



MIMOSA
SYSTEMS

Leitfaden

RA Robert Niedermeier

Heussen

Rechtsanwalts-gesellschaft,

München

25. Mai 2007

E-Mail Archivierung - ein Leitfaden für Geschäftsleitung, IT-Leiter und Administratoren

Mimosa Systems GmbH
Max-Planck-Straße 8
85609 Aschheim-Dornach
Tel: +49 (0) 89 9047 551 -0
www.mimosasystems.de

E-Mail Archivierung - ein Leitfaden für Geschäftsleitung, IT-Leiter und Administratoren

Hinweise zur Nutzung dieses Leitfadens

Dieses Dokument soll der Geschäftsleitung, dem IT-Leiter und dem Administrator bei der Überlegung des Einsatzes eines E-Mail-Archivierungssystems einen Weg aufzeigen, um zu einer rechtssicheren und der Organisationsverpflichtung entsprechenden Planung und Realisierung zu gelangen. Dabei stellt dieses Dokument einen generellen Leitfaden dar, der Hinweise für eine Vielzahl von Fallkonstellationen gibt. Es stellt daher keine verbindliche Rechtsauskunft dar, sondern soll dem Leser einen Überblick über rechtlich relevante Themen der E-Mailarchivierung verschaffen.

A) Rechtliche Hinweise zur E-Mail Archivierung

1. Verantwortliche Personen für E-Mail Archivierung

Der rechtliche Rahmen für jede Tätigkeit eines Unternehmens wird durch das Prinzip der Organisationsverpflichtung (Gewerbeordnung/Handelsgesetzbuch) gesetzt. Nach dem Prinzip der Organisationsverpflichtung haben Unternehmen in der Bundesrepublik rechtskonform zu handeln und sind verpflichtet, die für die Sicherstellung des rechtskonformen Handelns erforderlichen Strukturen in den einzelnen Bereichen des Unternehmens, z.B. in den Bereichen Finanzen, Personal, Administration und EDV auszubilden. Verstöße gegen diese Organisationsverpflichtung führen zu einem Organisationsverschulden der Organe des Unternehmens und der darunterliegenden Stabstellen jeweils mit persönlicher Haftung für diese Personen. Gesetze wie das Handelsgesetzbuch (HGB) und die Abgabenordnung (AO), sowie eine ganze Zahl weiterer Vorschriften verpflichten Unternehmen seit dem 1.1.2007 zur Archivierung von E-Mails.

Verantwortlich für die E-Mail Archivierung sind in persona:

- **Geschäftsleitung**

Die Geschäftsleitung ist als Organ der Gesellschaft, unabhängig von ihrer Rechtsform, primär der Haftung ausgesetzt. Sie ist für Strategie und Ausführung verantwortlich. Sie entscheiden ob und welche technischen und organisatorischen Maßnahmen erforderlich sind.

- **IT-Leiter**

Die Unternehmensleitung kann wiederum Entscheidungsbefugnisse an Mitarbeiter des Unternehmens delegieren, etwa an den Prokuristen oder den Leiter der IT-Abteilung. Der IT-Leiter haftet dann als der sachnächste Koordinator. Er hat den besten Überblick über die IT-Infrastruktur als Ganzes.

- **Administrator**

Der IT-Leiter kann seinerseits innerhalb des Verantwortungsbereichs Verantwortung delegieren, etwa an die Administratoren oder andere Mitarbeiter. Den Administrator trifft die Haftung dann ebenso. Darüber hinaus wird er ab grober Fahrlässigkeit auch seinem Arbeitgeber gegenüber haften.

2. Gesetzliche Verpflichtung zur E-Mail Archivierung

Die nachfolgenden Rechtsvorschriften bilden die wesentlichen Eckpfeiler für eine rechtskonforme und revisions sichere Archivierung von E-Mails:

- **Handelsgesetzbuch und Abgabenordnung**

Einkaufs- und Vertragsdokumente unterfallen der handelsrechtlichen¹ und der steuerrechtlichen² Buchführungspflicht. Vor diesem Hintergrund sind die gesetzlichen Vorgaben bei der Archivierung dieser Dokumente zu beachten.

Geschäftsrelevante E-Mails haben handelsrechtlich³ eine Aufbewahrungsfrist von bis zu zehn Jahren beginnend mit dem Schluss des Kalenderjahres in dem die E-Mail empfangen wurde. Des Weiteren ist durchaus die Führung von Handelsbüchern und sonst erforderlichen Aufzeichnungen auf Datenträgern handelsrechtlich erlaubt.

- **Ergänzende Anforderungen (GOB, GoBS, GDPdU)**

Soweit in den vorgenannten Rechtsbereichen auf die – ungeschriebenen – Grundsätze ordnungsgemäßer Buchführung als Maßstab für die Archivierung von Dokumenten Bezug genommen wird, werden diese Grundsätze im Hinblick auf den Einsatz optischer und digitaler Archivierungs- und Buchungssysteme konkretisiert (bzw. an die technische Entwicklung angepasst):

(1) die „Grundsätze ordnungsgemäßer Speicherbuchführung“ (**GoS**)

(2) die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (**GoBS**)

(3) die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (**GDPdU**)

Sowohl die GoS als auch die GoBS sind im Wesentlichen von der „Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.“ (AWV) ausgearbeitet und von dem Bundesfinanzministerium übernommen worden; sie beziehen sich primär auf den Einsatz digitaler Buchführungssysteme.

- **Sonstige Anforderungen**

Eine ausführliche Darstellung aller gesetzlichen Aufbewahrungspflichten und deren korrespondierenden Aufbewahrungsfristen würden den Umfang dieses Leitfadens bei Weitem sprengen. Regelmässig ist jedoch ein Aufbewahrungszeitraum von 10 Jahren ausreichend.

3. Regelung der rein betrieblichen E Mail Nutzung als Voraussetzung für E-Mail Archivierung

Nach der aktuellen rechtlichen Situation kann einem Unternehmen nur empfohlen werden, keinesfalls private E-Mailnutzung zuzulassen und eine bisher unregelmäßige Situation unverzüglich umzustrukturieren. Wie schon ausgeführt, herrscht im deutschen Rechtsraum das Prinzip der Organisationsverpflichtung. Diese Verpflichtung wird durch Gesetze konkretisiert. Alle diese Regularien besagen kurz gesagt:

„Du sollst keine gemeingefährlichen Anlagen betreiben wenn Du sie nicht beherrscht“.

¹ § 257 Handelsgesetzbuch (HGB)

² § 147 Abgabenordnung (AO)

³ §§ 238 Abs. 2, 257 Abs.1 Nr. 2, Abs. 2, Abs. 4 Alt.2, Abs.5 HGB

Insofern ist aus der Sicht des Rechts ein E-Mail System nichts anderes als eine technische Anlage für deren Betrieb das Unternehmen die Verantwortung trägt. Stellt das Unternehmen fest, dass es die Anlage nicht mehr beherrscht, so ist sie abzustellen, solange bis der Zeitpunkt der Beherrschbarkeit wieder eintritt. Es gelten hier die gleichen Haftungsgrundsätze wie auch bei anderen „gemeingefährlichen Anlagen“, z.B. beim Automobil.

So sprechen insbesondere nachfolgende Gründe für eine rein betriebliche Nutzung des E-Mailverkehrs:

- **Kennzeichnungspflicht von E-Mails**

Seit 01.01.2007 hat der Gesetzgeber im Rahmen einer Reform des Handelsgesetzbuchs festgelegt, dass E-Mails die Bezug zum Geschäft des Unternehmens haben mit den gleichen Angaben zu kennzeichnen sind wie der typische Geschäftsbrief. Dies führt dazu, dass jede E-Mail die über eine Domainkennung verschickt wird, die auf ein Unternehmen registriert ist, mit den entsprechenden Angaben zu versehen ist. Bei fehlender Angabe führt dies zu einem Bußgeld und es besteht das Risiko, dass das Unternehmen wegen Verstoß gegen gesetzliche Vorschriften abgemahnt wird.

Mit dieser Kennzeichnungspflicht hat der Gesetzgeber die private E-Mailnutzung faktisch abgeschafft, weil selbst unbedeutende Kommunikationsvorgänge im Unternehmen, z.B. der Hinweis, dass bei Verlassen der Büroräume die Fenster zu schließen sind, von geschäftlicher Relevanz sein können. Findet z.B. ein Diebstahl im Unternehmen statt, so kann es durchaus eine Rolle spielen ob die Dienstanweisung zum Fensterschließen von der korrekten Organisationseinheit in der angemessenen Art und Weise und nötiger Frequenz erfolgt ist, um eine Versicherungsdeckung zu erhalten.

Faktisch sind damit alle externen aber auch alle hausinternen E-Mails mit den gesetzlich vorgeschriebenen Angaben zu versehen. Dieses Regularium erfolgte Seitens des Gesetzgebers auch deswegen, damit etwa im Falle einer Überprüfung durch Wirtschaftsprüfer oder sonstige Instanzen eine entsprechende Transparenz der betrieblichen Kommunikation herbeigeführt werden kann, genau so wie sie seit vielen Jahren im Bereich der Papierkommunikation herrscht.

- **Gleichlauf physikalische und digitale Post**

Nach klassischer Anschauung ist E-Mailkommunikation das Gegenstück zur Papierkommunikation. Typischerweise unterhält ein Unternehmen eine physikalische Posteinlaufstelle, in der die Post des Unternehmens eingeht, gesichtet wird und über die hausinternen Papierpoststrukturen verteilt wird.

Parallel hierzu, gibt es bei der E-Mailkommunikation eine digitale Posteinlaufstelle, für die das Unternehmen die volle Verantwortung trägt. Ist eine Domain auf ein Unternehmen, insbesondere auf eine juristische Person registriert, so setzt diese Domain bei ihrer Verwendung den Rechtschein, dass das Unternehmen handelt. Die Versendung einer E-Mail über eine auf ein Unternehmen registrierte Domain ist deshalb vergleichbar mit der Versendung des Firmenbriefbogens und verpflichtet aufgrund des Rechtsscheins die juristische Person des Unternehmens.

In der Papierwelt verwenden Mitarbeiter nicht den Firmenbriefbogen um private Angelegenheiten zu erledigen, sprich es ist keine private Nutzung vorgesehen. Dementsprechend fordert die Organisationsverpflichtung vom Unternehmen, dass dies in der digitalen Welt auf gleiche Art und Weise abläuft, es sei denn, dass Unternehmen kann massive Gründe anführen, warum ein Strukturbruch zwischen Papierkommunikation und digitaler Kommunikation zulässig sein sollte. Bis jetzt sind solche Gründe nicht bekannt geworden.

Weitere Vorteile der rein betrieblichen E-Mail Nutzung ergeben sich aus den folgenden Erwägungen:

- **Compliance mit dem Fernmeldegeheimnis**

Darüber hinaus riskiert das Unternehmen im Falle des Zulassens der privaten E-Mailkommunikation durch den Arbeitnehmer über die betriebliche Domain einen Konflikt mit dem Fernmeldegeheimnis und dem Datenschutz. Das Unternehmen darf nämlich dann diese privaten E-Mails zumindest dem Inhalt nach nicht mehr zur Kenntnis nehmen und gibt plakativ zu erkennen, dass es im Bereich der E-Mailkommunikation einen Bereich gibt, der nicht transparent ist. Je nachdem wie intensiv dieser Bereich ausgestaltet ist, wird man zu der Erkenntnis gelangen müssen, dass das Unternehmen Teile seiner IT-Anlage nicht beherrscht, weil es diese wegen Verstoß gegen Gesetze nicht kontrollieren kann. Nach den oben genannten Grundsätzen führt dies zur Verpflichtung: „Abschalten“ des E-Mailsystems.

- **Erhaltung des vollen Versicherungsschutzes**

Lässt das Unternehmen einen Strukturbruch zwischen Papierwelt und digitaler Welt zu, prozessiert es z.B. gefälligkeithalber kostenlos private Arbeitnehmer E-Mails obwohl dies nicht zum Kernbereich seiner Geschäftstätigkeit gehört, so exponiert sich das Unternehmen haftungstechnisch besonders negativ, weil ein zusätzliches Risiko auf der IT-Infrastruktur des Unternehmens stattfindet, das mit dem Geschäftszweck des Unternehmens nichts zu tun hat. Aus einer solchen Konstellation resultiert typischerweise ein besonderes Risiko das regelmäßig im Rahmen der „Betriebshaftpflicht“ Versicherung des Unternehmens nicht mitversichert ist.

- **Compliance mit SOX, KonTraG und Basel II**

Der Sarbanes - Oxley Act (**SOX**) ist eine Folge diverser Finanzskandale in den Vereinigten Staaten. SOX betrifft vor allem deutsche Unternehmen, die in den USA auftreten. Ziel dieses Gesetzes ist es, das Vertrauen der Anleger in die Richtigkeit der öffentlichen Finanzdaten von Unternehmen, die den amerikanischen Rechtsvorschriften unterliegen, wiederherzustellen. Dies wird vor allem dadurch erreicht, dass strafrechtliche und zivilrechtliche Strafen für Sicherheitsverstöße, eine unabhängige interne und externe Unternehmensprüfung und eine erhöhte Mitteilungspflicht über Gehälter der Unternehmensleitung und zu veröffentlichender Unternehmensinformationen eingeführt worden sind.

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (**KonTraG**) stellt keine Mindestanforderungen an die Unternehmen, sondern definiert erweiterte Pflichten der Unternehmensleitung bezüglich des Risikomanagements und der Risikosteuerung. Wesen des mit dem KonTraG bezweckten Risikomanagements ist, dass ein Unternehmen keine Geschäfte betreiben soll, die nicht in seinen unmittelbaren Kernbereich gehören. Das Unternehmen wird dann in einem Bereich tätig, in dem es über kein unmittelbares Know-How verfügt. Bei einer privaten Zulassung von E-Mailnutzung erbringt das Unternehmen gefälligkeithalber kostenlose Providerdienstleistungen für Dritte, die Mitarbeiter. Das Unternehmen gibt hier plakativ zu erkennen, dass es plötzlich in einem Bereich tätig ist, in dem es, anders als etwa ein professioneller Provider, über kein Know-How verfügt. Eine solche riskante Tätigkeit darf deshalb – um nicht gegen das KonTraG zu verstoßen – nicht erfolgen.

Des Weiteren treffen die Verantwortlichen nicht nur direkte gesetzliche Pflichten. Die Verpflichtung zu einem ordnungsgemäßen E-Mail Kommunikationssystem kann sich vielmehr auch indirekt für ein Unternehmen ergeben. Die Unternehmensleitung ist schließlich vertraglich und gesetzlich dazu verpflichtet, vorhersehbare Vermögenseinbußen des Unternehmens zu verhindern. Eine solche Vermögenseinbuße droht beispielsweise auch dann, wenn sich das Unternehmen nicht hinreichend auf ein Rating nach den Vorschlägen des Baseler Ausschusses für Bankenaufsicht („**Basel II**“) vorbereitet und zu diesem Zweck für eine sichere unternehmensinterne IT-Infrastruktur sorgt. In diesem Zusammenhang seien besonders der geordnete Informationsfluss und dessen lückenlose Nachvollziehbarkeit im Unternehmen erwähnt.

- **Herstellung der Revisionssicherheit**

Den Begriff „Revisionssicherheit“ gibt es offiziell nicht, er stammt aus der Branche für Dokumentenmanagementsysteme. Der Begriff „revisionssichere Archivierung“ ist elektronischen Archivsystemen zugeordnet, die den Anforderungen der GoBs (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme) genügen, ordnungsgemäß betrieben werden und Dokumente unveränderbar und verfälschungssicher archivieren. Konsequenterweise muss deshalb auch für die E-Mail Archivierung gelten, dass die Prozesse der Archivierung die Unveränderbarkeit, Fälschungssicherbarkeit, Transparenz und Rückverfolgbarkeit der E-Mail Kommunikation gewährleisten. Es gelten hier die gleichen Anforderungen wie in der Papierwelt für die Nachvollziehbarkeit des Archivierungsprozesses z.B. durch einen Wirtschaftsprüfer.

B) Was muss ich als Verantwortlicher tun? (Checkliste)

Dieser Abschnitt soll den Verantwortlichen auf ihrem Weg zu einer erfolgreichen E-Mail Archivierung helfen. Die folgende systematische Aufarbeitung möchte den Geschäftsführer, den IT-Verantwortlichen und den Administrator auf seinem Weg an die Hand nehmen und ihn bezüglich der klassischen Lösungsansätze sensibilisieren.

Verantwortliche Personen für E-Mail Archivierung

1. Aufgaben für den Geschäftsführer/Vorstand

Der Geschäftsführer/Vorstand eines Unternehmens muss der oben dargelegten Organisationsverpflichtung genügen, indem er die gesetzeskonforme Tätigkeit der Firma sicherstellt und, wie in der Papierwelt, die nötigen Entscheidungen für Archivierung von E-Mails trifft, sowie deren Umsetzung einleitet und überprüft. Hierzu hat er sicher zu stellen:

1.1 Grundvoraussetzung: Rein betriebliche E-Mail Nutzung

Wie oben schon ausführlich aufgezeigt, ist die Grundvoraussetzung einer ordnungsgemäßen E-Mail Archivierung das Verbot der privaten Nutzung des E-Mailverkehrs. Deswegen sollte sich der Geschäftsführer/Vorstand zu aller erst die Frage stellen, ob in seinem Betrieb die private Nutzung des E-Mailverkehrs erlaubt ist oder eine unregelmäßige Situation vorliegt. Sollte er zu dem Schluss kommen, dass eine Erlaubnis vorliegt, oder ist er sich über die Lage nicht im Klaren, empfiehlt es sich mit der Archivierung **nicht** zu beginnen. Es muss dann zunächst ein Prozess im Unternehmen initiiert werden, der durch Dienstanweisung klare Fronten bei der E-Mail Nutzung schafft. Dies dürfte im Hinblick auf die Kennzeichnungspflicht für E Mails seit Januar 2007 deutlich leichter sein als früher, weil es sich kein Unternehmen leisten kann, diese gesetzliche Verpflichtung zu ignorieren.

1.2 Nächster Schritt: Initiierung einer Richtlinie für die Archivierung von E-Mails

Es ist eine klassische Aufgabe der Geschäftsleitung die Compliance mit den Vorschriften des Handelsgesetzbuches und der Abgabenordnung herzustellen. In Bezug auf E-Mail Archivierung müssen Parameter wie Umfang und Zeitfenster in einer Richtlinie definiert werden. Regelmäßig wird die Geschäftsleitung diesen Prozess initiieren und dann durch die Fachabteilung umsetzen lassen. Hierbei sind auch die technisch-organisatorischen Strukturen zu beschreiben, etwa weil neue Möglichkeiten der Speicherung beschafft werden müssen. Diese Richtlinie sollte regeln:

- **Definition der zu archivierenden Inhalte**

Zunächst ist festzustellen, welche Inhalte überhaupt in die Archivierung miteinbezogen werden sollen. Mit der neuen Kennzeichnungspflicht für E-Mails sind alle nach extern (außerhalb der firmeninternen IT-Infrastruktur) gerichteten E-Mails und alle hausinternen Mails, die geeignet sind geschäftsrelevant zu sein, mit den gesetzlichen Pflichtangaben zu versehen und werden damit zu zu archivierenden E- Mails. Faktisch handelt es sich damit um alle externen und internen Mails des Unternehmens, insbesondere

- Gesendete E-Mails
- Empfangene E-Mails
- Anhänge
- Bei elektronischen Signaturen sind auch diese zu archivieren

Sinnvoll ist hier die Archivierung des

- Kontextes zu Kalendereinträgen
- Kontextes zur Adressverwaltung

weil diese Kontexterfassung besser als das reine Wiedergeben von E-Mails die konkreten Vorgänge transparent macht.

- **Definition der Archivierungszeiträume**

Nunmehr kann zur Festlegung der Aufbewahrungszeiträume übergegangen werden. In dieser Phase ist festzulegen, welche Archivierungszeiträume bei der im Unternehmen anfallenden E-Mail-Kommunikation indiziert sind. Hierbei sind vor allem die gesetzlichen Aufbewahrungsfristen zu beachten. Dies entbindet sicherlich nicht davon, Aufbewahrungsfristen zu beachten die durch Drittbestimmungen relevant werden, wie z.B. BASEL II. Im Normalfall sind insoweit Aufbewahrungszeiträume von fünf, sechs und zehn Jahren angezeigt:

Es wird deshalb prinzipiell eine Archivierung über mindestens 10 Jahre empfohlen.

- **Gesetzliche Aufbewahrungsfristen:**

- Geschäftliche Kommunikation nach dem HGB: sechs bis zehn Jahre
- Steuerrelevante Kommunikation: bis zu zehn Jahre

- **Sonstige Aufbewahrungsfristen:**

- Anforderungen nach BASEL II: bis zu fünf Jahre.

1.3 Sicherstellung der Compliance

Den nächsten Schritt für die Geschäftsleitung stellt die Überprüfung der Archivierungsrichtlinie dar. Dieser Abschnitt ist existenziell für den Erfolg der Archivierung und deswegen sehr genau und Punkt für Punkt zu überprüfen. Hierbei muss sich die Geschäftsleitung die Frage stellen, ob durch die erfolgte Archivierung die gesetzlichen Vorgaben und Ziele erreicht wurden.

- **Konformität mit HGB /AO**

Nach handelsrechtlichen Vorgaben ist jeder Kaufmann verpflichtet, Bücher zu führen und in diesen seine Handelsgeschäfte so darzustellen, dass ein sachverständiger Dritter innerhalb einer angemessenen Zeit einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens gewinnen kann. Die Grundsätze ordnungsgemäßer Buchführung müssen dabei beachtet werden. Er ist verpflichtet, eine mit der Urschrift übereinstimmende Wiedergabe der abgesandten Handelsbriefe (Kopie, Abdruck, Abschrift oder sonstige Wiedergabe des Wortlauts auf einem Schrift-, Bild- oder anderem Datenträger) zurückzubehalten.

Der Gesetzgeber lässt hierbei den nach diesem Gesetz Handelnden bewusst die Freiheit, über die Technik der Wiedergabe der Handelsbriefe selbst zu entscheiden. Er überlässt es somit dem Kaufmann über die Technik und Art und Weise der Aufbewahrung von Unterlagen Regelungen im Unternehmen zu treffen, soweit sie den Grundsätzen ordnungsgemäßer Buchführung genügen.

- **Konformität mit GOB, Microfilm-Grundsätze, GoBS, GDPdU**

Die Grundsätze ordnungsgemäßer Buchführung bei der E-Mailarchivierung können wie folgt konkretisiert werden:

- Die E-Mails werden durch Übertragung der Inhalts- und Formatierungsdaten auf einen digitalen Datenträger archiviert.
- Es muss hard- und/oder softwareseitig sichergestellt sein, dass während des Übertragungsvorgangs auf das neue Speichermedium eine Bearbeitung/Veränderung nicht möglich ist.
- Die gespeicherten E-Mails müssen indexiert werden. Dies soll wie bei gescannten Dokumenten erfolgen. Der Erhalt der Verknüpfung zwischen Index, digitalem Archiv und dem Datenträger muss während der gesamten Aufbewahrungsfrist gewährleistet sein.
- Ist die E-Mail mit farblichen Merkmalen versehen und kommt diesen eine Beweisfunktion zu, so muss die archivierte E-Mail ebenfalls diese Merkmale aufweisen.
- Die archivierten E-Mails können nur unter dem zugeteilten Index bearbeitet und verwaltet werden. Die Bearbeitungen sind strikt zu protokollieren und mit der E-Mail abzuspeichern. Eine bearbeitete E-Mail muss als solche (Kopie) bezeichnet werden.
- Es muss sichergestellt sein, dass die archivierten E-Mails mit den empfangenen Handels- oder Geschäftsbriefen und Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.
- Es muss sichergestellt sein, dass die Wiedergabe der E-Mails während der Aufbewahrungszeit gewährleistet ist und diese jederzeit innerhalb einer angemessenen Frist lesbar gemacht werden können.
- Die Originalunterlagen können darüber hinaus nur vernichtet werden, soweit sie nicht nach anderen Rechtsvorschriften im Original aufzubewahren sind.

- **Dokumentation der Archivierungsstrukturen**

Zum Nachweis der Compliance ist die Geschäftsleitung zur Dokumentation verpflichtet. Hierunter fällt nicht nur die Dokumentation der Planung bis zu diesem Punkt, sondern auch die Dokumentation des gesamten Archivierungssystems für die Mitarbeiter im Betrieb. Dies dient der Beweissicherung bei der Planung nach bestem Wissen und Gewissen gehandelt zu haben, sowie der späteren Schulung der Mitarbeiter für das neue Archivierungssystem. Denn nur ein festgelegtes Verfahren kann schließlich durch die Mitarbeiter eingehalten werden und ist revisionssicher.

2. Aufgaben für den IT-Leiter und den Administrator

2.1 Schaffung und Umsetzung einer Richtlinie für E-Mail Archivierung

Auf Initiative der Geschäftsleistung entwickeln IT-Leiter und Administrator eine Richtlinie für die E-Mail Archivierung, die alle

- unternehmenstrategischen
- technischen
- organisatorischen
- rechtlichen

Themen regelt, wie z.B:

- **Komplette betriebliche Kommunikation archivieren**

Wurde definiert welche E-Mails als betriebliche Kommunikation anzusehen sind, regelmäßig sind das alle externen und internen E-Mails des Unternehmens mit gesetzlicher Kennzeichnung wie z.B:

*Message from Michael Müller of Heussen Rechtsanwaltsgesellschaft mbH
the firm 's address is:
Briener Str. 9, D-80333 München, Germany;
Telephone: +49 (0) 89 29097-443,
Facsimile: +49 (0) 89 29097 - 200;
e-mail-address: Michael.Müller@heussen-law.de*

*Geschäftsführer: Christian Weinheimer, Georg-René Lubinski,
Sitz: Frankfurt am Main - Amtsgericht Frankfurt am Main HRB 46 524
Visit our Webpage. www.heussen-law.de*

so ist deren Archivierung zu planen und korrespondierende Dienstanweisungen zu erlassen. Dabei ist sicherzustellen, dass alle als betrieblich eingestuften E-Mails ausnahmslos in das Archivierungssystem aufgenommen werden. Diese Zielsetzung stellt sich insbesondere im Blick auf die handelsrechtlichen Vorgaben als existenziell dar.

In der Praxis hat sich gezeigt, dass der Ansatz alle E-Mails zu archivieren hier deutlich zielführender ist, als eine Definition von nicht zu archivierenden E-Mails zu versuchen, weil eine solche Definition sich am Einzelsachverhalt orientieren müsste, um dem Transparenzgebot zu genügen.

In Zweifelsfällen hilft ein Vergleich mit der Papierwelt. Wird eine Telefonnotiz dort zur Akte genommen, so wäre auch eine korrespondierende E-Mail vergleichbaren Inhalts zu archivieren.

Da sich dies in der Praxis dann doch nicht ganz so einfach darstellt, sind die folgenden Hinweise zu beachten:

- **E-Mails vom Betriebsrat**

Diskussionswürdig ist zum Beispiel die Frage, inwiefern die Mails des Betriebsrats zu archivieren sind. Hier wird empfohlen keine „Sonderregelung“ zu fahren, sondern strukturkonform auch diese Mails zu archivieren. **Um ggf. Bedürfnissen des Betriebsrats Rechnung zu tragen, sollte eine Archivierungslösung die Möglichkeit bieten, bestimmte Postfächer von der Archivierung auszunehmen.**

- **Verschlüsselte E- Mails**

Für verschlüsselte E-Mails gelten die gleichen Archivierungspflichten wie für unverschlüsselte E-Mails. Für die Erfüllung des Transparenzgebots ist es aber ausreichend, die verschlüsselte E-Mail zu archivieren, wenn gleichzeitig sichergestellt ist, dass das Unternehmen die zentrale Kontrolle über alle verwendeten Schlüssel hat und die E-Mail im Bedarfsfalle, etwa auf Anfrage eines Wirtschaftsprüfers, wieder lesbar gemacht werden kann. Hieraus folgt auch die Notwendigkeit für das Unternehmen eine zentrale Organisation und Struktur für den Bereich der Verschlüsselung von E-Mails vor zu halten. In dieser Struktur könnte auch eine Regelung enthalten sein, die ein Öffnen verschlüsselter E-Mails des Betriebsrats nur mit dessen Zustimmung vorsieht.

- **Messaging**

Eine Kommunikation via Instant Messaging wird nach aktueller Meinung noch betrachtet wie ein Telefonat. Findet hier unternehmensrelevante Kommunikation statt, so ist eine Notiz zu fertigen und diese zu archivieren

- **Archivierung von elektronischen Signaturen (Electronic Invoicing)**

Versendet das Unternehmen im Rahmen des Electronic Invoicing digitale Rechnungen mit einer elektronischen Signatur, so ist darauf zu achten, dass entweder ein Nachweis über das Bestehen einer qualifizierten Signatur zum Zeitpunkt der Ausstellung der Rechnung vor zu halten ist oder aber, was technisch mehr Sinn macht, das Unternehmen verwendet unisono Signaturen, die für einen Zeitraum von mindestens 10 Jahren Gültigkeit haben.

- **Definition der Archivierungsprozesse**

Der IT-Leiter/Administrator wird im nächsten Schritt, unter Einbezug der Definitionen der zu archivierenden Inhalte und deren korrespondierend definierten Archivierungszeiträume, die Archivierungsprozesse erarbeiten.

- **Archivieren** von allen aktuellen E-Mails, die aufbewahrt werden müssen.
- **Löschen** von E-Mails, die definitiv nicht aufbewahrt werden müssen.

- **Workflow der Archivierungssoftware**

Um ein optimales Verfahren festlegen zu können, sollte der Administrator den technischen Ablauf der Archivierung (Workflow der Software) möglichst genau beschreiben:

- Erfassen
- Speichern
- Organisieren
- Wiederherstellen

So müssen z.B. steuerrechtlich relevante E-Mails in einer Art und Weise archiviert werden, dass eine Veränderung der originalen E-Mail nicht in Betracht kommt. Hierauf ist selbstverständlich auch beim Archivierungsvorgang zu achten. Denn das beste E-Mail Archivierungssystem läuft ins Leere, wenn schon beim Archivierungsvorgang Fehler auftreten.

Steht der Archivierungsprozess fest, muss sich der Administrator nunmehr über die Art und Weise des Wiederherstellungsverfahrens (d.h. nicht nur Backup sondern echtes Restore!) der E-Mails Gedanken machen. Er muss festlegen, welche E-Mails von wem unter welchen Voraussetzungen mit welchen Rechten abgerufen werden können.

- **Hinweise zum Archivierungsmedium**

Die Regelungen der Abgabenordnung und des Handelsrechts schreiben keine besondere Speichertechnik vor. Es gibt also keine gesetzliche Forderung nach einmal beschreibbaren Speichern, auch eine Festplatte oder ein anderes Speichermedium ist gesetzeskonform (*Quelle: GOBS 1995*), wenn die sonstigen Voraussetzungen erfüllt sind.

- **Hinweise zum Archivierungssystem**

Erforderlich ist eine technische Einrichtung Software- und/oder Hardware, die in Ihrer Gesamtheit sicherstellt, dass Aufzeichnungen nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist (§ 146 Abgabenordnung und § 239 Handelsgesetzbuch). Hierbei ist sich zu stellen:

- **Unmittelbarer Zugriff**

Sind die zu archivierenden Unterlagen mit Hilfe eines Datenverarbeitungsprogramms, z.B. E-Mail erstellt worden, hat die Finanzbehörde im Rahmen einer Außenprüfung das Recht, Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen.

- **Mittelbarer Zugriff**

Die Finanzbehörde kann verlangen, dass die Daten nach Ihren Vorgaben ausgewertet werden

- **Datenträgerüberlassung**

Die Finanzbehörde kann verlangen, dass die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden

- **Dokumentation der Archivierungsstrukturen**

Alle technischen und organisatorischen Abläufe der Archivierung sind durch den IT-Leiter/ Administrator fest zu halten.

- **Dokumentation der Compliance**

Sobald sich der Administrator den obengenannten Aufgaben gestellt hat und er mit dem Ergebnis zufrieden sein kann, wird er im letzten Schritt die Erkenntnisse der Compliance dokumentieren. Dieser Schritt ist in seiner Bedeutung nicht zu unterschätzen. So führt er sich nochmals exakt vor Augen, wie die jeweiligen Anforderungen zum Ergebnis stehen und kann das Ergebnis gegenprüfen. Des Weiteren ist die Dokumentierung vorrangig zum Zwecke der Beweissicherung durchzuführen. Denn eine ordentliche Dokumentation kann insoweit den Nachweis einer ordentlichen Planung und Zweitprüfung führen.

C) Was kann bei Nichtbeachtung passieren?

Fehler bei der E-Mailarchivierungspflicht und ebenso bei der Ausführung der Archivierung können ebenso große Risiken mit sich bringen, wie eine fehlerhafte Buchhaltung. So wurde z.B. in den Vereinigten Staaten ein großes deutsches Unternehmen von der Börsenaufsicht zu einem 7stelligen Bußgeld verurteilt, weil es seiner Archivierungspflicht bei digitalen Dokumenten nur unzureichend nachgekommen ist ⁴. Darüber hinaus sind noch weitere Szenarien denkbar.

• Persönliche Haftung

Ist im Unternehmen die notwendige E-Mailarchivierung nicht oder unzureichend implementiert worden, so riskiert der Verantwortliche die Haftung des Unternehmens und seiner eigenen Person, d.h. er muss gegebenenfalls mit seinem Privatvermögen für entstandene Schäden aufkommen. Anders als im Strafrecht haftet er im Zivilrecht auch für Fahrlässigkeit. Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt nicht beachtet. Auf ein Unternehmen abgestellt, handelt also derjenige fahrlässig, der die im Geschäftsverkehr einem ordentlichen Geschäftsmann obliegende Sorgfaltspflicht verletzt. Woraus sich die Sorgfaltspflichten ergeben können, wurde bereits oben dargestellt. Wer grob fahrlässig handelt, muss übrigens damit rechnen, dass ihm entstandene Schäden nicht oder nicht vollständig ersetzt werden. So kann der Schädiger den Einwand des Mitverschuldens anführen, weil der Schaden nur in geringerem Umfang entstanden wäre. Jedoch auch der grob fahrlässig handelnde Arbeitnehmer muss mit einer, zumindest teilweisen, Inanspruchnahme durch seinen Arbeitgeber rechnen.

• Verlust von Beweisen

Einkaufs- und Vertragsdokumente stellen – sofern sie vom Aussteller unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet worden sind – im Original regelmäßig Privaturkunden im Sinne der Zivilprozessordnung dar. Der Gesetzgeber hat inzwischen eine entsprechende Anwendung der Vorschriften über Privaturkunden bei solchen E-Mails begründet, die mit einer qualifizierten elektronischen Signatur versehen sind ⁵. Als Privaturkunden begründen sie zivilprozessrechtlich Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern tatsächlich abgegeben worden sind (sog. formelle Beweiskraft ⁶). Die inhaltliche Richtigkeit der in einer Privaturkunde enthaltenen Erklärungen (sog. materielle Beweiskraft) unterliegt demgegenüber der freien richterlichen Beweiswürdigung. Danach ist das Gericht prinzipiell frei in der Beurteilung des Wertes und der Überzeugungskraft jedes einzelnen Beweismittels und kann/muss die Beweiswürdigung in jedem Einzelfall neu aus dem Inbegriff des gesamten Prozessstoffes vornehmen. Eine Ausnahme gilt lediglich im Hinblick auf Vertragsurkunden; hier wird vermutet, dass der schriftliche Vertragstext die Abreden der Parteien vollständig und richtig wiedergibt ⁷.

Für nicht qualifiziert digital signierte E-Mails, gelten diese Grundsätze jedoch nicht. Diese E-Mails sind in ihrer Eigenart nach nicht fälschungssicher. Die Schlussfolgerung hieraus, eine ordnungsgemäße Archivierung sei dann nicht notwendig ist aber im Ergebnis falsch. Denn wird in Privaturkunden auf E-Mails Bezug genommen, so wird dem Gegner in einem gerichtlichen Verfahren der Nachweis der Identitätsfälschung oder der Nichtversendung schwerlich gelingen. Insofern können selbst solche E-Mails eine Beweisführung vor Gericht erheblich erleichtern.

⁴ <http://www.tecchannel.de/storage/server/402304/index3.html>

⁵ § 371a ZPO

⁶ § 416 ZPO

⁷ Vgl. Zöller, *Zivilprozessordnung*, 23. Auflage 2002 §416 Rdnr. 10; Baumbach/Lauterbach/Albers/Hartmann, *Zivilprozessordnung*, 60. Auflage, § 416 Rdnr. 7.

Werden jedoch E-Mails gar nicht archiviert, oder ist die Umsetzung unzulänglich, drohen massive Beweisverluste, die in ihrer Konsequenz bis zum Unterliegen in einem Rechtsstreit führen können. Noch schlechter wird die Situation des Unternehmens, wenn ein Gegner sich auf korrekte Archivierung stützt und Beweise vorlegt, die das Unternehmen - mangels rechtskonformer Archivierung- nicht widerlegen kann. Hier wird man von grober Fahrlässigkeit der Verantwortlichen ausgehen müssen.

- **Keine Freizeichnung durch WP oder StB**

Wird im Unternehmen eine Betriebsprüfung durch den Wirtschafts- oder den Steuerprüfer vorgenommen, sollte ein lückenloser Nachweis gelingen, dass die relevanten E-Mails unveränderbar im Original abgelegt wurden. Gegenüber den Prüfern und anderen Instanzen ist die erforderliche Transparenz herzustellen. Wird dem nicht in ausreichender Weise Folge geleistet, ist zu befürchten, dass eine Freizeichnung durch die entsprechende Stelle nicht vorgenommen wird.

Für Interessierte bietet die IHK Hannover im Internet ⁸ einen nützlichen Fragen- und Antwortenkatalog zum Datenzugriffsrecht der Finanzverwaltung an.

- **Verlust von Versicherungsschutz bei D&O und Betriebshaftpflicht**

Wird durch die eine fehlende, oder auch nur fehlerhaft durchgeführte E-Mailarchivierung gegen Versicherungsbestimmungen verstoßen, so kann dies den teilweisen, oder sogar den totalen Ausfall des Versicherungsschutzes bedeuten.

Unternehmen, die ihrer Organisationsverpflichtung nicht genügen, bezahlen Teile ihrer Versicherungsprämie für die Betriebshaftpflicht umsonst. Bei Versicherungsschäden im Zusammenhang mit solchen Defiziten werden Versicherer die Versicherungsleistungen unter dem Vorbehalt eines Mitverschuldens kürzen und gegebenenfalls, für zukünftige Fälle, die Versicherungsprämie erhöhen.

Zudem besteht hier die Gefahr, dass Versicherungen, wie die Directors & Officers Versicherung, zur Absicherung der Geschäftsleitung keine volle Protektion entfalten.

München, 25. Mai 2007
 RA Robert Niedermeier
 Heussen Rechtsanwalts-gesellschaft, München

⁸ http://www.hannover.ihk.de/fileadmin/pdf/ihk/themen/handel_dienstleistungen/070417_Frage-_und_Antwortkatalog_.pdf



ÜBER MIMOSA SYSTEMS

Mimosa Systems stellt Informationsmanagement-Lösungen der jüngsten Generation her. Mimosa NearPoint™ stellt ein permanent aktives Content-Archiv für den Microsoft®-Exchange-Server zur Verfügung. NearPoint bietet Archivierung, Rechercheoptionen und Storage Management in einer einzigen Lösung und stellt so den kontinuierlichen und rechtskonformen Betrieb des E-Mail-Servers sicher.

Weitere Informationen:
sales_germany@mimosasystems.com