel zum erleichterten Wiederauffinden oder als Ordnungsmerkmal) erzeugt und ebenso gesichert. Neue und geänderte Daten werden immer separat als neue Archivdaten übernommen (implizite Versionierung). Darüber hinaus verfügt EMA über leistungsfähige Importfunktionen für Altdatenbestände, die nach denselben Prinzipien funktionieren.

GESCHÜTZTE AUFBEWAHRUNG

Die geschützte Aufbewahrung wird bei EMA durch eine Vielzahl an integrierten Maßnahmen sichergestellt. Das Sicherheitsfundament des Archivs bildet der hardwarebasierte Schutz durch modernste Trusted Computing Technologie. EMA wird damit zum Schlüssel und Garant aller archivierten Daten, eine Veränderung der Daten im Archivspeicher durch Dritte ist unmöglich und ein Versuch kann durch Konsistenzchecks jederzeit aufgedeckt werden. Durch die Kombination von hardwarebasiertem Integritätsschutz mit verketteten Hashwerten und digitalen Signaturen (ähnlich der Blockchain-Technologie) sowie Verschlüsselung der Archivdaten erreicht EMA höchste Langzeitsicherheit auch für längste Aufbewahrungsfristen[21]. Zudem kann EMA automatisch korrupte Archivdaten erkennen und korrigieren. Für noch höhere Anforderungen an Sicherheitsnachweise lassen sich eingehende Daten mit von einem ANA-Server unabhängig erzeugten kryptographischen Zeitstempel versehen. Alle Operationen im Archiv werden von EMA sicher protokolliert, womit die Nachvollziehbarkeit aller Aktionen – durch Nutzer oder automatisch – gewährleistet ist. Schließlich schützt EMA Archivdaten durch ausgefeilte, rollenbasierte Zugriffskontrollen und besondere Funktionen wie dem Zugriff nach dem 4-Augen-Prinzip. Als eines von wenigen Archivierungssystemen am Markt bietet EMA mit dem 4-Augen-Prinzip eine praxisnahe Lösung für Zugriffsicherheit und Datenschutz. Viele Produkte, die von ihren Herstellern mit dem Prädikat „rechtskonform“ beworben werden, räumen Administratoren Zugriffsmöglichkeiten ein, die mit umfassendem, DSGVO-konformem Datenschutz nicht vereinbar sind. Durch das 4-Augen-Prinzip kann zum Beispiel der Zugriff auf besonders sensitive Dokumente oder E-Mails nur gemeinsam mit einer zusätzlichen Person, etwa einem Mitglied des Betriebsrats, erfolgen.

→ 21 Wollte ein Angreifer Daten im Archiv verändern müsste er oder sie nicht nur den Hashalgorithmus und die digitale Signatur zum Eingangszeitpunkt brechen sondern auch die verschlüsselten Daten austauschen, also die Verschlüsselung aushebeln.

KORREKTES AUFFINDEN

Das zielgenaue Suchen und Auffinden von Daten ist eine der zentralen Stärken von EMA. Der hoch performante Volltextindex über alle Medien, Dokumenten- und Datenarten erlaubt eine blitzschnelle Suche über beliebig große Datenbestände und verteilte Standorte. Mit der umfangreichen, logikbasierten Suchfunktion mit ihrem modernen, intuitiven Interface ist sichergestellt, dass unmittelbar alle relevanten Dokumente und Daten zu einem zu prüfenden Vorgang zur Verfügung stehen. Dabei greifen Zugriffskontrolle und Datenschutzregeln auch bei der Suche, zum Beispiel durch eine automatische und fein einstellbare Begrenzung der Ergebnisanzeige. Suchvorgänge werden sicher protokolliert. Damit ist jederzeit nachvollziehbar, wer wann mit welchem Suchbegriff eine Suche gestartet hat, von wo aus der Zugriff erfolgte, welches Dokument geöffnet wurde, etc.

GETREUE WIEDERGABE

EMA garantiert die originalgetreue Wiedergabe für alle archivierten Objekte und enthält für alle Eingangsdatentypen eingebaute Viewer, die den gängigen technischen Standards entsprechen. Damit bleiben Daten dauerhaft darstellbar. Die Originaltreue wird dabei unmittelbar durch Prüfung und Anzeige der digitalen Signatur augenscheinlich erwiesen. Daten und Signaturen lassen sich ohne Aufwand auf beliebige Medien exportieren und externen Prüfern zugänglich machen. Die gerichtsfeste Beweiskraft des gesamten Archivbestandes ist durch die umfangreichen kryptographischen Sicherungsmaßnahmen und die vollständige Protokollierung aller Ereignisse im Archiv gewährleistet. Für die inhaltliche Auditierung bietet EMA mit eDiscovery und Case Management mächtige Funktionen, mit denen sich Daten für Prüffälle strukturiert zusammenfassen lassen. Damit kann die Vollständigkeit und Sachbezogenheit der zu prüfenden Dokumente nachvollzogen werden.

Ein entscheidender Faktor für die revisionssichere Archivierung ist hier die Sicherstellung des Beweiswerts beziehungsweise des unveränderten Originalzustands. Speziell für E-Mails trennen einige Wettbewerber zum Beispiel E-Mails bei der langfristigen Speicherung in einzelne Bestandteile wie Body, Header und Anhang. Die Problematik dabei: Werden diese Fragmente später wiederhergestellt, kann nicht von einem unveränderten Originalzustand gesprochen werden. Gleiches gilt, wenn statt der Aufbewahrung im ursprünglichen Format eine Konvertierung der Mails in typische Langzeitformate wie etwa TIFF oder PDF erfolgt. EMA löst diesen Aspekt durch die Speicherung aller Daten im kompletten Originalzustand und bei E-Mails inklusive aller Attachments. So wird sichergestellt, dass sich später in Verbindung mit den digitalen Zeit- und Datumsstempeln zweifelsfrei die unveränderte Echtheit eines Dokuments / einer E-Mail belegen lässt.

FAZIT

EMA ist bereits durch die grundsätzliche Konzeption als hochsicheres, in sich geschlossenes System darauf ausgelegt, die geltenden Anforderungen zur rechtskonformen Archivierung zu erfüllen, egal ob EMA in der Cloud, gehostet oder On-Premises eingesetzt wird. Dies umfasst wie bereits gezeigt, den Schutz vor einer nachträglichen Veränderung archivierter Daten, die Zugriffs- und Datensicherheit, den Schutz vor Missbrauch durch unbefugte Dritte sowie die Möglichkeit der schnellen und vollständigen Wiederherstellung von Dokumenten aus dem Archiv während der gesamten Aufbewahrungsfrist. Zusammenfassend werden mit EMA Daten so archiviert, dass die Erfüllung der Anforderungen der Revisionssicherheit ohne großen organisatorischen Aufwand oder zusätzliche technische Maßnahmen vollständig umgesetzt, stringent dokumentiert und leicht geprüft werden können. Revisoren und Auditoren können EMA direkt als Arbeitsplatz nutzen und auch ihre Zugriffsrechte können nach gesetzlichen Vorgaben und den Richtlinien des Unternehmens durchgesetzt werden. EMA wird so zum zentralen Baustein eines umfassenden, organisationsweiten Daten- und Dokumentenarchivs. Dies erleichtert insbesondere die Zertifizierung des Anwendungssystems durch Instanzen wie zum Beispiel TÜViT[22].

→ 22 ARTEC unterstützt Sie gerne bei der Erstellung entsprechender Verfahrensdokumentationen.

CHECKLISTE ZUR RECHTSKONFORMEN E-MAIL-ARCHIVIERUNG

	EMA	Vergleichsprodukt
Vollständigkeit	✓ Automatische, vollständige Archivierung aller ein- und ausgehenden sowie internen E-Mails inklusive Anhänge.	
Richtigkeit	✓ Fortgeschrittene digitale Signatur garantiert Authentizität. ✓ Langzeitsicherheit durch Blockchain-artige kryptographische Technologie. ✓ Automatische Erkennung und Korrektur korrupter Datensätze.	
Zeitgerechtigkeit	✓ Alle ein- und ausgehenden E-Mails werden unmittelbar archiviert.	
Zugriffsregelungen	✓ Zugriffschutz durch Anbindung an LDAP, Open LDAP, Active Directory und andere. ✓ Administrativer Zugriffschutz unter Verwendung des 4-Augen-Prinzips.	
Originalformat	✓ Archivierung im unveränderten Originalformat (SMTP, RFC 2822).	
Manipulationssicherheit	✓ Digitaler Zeit- und Datumsstempel dokumentiert Originalität bzw. jegliche Änderungen.	
Nachvollziehbarkeit	✓ Jederzeitiger, schneller Zugriff auf archivierte Daten. ✓ Schnelle, leistungsstarke Suchfunktion und einfache Wiederherstellung. ✓ Jedes Dokument (auch in E-Mail Anhängen) wird automatisch indexiert und ist im Volltext durchsuchbar.	
Maschinelle Auswertbarkeit	✓ Sämtliche Archivdaten stehen stets zur maschinellen Auswertung zur Verfügung und können über konkrete Suchanfragen, Export-Dateien oder spezielle APIs bereitgestellt werden. ✓ Mit eDiscovery und Case Management stehen mächtige Funktionen zum kontextbezogenen Auffinden, Filtern und Herausgeben zugehöriger Daten zur Verfügung.	
Aufbewahrungsfristen	✓ Über Attribute-System individuell definierbar.	
Zukunftssicherheit	✓ Unabhängig vom verwendeten Mail-Server, Hardwarekomponenten oder Betriebssystem einsetzbar. ✓ Auch Migration auf sämtliche Arten von Archiv-Speicher fester Bestandteil des Konzepts.	
Verschlüsselung	✓ Alle Dokumente werden mit EMA individuell verschlüsselt. ✓ Fortschrittliche, ausgeklügelte Verschlüsselungs-Konzepte sorgen für maximale Sicherheit: Personalisierte Schlüssel individuell pro Kunde, Auslieferung von Ersatzgeräten nur an autorisierte Kunden, Sicherheit auf Archivspeicher ausgedehnt.	
Löschen aus dem Archiv	✓ Nur mit entsprechenden Administrator-Rechten möglich. Mindestvorhaltezeiten und Löschfristen und –regeln können bindend und somit absolut manipulationssicher eingerichtet werden. ✓ Protokolliertes Löschen. ✓ Löschvorgaben nach DSGVO können durch Fallbezogenes suchen mit eDiscovery und Löschregeln abgebildet werden.	
Security	✓ Geschlossenes System, hochsichere Software mit ARTEC-OS. ✓ Trusted-Computing-Technologie, asymmetrische (Signatur) und symmetrische (Verschlüsselung) Kryptographie nach neuesten Standards und sicheres Logfile für maximale Datensicherheit. ✓ Permanente Überwachung sicherheitsrelevanter Authentifizierungen. ✓ Single-Sign-On. ✓ Granulare Zugriffsregeln. ✓ 4-Augen-Prinzip.	
Signaturen	✓ Jedes Dokument erhält einen digitalen Datums- und Zeitstempel sowie eine fortgeschrittene elektronische Signatur durch eine dritte vertrauenswürdige Partei (ANA-Server).	
Datenschutz	✓ Verschlüsselung und granulare Zugriffsrechte. ✓ Separat geschützte Metadaten. ✓ Zugriffsprotokolle. ✓ Datensparsamkeit durch Filter. ✓ Aufbewahrungsfristen und kontrolliertes Löschen. ✓ 4-Augen-Prinzip.	
Private E-Mails	✓ Können gefiltert und über Attribute-System entsprechend gekennzeichnet und somit auch für Administratoren und Vertreter „maskiert“ und ausgeblendet werden.	
Spam	✓ Ausschluss von Spam konfigurierbar und über Attribute-Editor zudem weiter klassifizierbar: Spam kann zum Beispiel komplett ausgeschlossen oder nur ausgeblendet werden.	
Ordnungsmäßigkeit	✓ Durch Umsetzung aller Kriterien für Revisionssicherheit.	

ANHANG: AUFBEWAHRUNGSFRISTEN

Nachfolgend finden Sie eine Übersicht der gesetzlichen Aufbewahrungsfristen der IHK Frankfurt am Main, alphabetisch angeordnet nach Schriftgutarten. Entscheidend für die Frist ist jedoch nicht die Bezeichnung des Dokuments allein, sondern seine Funktion innerhalb der Organisation. Es besteht kein Anspruch auf Vollständigkeit und Richtigkeit. Die Zahl hinter dem aufgelisteten Schriftgut steht für dessen Aufbewahrungsfrist in Jahren.

A

Abhängigkeitserklärungen	10
Abkürzungsverzeichnis (erklärend)	10
Abrechnungsunterlagen	10
Abschlagszahlungen	10
Abschlussbuchungsbelege	10
Abschlusskonten	10
Abschlussrechnungen	10
Abschreibungsunterlagen	10
Abtretungserklärungen	6
Abwertungsbelege	10
Akkordunterlagen	10
Akkreditive	6
Aktenvermerke	6
An-, Ab- und Ummeldungen zur Krankenkasse	6
Änderungsnachweise der EDV-Buchführung	10
Angebote mit Auftragsfolge (erhaltene und Kopien versandter)	6
Angestelltenversicherung (Belege)	10
Anhang (zum Jahresabschluss)	10
Anlagenvermögensbücher	10
Anlagenkartei	10
Anlagenunterhaltungskosten	10
Anlagenverzeichnis	10
Anlagevermögensbücher und -karteien	10
Anleihebücher	10
Anleihen	6
Anträge auf Arbeitnehmersparzulage	6
Anwesenheitslisten (wenn für die Lohnbuchhaltung erforderlich)	6
Anzahlungsunterlagen	6
Arbeitgeberzuschussskarten	6
Arbeitnehmersparzulage (Verträge)	6
Arbeitsanweisungen für die EDV-Buchführung	10
Aufbewahrungsvorschriften f. betr. EDV-Dokumentation	10
Auftragsbestätigungen	6
Auftragsbestätigungen (erhaltene und Kopien versandter)	6
Auftragsbücher	6
Auftragskostenbelege	10
Auftragszettel	10
Aufzeichnungen	10
Ausfuhrunterlagen	6
Ausgangsrechnungen	10
Ausschusslisten als Buchungsbelege	10
Außendienstabrechnungen	10
Außendienstabrechnungen (soweit keine Buchungsbelege)	6
Außenhandelsunterlagen	6
Auszahlungsbelege	10

B

Bahnabrechnungen	10
Bahnfrachtbriefe	6
Bankbelege	10
Bankbürgschaften	6
Bareinkaufs- und -verkaufsrechnungen	10
Bauakten	6
Bauantragskostennachweise	6
Baubeschreibungen	6
Baubücher	10
Baugenehmigungen	6
Bedienerhandbücher Rechnerbetrieb	10
Beförderungspapiere	6
Beherrschungsverträge	10
Beitragsabrechnungen der Sozialversicherungsträger	10
Belegformate	10
Belege, soweit Buchungsfunktion (Offene-Posten-Buchhaltung)	10
Benutzerhandbücher bei EDV-Buchführung	10
Bestandsberichtigungen	10
Bestandsermittlungen	10
Bestandsverzeichnisse	10
Bestellungen (erhaltene und Kopien versandter)	6
Betriebsabrechnungsbögen mit Belegen als Bewertungsgrundlagen	10
Betriebskostenabrechnung (soweit keine Buchungsbelege)	6
Betriebskostenrechnungen	10
Betriebskrankenkasse (Buchungsbelege)	10
Betriebsprüfungsberichte	6
Betriebsunfallunterlagen	6
Bewertungsunterlagen	10
Bewirtungsunterlagen	10
Bilanzbücher	10
Bilanzen (Jahresbilanzen)	10
Bilanzkonten	10
Bilanzprotokolle für die EDV	10
Bilanzunterlagen	10
Blockdiagramme, soweit Verfahrensdokumentation	10
Bons	10
Börsenaufträge	6
Bruttoerlösnachweise	6
Bruttolohnlisten	6
Bruttolohnsammelkarten	6
Bruttolohnstreifen	6
Buchführungsprogramme	10
Buchführungsunterlagen	10
Buchungsanweisungen	10
Buchungsbelege	10
Buchungsprotokolle für die EDV	10
Buchungsunterlagen	10
Bürgschaftsunterlagen	6

C

Carnetunterlagen	6
Clearingauszüge	6
Clearing-Belege	10
Code-Pläne für Verständnis der Buchführung	10
Computerausdrucke mit Buchungsdaten	10
COM-Verfahrensbeschreibungen	10

D

Darlehenskonto	10
Darlehensunterlagen (nach Ablauf des Vertrages)	6
Datensicherungen	10
Dauerauftragsunterlagen	6
Dauerauftragsunterlagen (nach Vertragsablauf)	10
Dauervorschüsse	10
Dateien, Beschreibungen der	10
Dateiverzeichnisse	10
Datensätze, Beschreibung und Aufbau	10
Datensicherungsregeln	10
Debitorenkonen	10
Debitorenlisten (soweit Bilanzunterlagen)	10
Deklarationen (Versandunterlagen)	6
Depotauszüge (soweit nicht Inventare)	10
Depotbestätigungen	10
Depotbücher	10
Deputatunterlagen	6
Devisenunterlagen	6
Dokumentation für Programme und Systeme bei EDV	10
Dubiosenbücher	10

E

Edelmetallbestände	10
Edelmetallumsätze	10
EDV-Journal	10
Effektenbuch	10
Effektenkassenquittungen	10
Eichaufnahmen	6
Einfuhrunterlagen	6
Eingabebeschreibungen bei EDV-Buchführung	10
Eingabedatenformate	10
Eingangsrechnungen	10
Eingangsüberweisungsträger	6
Eingliederungsverträge	10
Einheitswertunterlagen	6
Einkaufsbücher	10
Einnahmenüberschussrechnung	10
Einzahlungsbelege	10
Energieverbrauchsunterlagen	6
Erlösjournale	10
Eröffnungsbilanzen	10
Ersatzkassenunterlagen	6
Essensmarkenabrechnungen (soweit keine Buchungsbelege)	6
Exportunterlagen	6
Expressauslieferungsbücher	10

F

Fahrtenbücher	10
Fahrtkostenerstattungen	10
Fahrtkostenerstattungsunterlagen Arbeitnehmer/ Unternehmer (soweit keine Buchungsbelege)	6
Fakturierjournale	10
Fehlerjournale als Buchungsbelege	10
Fehlermeldungen, Fehlerkorrekturanweisungen bei EDV-Buchführung	10
Fernschreiben (Handelsbriefe)	6
Feuerversicherungsunterlagen	6
Finanzberichte	6
Frachtbriefe	6
Frachtunterlagen	6
Freistemplerabrechnungen	10
Fremdenbücher (Hotel- und Pensionsgewerbe)	10
Fürsorgeunterlagen	6

G

Gebrauchsmusterunterlagen	6
Gehaltsabrechnungen und -bücher (soweit Bilanzunterlage oder Buchungsbeleg)	10
Gehaltskonten	6
Gehaltslisten	10
Gehaltsquittungen	10
Gehaltsvorschusskonten	10
Geschäftsberichte	10
Geschäftsbriefe (außer Rechnungen u. Gutschriften)	6
Geschenknachweise	6
Gesellschaftsverträge	10
Gewährleistungsverpflichtungen	6
Gewerbesteuerunterlagen	6
Gewinn- und Verlustrechnung	10
Gewinnabführungsverträge	10
Gewinnfeststellungen	6
Grundbuchauszüge	10
Grundlohnlisten	10
Grundstücksunterlagen	6
Grundstücksverzeichnis (soweit Inventar)	10
Gutschriftanzeigen	10

H

Haftungsverhältnisunterlagen als Bilanzunterlagen	10
Handelsbilanz	10
Handelsbriefe (außer Rechnungen/Gutschriften)	6
Handelsbücher	10
Handelsregisterauszüge	6
Hauptabschlussübersicht (wenn anstelle der Bilanz)	10
Hauptbücher und -karteien	10
Hauptbuchkonten	10
Hinterlegungsscheine	6
Hypothekenpfandbriefe	6

I

Importrechnungen	10
Importunterlagen	6
Inkassobücher	10
Inventare	10
Inventare als Bilanzunterlagen	10

Inventurunterlagen	10
Investitionsabrechnungen	6
Investitionszulagenunterlagen	6

J

Jahresabschlüsse	10
Jahresabschlusserläuterungen	10
Jahresabschlusslisten	10
Jahreskontoblätter	10
Journale für Hauptbuch und Kontokorrent	10
Jubilarfeierunterlagen	10
Jubiläumsunterlagen	10

K

Kalkulationsunterlagen	6
Kantinenunterlagen	10
Kapitalerhöhungsunterlagen	6
Kapitalverkehrsteuerunterlagen	6
Kassenberichte	10
Kassenbücher u. -blätter	10
Kassenstreifen	6
Kassenzettel (Buchungsunterlage)	10
Kassenzettel (soweit keine Buchungsbelege)	6
Kaufverträge	6
Kilometergeldabrechnungen	10
Kommissionslisten	6
Konnossemente	6
Konsignationsunterlagen	6
Kontenpläne und Kontenplanänderungen	10
Kontenregister	10
Kontoauszüge	10
Kontokorrentbücher	10
Kostenartenpläne	10
Kostenstellenpläne	6
Kostenträgerrechnung	6
Kostenträgerrechnung (Bewertungsunterlage)	10
Kostenvoranschläge	6
Kreditorenkonten	10
Kreditunterlagen (nach Ablauf des Vertrages)	6
Kurssicherungsunterlagen	10
Kurzarbeitergeldanträge	6
Kurzarbeitergeldlisten	6

L

Ladescheine	10
Lageberichte	10
Lagerbuchführungen	10
Lagerprotokolle	6
Leasingunterlagen	6
Leergutabrechnungen	6
Lieferscheine im zusammenhang mit einer Rechnung	10
Lieferscheine als Belegnachweis	6
Liquidation einer GmbH (Bücher und Schriften)	10
Lizenzunterlagen	10
Lohnbelege	10
Lohnkonto (siehe Anmerkungen)	6
Lohnlisten	10
Lohnssteuerunterlagen	10
Lohnunterlagen	6
Lohnvorschusskonten	10
Luftfrachtbriefe	6

M

Magnetbänder mit Buchfunktion	10
Mahnbescheide	6
Mahnungen	6
Maklerschlussnoten	6
Maske (Bildschirm-, Druck-)	10
Materialabrechnungen	10
Materialbeanstandungen	6
Materialentnahmescheine	6
Menueübersicht	10
Mietunterlagen (nach Ablauf des Vertrages)	6
Mikrofilme zur Datensicherung der Buchführung	10
Mikrofilme zur Datensicherung von Geschäftsbriefen	6
Mikrofilmverfahrensbeschreibungen	10
Montageversicherungsakten	10
Mutterschaftsgeldunterlagen	10

N

Nachkalkulationen	10
Nachnahmebelege	10
Nachnahmebelege (soweit keine Buchungsbelege)	6
Nebenbücher	10
Nettolohnlisten	10
Nutzflächenermittlung	10

O

Obligationen	6
Offene-Posten-Listen	10
Orderpapiere	6
Organisationsunterlagen der EDV-Buchführung	10
Organschaftsabrechnungen	10
Organschaftsverträge	10

P

Pachtunterlagen (nach Ablauf des Vertrages)	6
Patentunterlagen	6
Pensionsrückstellungsunterlagen	10
Pensionszahlungen	10
Pfandleihbücher	10
Pfändungsunterlagen	10
Portokassenbücher	10
Postaufträge	6
Postbankauszüge	10
Postbankbelege	10
Postscheckbelege	10
Preislisten	6
Preisvereinbarungen	6
Privatentnahmebelege	10
Programmablaufbeschreibungen für EDV	10
Programmverzeichnisse	10
Proteste (Scheck, Wechsel)	6
Protokolle (Buchungsbelege)	10
Protokolle (soweit keine Buchungsbelege)	6
Protokolle von DÜVO-Meldungen	3
Provisionsabrechnungen	10
Prozessakten	10
Prüfungsberichte (des Abschlussprüfers)	10

Q

Qualitätsberichte	6
Quittungen	10

R

Rechnungen	10
Rechnungsabgrenzungsermittlung	10
Registrierkassenstreifen (soweit keine Buchungsbelege)	6
Reisekostenabrechnungen für Arbeitnehmer/ für Unternehmer	10
Rentenversicherungsnachweise	6
Repräsentationsaufwendungen	10
Repräsentationskosten	10
Rückstellungsunterlagen	10
Rückwareneingangsjournale	6

S

Sachanlagevermögenskarteien	10
Sachkonten	10
Saldenbestätigungen	10
Saldenbilanzen	10
Schadensmeldungen und -unterlagen	6
Scheck- und Wechselunterlagen	6
Scheckbestandsaufnahmen	10
Schecks	10
Schreiben im Rahmen eines Unternehmens (soweit Handelsgeschäfte)	6
Schriftwechsel	6
Schuldtitel	10
Sicherungsübereignungen	6
Skontounterlagen	10
Sondergutschriften	10
Sozialpläne	6
Sozialversicherungsbeitragskonten	6
Sparprämienanträge	6
Speicherbelegungsplan der EDV-Buchführung	10
Spendenbescheinigungen	10
Steuerbescheide und -erklärungen	10
Steuerrückstellungsberechnungen	10
Steuerunterlagen	6
Stornobelege	10
Stundenlohnzettel als Buchungsbelege	10
Systemhandbücher	10

T

Teilzahlungsbelege	6
Telefonkostennachweise	10
Telefonkostennachweise (soweit keine Buchungsbelege)	6
Testate als Bilanzteil	10
Transportschadenunterlagen	6
Transportversicherungsanmeldungen	6
Trennungsgeldermittlungen	10

Ü

Überstundenlisten	6
Überweisungsbelege	10
Umbuchungsbelege	10
Umsatzsteuervergütungen	10
Umsatzsteuervoranmeldungen	10
Umwandlungsbilanzen	10
Umwandlungsunterlagen	6
Unfallversicherungsunterlagen	6
Unternehmerlohnverrechnungen	6
Urlaubslisten für Rückstellungen	10

V

Valuta-Belege	10
Verbindlichkeiten	10
Verbindlichkeiten (Zusammenstellung)	10
Verfrachtungsaufträge	6
Verkaufsbücher, -journale	10
Vermögensteuerunterlagen	6
Vermögensverzeichnis	10
Vermögenswirksame Leistungen (wenn Unterlagen = Handels- oder Geschäftsbrief)	6
Vermögenswirksame Leistungen (wenn Unterlagen = Buchungsbeleg)	10
Verpfändungsunterlagen	10
Verrechnungskonten	10
Verrechnungspreisunterlagen	10
Versand- und Frachtunterlagen	6
Verschiffungsunterlagen als Buchungsbelege	10
Versicherungspolicen	6
Versteigerungsunterlagen	6
Verträge	6
Vertreterunterlagen	6
Verwahrungsbücher für Wertpapiere	10
Viehregister	10
Vollmachten (Urkunden)	6
Vollständigkeitserklärungen	10
Vorauszahlungsbelege	10
Vorschusskonten	10
Vorschusslisten als Buchungsbelege	10

W

Währungsforderungen	10
Warenabgabescheine	6
Warenbestandsaufnahmen	10
Wareneingangs- und -ausgangsbücher	10
Wareneingangs-/ausgangsbücher	10
Warenverkehrsbescheinigungen	6
Wechsel	6
Wechsel als Buchungsbeleg	10
Wechselbuch	10
Wechselobligation	10
Weihnachtsgratifikation	10
Werbegeschenknachweise	10
Werbekosten, Belege über	10
Werksrentenanträge	6
Werkstattabrechnungen	10
Werkzeugkosten, Belege über	10
Werkzeugregister als Inventar	10
Wertberichtigungen	10
Wertpapieraufstellungen als Bilanzunterlagen	10
Wertpapierkurse als Buchungsbelege	10
Wildhandelsbücher	10
Wohnungsbauunterlagen	6

Z

Zahlungsanweisungen/-belege	10
Zahlungsträger	10
Zeichnungsvollmachten	6
Zessionen	6
Zinsabrechnungen	10
Zinsberechnungen als Buchungsbeleg	10
Zinsberechnungsunterlagen	6
Zinsstaffeln	6
Zollbelege	6
Zollbelege über Einfuhrumsatzsteuer	10
Zugangsbelege	10
Zugriffsregelungen bei EDV-Buchführung	10
Zuschüsse des Arbeitgebers	10
Zustellungsquittungen	6
Zwischenbilanz bei Gesellschafterwechsel oder Umstellung des Wirtschaftsjahres	10

Quelle: IHK Frankfurt am Main, Stand September 2016

Haftungsausschluss

Dieses Whitepaper dient lediglich der Information und stellt keine Rechtsberatung dar. Die Inhalte dieses Dokuments wurden mit größtmöglicher Sorgfalt erstellt. Irrtümer und Änderungen sind vorbehalten. Der Anbieter übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Inhalte. Die Nutzung der Inhalte erfolgt auf eigene Gefahr des Nutzers. Mit der reinen Nutzung des Dokuments kommt keinerlei Vertragsverhältnis zwischen dem Nutzer und dem Anbieter zustande. Die in diesem Dokument veröffentlichten Inhalte unterliegen dem deutschen Urheber- und Leistungsschutzrecht. Jede vom deutschen Urheber- und Leistungsschutzrecht nicht zugelassene Verwertung bedarf der vorherigen schriftlichen Zustimmung des Anbieters oder jeweiligen Rechteinhabers.

Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Übersetzung, Einspeicherung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien und Systemen. Inhalte und Rechte Dritter sind dabei als solche gekennzeichnet. Die unerlaubte Vervielfältigung oder Weitergabe einzelner oder kompletter Inhalte ist nicht gestattet und strafbar. Lediglich die Herstellung von Kopien und Downloads für den persönlichen Gebrauch ist erlaubt.

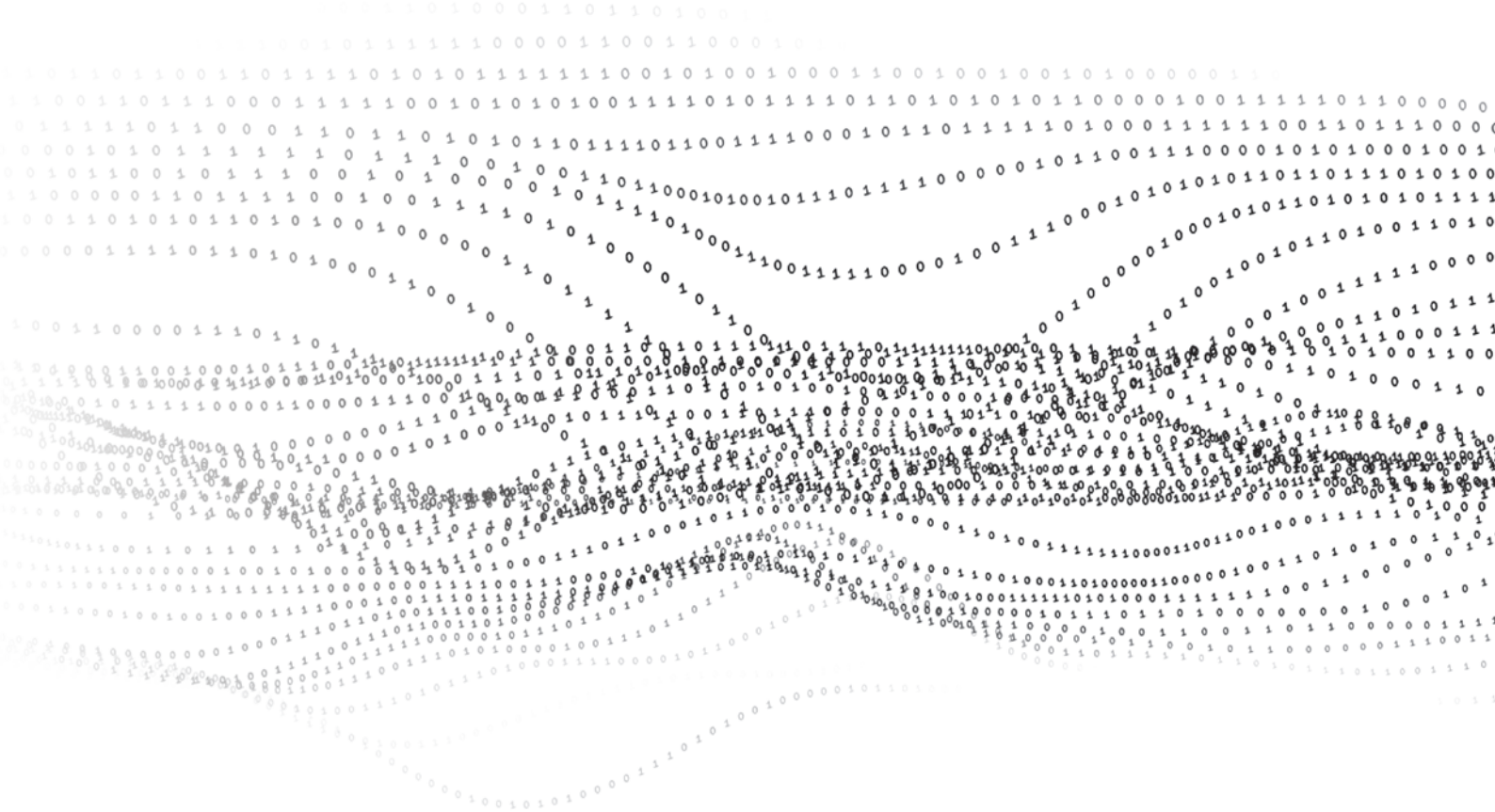
Rechtliche Hinweise

Autor

Dr. Andreas Schmidt, Chief Information Officer (CIO), ARTEC IT Solutions AG

Haftungshinweis

Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung oder Garantie für Vollständigkeit, Richtigkeit und Aktualität aller zur Verfügung gestellten Texte und Daten.



AMERICA

ARTEC IT Solutions USA
1600 Parkwood Circle
Atlanta, Georgia 30339, USA
Telefon: +1 - 855 - 462 - 7832
Telefax: +1 - 678 - 666 - 5153
E-Mail: info@artec-it.com
Internet: http://www.artec-it.com

EMEA

ARTEC IT Solutions AG
Robert-Bosch-Str. 38
61184 Karben, Germany
Telefon: +49 - 6039 - 9154 - 0
Telefax: +49 - 6039 - 9154 - 54
E-Mail: info@artec-it.de
Internet: http://www.artec-it.de

ASIA PACIFIC

ARTEC IT Solutions AP
#1003 U-Top Tech Valley, 7, Beobwon-ro 6-gil,
Songpa-gu, Seoul 05855, Korea
Telefon: +82 - 2 - 515 - 3349
Telefax: +82 - 2 - 6008 - 3403
E-Mail: info-ap@artec-it.com
Internet: http://www.artec-it.com

ARTEC® IT Solutions

Turning Data Into Information