



E-Mail Archivierung – Leitfaden für Geschäftsleitung, EDV-Leitung und Administration

Die gesetzliche Lage im Hinblick auf das Thema E-Mail-Archivierung ist mittlerweile klar geregelt. Die Bedeutung und welche Aufgaben und Folgen dies mit sich bringt, ist aber vielen Verantwortlichen noch unbekannt.

Seit 1. Januar 2007 sind neue Anforderungen an die E-Mails mit Bezug zum Geschäftsverkehr eines Unternehmens geregelt worden. Sie sind mit den gleichen Angaben zu kennzeichnen wie der typische Geschäftsbrief (Angaben gemäß HGB § 37a, GmbH § 35a sowie AktG § 80 – genau wie auf dem Briefkopf). Somit erhalten geschäftliche E-Mails, die über eine Firmenadresse gesendet werden, eine finanztechnische Relevanz. Wenn ein Unternehmen über eine registrierte Domain eine E-Mail versendet, ist dies vergleichbar mit der Versendung eines Handelsbriefes und verpflichtet auf Grund des Rechtsscheins die juristische Person des Unternehmens.

Es gibt nicht nur direkte, gesetzliche Pflichten was die Archivierung von E-Mails betrifft, sondern auch indirekte Verpflichtungen: So kann eine unsichere, unternehmensinterne IT-Infrastruktur, die durch private E-Mail-Nutzung verursacht werden kann, ein nachteiliges Rating gemäß Basel II nach sich ziehen.

Zur E-Mail-Archivierung zählen nicht nur ausgehende und empfangene E-Mails, sondern auch alle internen E-Mails inkl. der Anhänge, die geschäftsrelevant sind. Es gibt jedoch gute Gründe den Blickwinkel über die gesetzlichen Anforderungen hinaus zu erweitern. Neben den indirekten Verbesserungen wie dem Rating, gibt es IT-technische Anforderungen. So ist im täglichen Umgang in vielen Fällen die Postbox in der Größe limitiert. Die Folgen: ausbleibende E-Mails, da Anhänge zu groß sind – letztlich viel organisatorischer Aufwand – für ein Arbeitsmedium, das heute Standard ist und nicht in der Größe eingeschränkt sein sollte. Ein wesentlicher Aspekt ist die in einem zentralen System zur Verfügung stehende Suchfunktion, die in lokalen Dateien nicht vorhanden ist.

Alle Welt spricht von revisionssicherer Archivierung

Den Begriff »Revisionssicherheit« gibt es offiziell weder in der IT noch in den gesetzlichen Anforderungen. Das Synonym »revisionssichere Archivierung« ist den elektronischen Archivsystemen zugeordnet, die den Anforderungen der GoBS genügen, ordnungsgemäß betrieben werden und Dokumente unveränderbar und verfälschungssicher archivieren. Im Falle der E-Mail-Archivierung bedeutet dies, dass hier die gleichen Faktoren gelten:

- Speicherung im originär digitalen Format (unverändert)
- fälschungssicher
- Rückverfolgbarkeit der E-Mail-Kommunikation
- indexiert
- farbliche Merkmale, die eine Beweisfunktion haben, müssen erhalten bleiben
- Änderungen müssen protokolliert und ausgewiesen (z.B. Kopie, Version) werden

Für eine ordnungsgemäße Aufbewahrung von E-Mails reicht es nicht aus, wenn diese nur im Personal Information Manager (z.B. Outlook) gesondert abgelegt werden. Hier sind sie nicht ausreichend vor Manipulationen geschützt.



Gesetzliche Verpflichtung zur E-Mail Archivierung

Durch HGB und AO:

Vertrags- und Einkaufsdokumente unterliegen den handels- und steuerrechtlichen Buchführungsbedingungen und somit den gesetzlichen Vorgaben für die Archivierung. Geschäftsrelevante E-Mails haben handelsrechtlich eine Aufbewahrungsfrist von bis zu zehn Jahren, beginnend mit dem Schluss des Kalenderjahres in dem die E-Mail empfangen wurde.

Ergänzende Anforderungen folgen aus der GOB, GoBS und der GDPdU.

Wer ist verantwortlich – Wer wird belangt?

Dies ist abhängig von der Organisationsform der Unternehmen. An erster Stelle steht hier die Geschäftsleitung in der Verpflichtung. Je nach Delegationsmodell stehen aber auch der IT-Leiter und der Administrator, in Bezug auf die Archivierung von E-Mails, in der Verantwortung und sind damit haftbar – im schlimmsten Fall auch persönlich und mit ihrem Privatvermögen.

Welche Maßnahmen schützen mich?

Der einfachste Weg ist das Verbot der privaten E-Mail-Nutzung. Dies kann durch eine Betriebsvereinbarung geregelt werden. Die Durchsetzung und die Einhaltung sollten aber stichprobenartig kontrolliert werden, damit das Unternehmen nicht wieder Gefahr läuft, als Telekommunikations-Dienstleister zu gelten. Sobald ein Unternehmen die Privatnutzung während der Arbeitszeit duldet, wird es zum Anbieter von Telekommunikations-Diensten nach dem Telekommunikationsgesetz (TKG). Das Unternehmen kann nicht ohne weiteres auf private Nutzungs-, Abrechnungs- und Inhaltsdaten der Arbeitnehmer zugreifen. Daher sollten privates Mailen und Surfen über den Firmen-Account per Firmenvereinbarung untersagt und nur über einen freien Account genehmigt werden.

Userbezogene E-Mail-Ablage

Bei dieser Art der E-Mail-Archivierung wird vom Anwender selbst entschieden, welche E-Mails im DMS einem Vorgang zugeordnet und archiviert werden. Der Gesetzgeber will aber, dass alle E-Mails, die steuerlich relevant oder den Charakter eines Handelsbriefes haben, ohne Möglichkeit der Manipulation, archiviert werden. Dies ist auf diesem Wege also nicht gewährleistet. Auch die Vollständigkeit ist hier fraglich. Wer entscheidet, was steuerlich relevant ist? Wer entscheidet, welche E-Mail ein Handelsbrief ist? Diese Verantwortung sollte man nicht dem Anwender überlassen, zumal eine Ablage aller E-Mails nicht gewährleistet, sowie auch ein versehentliches Löschen nicht ausgeschlossen werden kann.

Serverbezogene E-Mail-Ablage

Am häufigsten findet man auf dem Markt Lösungen, welche die E-Mails lediglich 1:1 in ein Archiv verschieben oder auf E-Mail-Boxen auslagern. Zweifelsfrei werden dadurch Kommunikationslösungen



wie Exchange entlastet, dies hat aber oftmals noch rein gar nichts mit der Erfüllung der gesetzlichen Vorgaben zu tun.

Lösungen, die den gesetzlichen Anforderungen genügen, stellen serverbezogene E-Mail-Ablagen zur Verfügung, die gleichzeitig mehrere Vorgaben erfüllen.

1. Eine Übernahme aller E-Mails in ein Archiv, auf das nur der Administrator Zugang hat, so wie es auch im Exchange Server üblich ist. Private E-Mails (wenn dies weiterhin zugelassen wird) dürfen nicht einsehbar sein, um das Postgeheimnis nicht zu verletzen.
2. E-Mails werden zeitgleich mit dem Eintreffen im E-Mail-Server/Postfach automatisch archiviert. Der Anwender hat somit erst gar nicht die Möglichkeit der Manipulation oder einer Veränderung.
3. Das Postgeheimnis wird über die Benutzer- und Rechteverwaltung gewahrt.
4. Hinterlegte Regeln erlauben es, die E-Mails direkt nach dem Eintreffen zu klassifizieren und zum jeweiligen Geschäftsvorgang zuzuordnen.

Bei der Zuordnung zum Geschäftsvorfall handelt es sich um eine gesetzliche Anforderung, welche aber derzeit von den wenigsten Lösungen unterstützt wird. Intelligente Produkte erlauben es, Inhalte aus den E-Mail-Feldern (An, Betreff, ...) und dem Textbody herauszufiltern und zu interpretieren.

So kann die E-Mail aus den gewonnenen Informationen, wie E-Mail-Adresse des Absenders (mail-von@musterfirma.de), dem Inhalt des Betreffs (Rechnung) und einem Textinhalt (fehlerhafte Rechnung), automatisiert dem Kunden zugeordnet werden. Ohne Eingriff eines Anwenders liegt die E-Mail vorgangsbezogen im Archiv, den richtigen Geschäftsvorfall betreffend, zugeordnet. Anwender können E-Mails nicht mehr physisch löschen, sondern lediglich die in ihrem E-Mail-Programm verbliebenen Links (Referenzen).

Diese Lösungen bieten darüber hinaus noch einen weiteren Nutzen. Durch die Extraktion der E-Mail-Daten ist auch eine automatisierte Zuordnung der E-Mail bei der Verwendung von Gruppen-Accounts, wie support@musterfirma.de, möglich. Wird innerhalb der E-Mail Bezug auf bestimmte Produkte, Dienstleistungen, etc. genommen, können diese an die richtigen Betreuer weitergeleitet werden.

Ferner bilden solche Lösungen eine Brücke zwischen den gesetzlichen Erfordernissen, die private E-Mail-Archivierung im Unternehmen zu verbieten (gerade aus Sicht der Compliance mit SOX, KonTraG und Basel II), zum anderen private E-Mails so zu archivieren, dass die Veröffentlichung in DMS-Archiven ausgeschlossen ist. Gerade Hersteller die keine vorgangsbezogene Archivlösung bieten, haben hier Schwierigkeiten, diese gesetzlichen Anforderungen zu gewährleisten.

Besonderheiten:

Im Falle von E-Mails bei Betriebsräten kann es sinnvoll sein, diese ebenso wie private E-Mails, von der Archivierung auszuschließen.



Rechtliche Auswirkungen:

- Verlust des Versicherungsschutzes bei der Betriebshaftpflicht durch fehlende oder fehlerhafte E-Mail-Archivierung. Kann zum teilweisen oder totalen Ausfall führen.
- Keine Anerkennung einer ordnungsgemäßen Buchführung
- Persönliche Haftung.
- Verlust von Beweismaterial vor Gericht.
- Schadensersatz.
- Straftatbestand im Falle von vorsätzlichen Falschablagen oder Verschleierungen von Vermögensverhältnissen

Persönliche Haftung

Verlust von Beweisen, was qualifiziert signierte Dokumente (signierte E-Mails) betrifft, da diese wie Privaturkunden betrachtet werden.

Die zukünftige Lesbarkeit der E-Mails (bis 10 Jahre Aufbewahrungsfrist) wird dadurch gewährleistet, dass diese nicht in den proprietären Herstellerformaten (.MSG etc.) gespeichert, sondern im herstellerunabhängigen Urformat für E-Mails (EML) archiviert werden.

Auch die Basel II-Anforderungen, z.B. doppelte Ablage von archivierten E-Mails, werden von E-Mail-Archiven teilweise berücksichtigt und durch automatische Backup's gelöst.

Weitergehende Informationen:

Summary E-Mailarchivierung und nn-MailConnect
GDPdU kurz und bündig