

FACTSHEET //

Eine Frage der Compliance -

**Die rechtssichere Archivierung von E-Mails
und Dokumenten**



INHALTSVERZEICHNIS

- 3 Über ARTEC IT Solutions AG
- 4 Einleitung
- 5 Unterschiedliche Aufbewahrungsfristen und die Konsequenzen für die Praxis
- 6 Original ist nicht gleich Original: Zivil- und steuerrechtliche Unterschiede
- 7 Wer hat Zugriff auf welchen Content: Compliance-konforme Archivierung und der Datenschutz
- 8 Die Wahl des Speichersystems: Es muss nicht immer WORM sein
- 9 Dokumentierte Sicherheit: Verschlüsselung und digitale Signaturen
- 10 Fazit
- 11 Impressum



ÜBER ARTEC IT SOLUTIONS AG



Die ARTEC IT Solutions AG ist einer der führenden Hersteller von Lösungen für die elektronische Archivierung von Geschäftsvorgängen. Im Mittelpunkt steht dabei die langfristige, rechtssichere Aufbewahrung von relevanten Informationen wie etwa E-Mails, gedruckten Dokumenten, Dateien oder Sprach- und Telefondaten im Unternehmen. Die Lösungen von ARTEC orientieren sich an den unterschiedlichen gesetzlichen Grundlagen und Anforderungen (beispielsweise GDPdU, Abgabenordnung, Handelsgesetzbuch oder Bundesdatenschutzgesetz) und setzen diese durch innovative Entwicklungen und Features um. Besondere Berücksichtigung finden dabei die Aspekte maximale Sicherheit, einfache Implementierung und hohe Wirtschaftlichkeit.

Wichtigstes und bekanntestes Produkt des Herstellers ist die Dokumenten- und E-Mail-Archivierungs-Appliance EMA[®], die sich innerhalb kürzester Zeit in ein Firmennetzwerk einbinden lässt. Die Appliance ermöglicht auf besonders komfortable Weise die rechtskonforme Archivierung der geschäftlichen E-Mail-Korrespondenz per Plug & Play und bietet leistungsstarke Recherche- und Wiederherstellungsfunktionen. Unternehmen behalten so jederzeit die volle Kontrolle über ihre Daten, ohne auf die verwendeten Applikationen Rücksicht nehmen zu müssen. Durch zusätzliche Module kann EMA[®] jederzeit und ohne Unterbrechung zur umfassenden, ganzheitlichen Archivlösung für den gesamten geschäftlich relevanten Content ausgebaut werden (Enterprise Managed Archive).

ARTEC wurde 1995 durch Jerry J. Artisdhad gegründet. Der Hauptsitz befindet sich in Karben bei Frankfurt am Main. Das Unternehmen arbeitet weltweit mit Technologie- und Vertriebspartnern zusammen.

Weitere Informationen unter:

<http://www.artec-it.de>



EINLEITUNG

Bei der Archivierung von unternehmensrelevanten Informationen spielen Compliance-Anforderungen oft die wichtigste Rolle. Gesetze, Richtlinien und Verordnungen bilden ein umfangreiches Regelwerk für die rechtskonforme Aufbewahrung von Inhalten wie etwa E-Mails oder Dokumenten. Dazu kommen interne betriebliche Richtlinien, die beispielsweise die Privatsphäre der Mitarbeiter betreffen.

Schutz und Sicherheit der Daten sowie die Verfügbarkeit stellen die Grundlagen dar. Als entscheidender Punkt wird häufig die Manipulationssicherheit und Unveränderbarkeit (Revisionssicherheit) der archivierten Daten angeführt. Fakt ist allerdings: Der Passus „Revisionssicherheit“, mit dem viele Hersteller von Archivierungslösungen auch sehr offensiv werben, taucht in der entsprechenden Gesetzgebung im Wortlaut so gar nicht auf. Die Notwendigkeit, die Echtheit archivierter Informationen belegen zu können, ergibt sich vielmehr aus der Gesamtheit der rechtlichen Bestimmungen.

Ebenso wenig sind bestimmte technische Verfahren bei der Archivierung auf exakte Art und Weise vorgeschrieben, so dass grundsätzlich viel Auslegungsspielraum bleibt.

Die große Herausforderung für Unternehmen ist daher, im dichten Dschungel der relevanten Anforderungen nicht die Orientierung zu verlieren:

- Abgabenordnung (AO)
- Handelsgesetzbuch (HGB)
- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- Basel II-Kriterien
- Sarbanes-Oxley Act
- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)
- Interne Regelungen und betriebliche Besonderheiten

Eine nach heutigem Maßstab rechtssichere Archivierung entsteht letztlich aus der Berücksichtigung und Kombination der unterschiedlichen gesetzlichen Richtlinien sowie der technisch sinnvollsten Vorgehensweisen.



UNTERSCHIEDLICHE AUFBEWAHRUNGSFRISTEN UND DIE KONSEQUENZEN FÜR DIE PRAXIS

Die Zeitspanne, für die beispielsweise E-Mails im Archiv aufbewahrt und verfügbar gehalten werden müssen, variiert je nach Inhalt und Bedeutung der jeweiligen Dokumente.

Häufig wird vor allem die steuerrechtliche Betrachtungsweise herangezogen. Danach müssen Mails, die besondere steuerliche bzw. buchhalterische Relevanz haben (wie beispielsweise Rechnungen), zehn Jahre lang aufbewahrt werden. Da die offizielle Aufbewahrungsfrist erst mit dem Ende des jeweiligen Geschäftsjahres beginnt, können sich in der Praxis Zeiträume von bis zu annähernd elf Jahren ergeben. Für viele andere kaufmännische Dokumente, zum Beispiel empfangene und versendete Handelsbriefe, gilt eine allgemeine Aufbewahrungsfrist von sechs Jahren.

Neben den Vorgaben des Gesetzgebers spielen bei der Aufbewahrungsdauer allerdings auch interne Besonderheiten des jeweiligen Unternehmens beziehungsweise der Branche eine Rolle. So müssen wichtige Dokumente in manchen, stark regulierten Bereichen (etwa im Gesundheitswesen) bis zu 30 Jahre oder gar noch länger vorgehalten werden, um bei Bedarf entsprechende Nachweise führen zu können.

Die Beispiele verdeutlichen bereits, dass eine globale Archivregelung in Bezug auf die Aufbewahrungsfristen in aller Regel nicht praktikabel ist. Eine sinnvolle Lösung für diese Problematik können fachbereichsbezogene Archive darstellen, die individuelle festlegbare Archivzeiträume ermöglichen.

Eine Löschung der Daten erfolgt dann frühestens nach Ablauf der jeweiligen Frist. Mit der Archivierungsappliance EMA® von ARTEC etwa können E-Mails oder andere Dokumente durch die Vergabe von Attributen entsprechend eingeordnet werden. Auf diese Weise können individuell angepasste Facharchive mit frei wählbaren Vorhalte- und Löschungskriterien angelegt werden.



ORIGINAL IST NICHT GLEICH ORIGINAL: ZIVIL- UND STEUERRECHTLICHE UNTERSCHIEDE

Nicht nur die vorgeschriebenen Aufbewahrungszeiten für geschäftliche Dokumente und E-Mails sind unterschiedlich. In einigen Punkten gibt es auch wichtige Unterschiede zwischen der zivil- und steuerrechtlichen Betrachtung, die im Rahmen der Compliance-Anforderungen berücksichtigt werden müssen.

So reicht es auf der Grundlage des Steuerrechts beispielsweise aus, wenn eine Kopie des originalen Dokuments beziehungsweise der ursprünglichen E-Mail aufbewahrt wird, die rein optisch mit dem Original identisch ist. Eine Ausnahme davon bilden lediglich Dokumente mit qualifizierter Signatur.

Deutlich höher liegen die Anforderungen jedoch aus zivilrechtlicher Sicht. Denn hier kommt der Faktor „Beweiskraft“ ins Spiel. Sollen etwa Sachverhalte im Rahmen eines Rechtsstreits durch E-Mails belegt werden (zum Beispiel vertragliche Absprachen), dann wird das unveränderte Original benötigt.

Konträr dazu steht die gängige Praxis vieler Archivierungslösungen, E-Mails nicht im Ganzen, sondern zerlegt in die einzelnen Bestandteile Header, Body und Attachment zu speichern. Problematisch ist auch die Konvertierung in Fremdformate, gängigerweise beispielsweise PDF oder TIFF. Eine Vorgehensweise, von der abgeraten werden muss, da später massive Schwierigkeiten bei der Beweisführung auftreten können beziehungsweise Dokumente rechtlich unter Umständen nicht anerkannt werden.

Im Vorteil sind hier ganz klar Lösungen, die E-Mails im vollständigen Originalzustand und -format archivieren, inklusive eventuell vorhandener Dateianhänge und ohne Aufteilung. Denn dies ist die wichtigste Voraussetzung dafür, später zweifelsfrei den unveränderten Originalzustand einer Mail nachweisen zu können.



WER HAT ZUGRIFF AUF WELCHEN CONTENT: COMPLIANCE-KONFORME ARCHIVIERUNG UND DER DATENSCHUTZ

Der Datenschutz im Unternehmen hinsichtlich des Archivs wird gerne vernachlässigt, ist aber von großer Bedeutung. Dabei geht es nicht ausschließlich um gesetzliche Anforderungen, sondern oftmals auch um die Umsetzung interner, betrieblicher Vereinbarungen.

Zu lösen ist beispielsweise die Thematik, was mit privaten E-Mails der Mitarbeiter geschieht, sofern diese über Unternehmenssysteme verschickt werden.

Im Fokus steht außerdem die Zugriffssicherheit. Es muss einerseits gewährleistet sein, dass nur berechtigte Nutzer auf die Archivdaten zugreifen können. Gleichzeitig muss sichergestellt werden, dass auch diese Anwender nicht unbemerkt Veränderungen vornehmen oder zum Beispiel einzelne E-Mails oder Dokumente einfach aus dem Archiv löschen können.

Ein Spagat, der in vielen Archivierungssystemen, gerade bei rein softwarebasierten Lösungen, nur unzureichend berücksichtigt wird. Denn häufig haben Systemadministratoren und IT-Verantwortliche sehr weit reichende Nutzerrechte und sind nur schwer kontrollierbar. Neben der Möglichkeit von Änderungen an den Archivdaten wirft dies auch die Problematik des individuellen Datenschutzes bei der Einsichtnahme einzelner, sensibler Inhalte auf.

Eine Lösung für diese Herausforderung bietet die Archivierungsalpliance EMA® mit dem innovativen Vier-Augen-Prinzip. Damit kann beispielsweise festgelegt werden, dass der Zugriff auf gespeicherte E-Mails grundsätzlich nur gemeinsam mit einer zusätzlichen Person, wie etwa einem Mitglied des Betriebsrats, erfolgen kann. Dieser zusätzliche Sicherungsmechanismus beugt Missbrauch wirksam vor und eignet sich dadurch in besonderem Maße auch zur Umsetzung betriebsinterner Datenschutzrichtlinien.



DIE WAHL DES SPEICHERSYSTEMS: ES MUSS NICHT IMMER WORM SEIN

Häufig wird fälschlicherweise die Meinung vertreten, die Compliance-Richtlinien bei der Mail-Archivierung wären nur durch den Einsatz von WORM-Speichern umsetzbar - also mit Hilfe von Speichermedien, die lediglich ein einziges Mal beschrieben werden können. Auf diese Weise sollen die Archivdaten bereits durch die grundsätzlichen technischen Eigenschaften des Speichersystems vor nachträglichen Manipulationen geschützt werden – vom Ansatzpunkt her soweit grundsätzlich durchaus nachvollziehbar.

Übersehen wird dabei allerdings, dass es andererseits eben gerade wieder Vorgaben aus dem Datenschutz-Bereich sind, die es fallweise erforderlich machen, bestimmte E-Mails oder Dokumente aus dem Archiv löschen zu können (Beispiel: private E-Mails). Da genau dies mit einem WORM-System technisch nicht möglich ist, sollten Unternehmen bei der Einführung einer Archivierungslösung davon Abstand nehmen.

Wie im folgenden Absatz ausgeführt, lassen sich archivierte Daten durch die Kombination aus Verschlüsselung und digitalen Signaturen höchstwirksam vor späteren Veränderungen schützen.



DOKUMENTIERTE SICHERHEIT: VERSCHLÜSSLUNG UND DIGITALE SIGNATUREN

Bei den Daten in einem Unternehmensarchiv handelt es sich um hochsensible Informationen, die durch technische Vorkehrungen entsprechend geschützt werden müssen. Dies betrifft sowohl die Sicherung des Archivs gegenüber unbefugtem Zugriff von außen als auch den Schutz vor absichtlichen oder versehentlichen Manipulationen durch die Mitarbeiter selbst.

Es empfiehlt sich, hier auf ein vielfach bewährtes und weit verbreitetes Standard-Verfahren wie AES (Advanced Encryption Standard) zu setzen, um die langfristige Zukunftssicherheit zu gewährleisten. Schließlich sind die Aufbewahrungszeiträume, wie eingangs bereits beschrieben, teilweise extrem lang und können kurzlebige Technik-Trends deutlich überdauern.

Die Archivierungsappliance EMA® etwa verschlüsselt alle E-Mails oder Dokumente bei der Übergabe an das Archiv nach dem AES-Verfahren. Auch der Archivzugriff selbst erfolgt SSL-verschlüsselt. Gleichzeitig werden die Daten digital signiert und mit fälschungssicheren elektronischen Zeit- und Datumsstempeln versehen.

Diese Vorgehensweise macht jede einzelne E-Mail beziehungsweise jedes Dokument eindeutig identifizierbar. Auch Jahre später kann über die digitale Signatur eindeutig der Ursprung der Daten nachvollzogen werden. So lässt sich beispielsweise der Weg einer einzelnen E-Mail (wann und von wem an wen verschickt?) exakt verfolgen und deren unveränderte Echtheit belegen.



FAZIT

Die Compliance-Regelungen sind in vielen Fällen der Hauptgrund für die Einführung eines elektronischen Archivsystems für E-Mails und Dokumente im Unternehmen.

Geschäftsführer, CIOs, IT-Entscheider und Netzwerkadministratoren müssen sich dabei bewusst machen, dass es nicht die eine relevante Verordnung gibt, die alles beinhaltet, sondern dass sich eine rechtssichere Archivierung aus verschiedensten Komponenten zusammensetzt.

Nur durch die ganzheitliche Berücksichtigung der unterschiedlichen Anforderungen wird eine Aufbewahrung ermöglicht, die sowohl den gesetzlichen Anforderungen entspricht als auch wirtschaftliche und organisatorische Vorteile für das Unternehmen mit sich bringt.

Die Lösung EMA[®] von ARTEC IT Solutions ist als geschlossenes Appliance-System optimal darauf ausgerichtet, per Plug & Play eine rechtskonforme Archivierung bereitzustellen. Dafür sorgen die automatische Verschlüsselung und digitale Signierung aller E-Mails und Dokumente direkt bei der Archivierung. Denn sie bilden letztlich die wichtigste Voraussetzung dafür, um später jederzeit den unveränderten Originalzustand der Daten belegen zu können.

Durch spezielle Features wie das Vier-Augen-Prinzip und die Verwaltung individueller Rechte für Benutzer und Administratoren lassen sich mit EMA[®] zudem auch betriebsinterne Vorgaben umsetzen, die beispielsweise den Schutz persönlicher Daten der Mitarbeiter betreffen.



IMPRESSUM

ARTEC IT Solutions AG
Robert-Bosch-Str. 38
61184 Karben

Ansprechpartner:

Friedhelm Peplowski

Director Global Sales & Marketing

E-Mail: f.peplowski@artec-it.de

Telefax: +49 (0) 6039 - 9154 - 7425

Telefax: +49 (0) 6039 - 9154 - 6425

Mobil: +49 (0) 0172 - 1858161

Disclaimer

Die Inhalte dieses Dokuments werden mit größtmöglicher Sorgfalt erstellt. Der Anbieter übernimmt jedoch 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.