# Rechtsaspekte der E-Mail-Kommunikation

von Rechtsanwalt Dr. Ivo Geis

GROUP TECHNOLOGIES
Email simplified

## Abstrakt

E-Mail ist eine etablierte Form der Unternehmenskommunikation, die ständig wächst. So vielfältig die Nutzung der E-Mail-Kommunikation ist, so vielfältig sind auch die Rechtsaspekte. Als problematisch hat sich die Nutzung des E-Mail-Accounts für private Zwecke der Mitarbeiter entwickelt (1). E-Mail-Kommunikation enthält personenbezogene Daten und muss damit die Anforderungen des Datenschutzrechtes erfüllen (2). E-Mail-Kommunikation mit unternehmensbezogenen Inhalten muss als steuerlich erheblich archiviert werden. Die Archivierung nach den Grundsätzen der Ordnungsmäßigkeit bedeutet Integrität der Dokumente (3). In einer rechtlichen Auseinandersetzung ist diese Integrität der Dokumente das Argument für deren Beweissicherheit (4). Damit der Empfänger einer E-Mail sich auf die Identität des Absender verlassen kann, muss die E-Mail eines Unternehmens Angaben enthalten, die dem Empfänger die Identifikation des Absenders ermöglichen (5). Im Ergebnis entsteht die Rechtssicherheit der E-Mail-Kommunikation, indem verschiedenartige rechtliche Anforderungen erfüllt werden (6).

## Über den Autor

Dr. Ivo Geis ist Rechtsanwalt in Hamburg und arbeitet im Recht der Informationstechnologie mit dem Schwerpunkt in den Themen Rechtsfragen der elektronischen Kommunikation, Dokumentation und des Datenschutzes. Zu diesen Themen nimmt Dr. Geis auch in seinen Veröffentlichungen Stellung.

Ehrenamtlich ist Dr. Geis Leiter des Arbeitskreises Rechtsfragen der digitalen Kommunikation der AWV Arbeitsgemeinschaft für wirtschaftlichen Verwaltung e.V. in Eschborn. Von Anfang des Jahres 1998 bis zum Anfang des Jahres 2003 war Dr. Geis Vorsitzender der Hamburgischen Datenschutzgesellschaft e.V.

## Inhalt

# 1 Nutzung des E-Mail-Accounts in Unternehmen für private Zwecke

Die private Nutzung des E-Mail-Accounts durch Mitarbeiter ist ein Konfliktbereich zwischen Mitarbeiterinteressen und Unternehmensinteressen. Dieser Konflikt bedeutet Rechtsrisiken bei der Abwehr von SPAM und dem Schutz vor Viren (1.1). Rechtssicherheit kann durch eine Betriebsvereinbarung oder, wenn ein Betriebsrat nicht besteht, durch eine E-Mail-Policy erreicht werden (1.2).

## 1.1 Die Rechtsfragen von SPAM-Abwehr und Virenschutz

SPAM und Viren sind Belästigungen, die den Betriebsablauf beeinträchtigen. E-Mail-Nachrichten mit unternehmensbezogenem Inhalt können die Unternehmen als SPAM oder wegen Virenverdachts löschen. Die Abwehr von Nachrichten, die mit persönlichem Inhalt an Mitarbeiter gerichtet sind, sind wegen SPAM-Abwehr (1.1.1) und Virenschutz (1.1.2) zum rechtlichen Problem geworden.

### 1.1.1 SPAM-Abwehr

Provider und Internutzer werden von unerbetenen Werbe-Mails, sogenannter SPAM-Mail, überflutet. SPAM ist eine Belästigung in mindestens zweifacher Hinsicht. SPAM-Mails können Viren, Würmer und andere Schadprogramme transportieren und der Aufwand für das Löschen ist ein wirtschaftlicher Faktor. Im Kampf gegen SPAM setzen Provider und Nutzer Filtersysteme ein. Ziel einer Filterung ist es, auf Grund charakteristischer Merkmale die Nachricht als SPAM zu identifizieren, um sie im nächsten Schritt zu löschen oder in Ordner zu verschieben. Diese SPAM- Filterung ist für Unternehmen sowohl in dem Fall, in dem die private E-Mail-Nutzung der Mitarbeiter erlaubt ist, ein Rechtsrisiko als auch in dem Fall, in dem sie verboten ist. Ist Mitarbeitern die private Nutzung ihres E-Mail-Accounts ausdrücklich erlaubt oder wird sie stillschweigend geduldet, so stellt das Unternehmen Telekommunikationsdienste zur privaten Nutzung zur Verfügung und wird zum TK-Diensteanbieter. Damit ist das Fernmeldegeheimnis gemäß § 88 TKG (Telekommunikations-Gesetz) zu beachten, dessen Verletzung gemäß § 206 Abs. 2 StGB (Strafgesetzbuch) strafbar ist. Diese Strafbarkeit riskieren Unternehmensleitung und Administratoren durch Filtern von E-Mail-Nachrichten. Dieses Risiko ist durch das Verbot der privaten E-Mail-Nutzung nicht beseitigt. In diesem Falle ist die nach Artikel 1 und Artikel 2 GG verfassungsrechtlich geschützte Privatsphäre der Mitarbeiter zu beachten. Im Ergebnis ist SPAM-Filterung nach der Gesetzeslage ein Rechtsrisiko.

### 1.1.2 Virenschutz

Virenscanning ist notwendig, um interne Netze und Dateien gegen Angriffe von außen durch Viren, Würmer und trojanische Pferde zu schützen. Aus rechtlicher Sicht sind bei diesen Maßnahmen die widerstreitenden Interessen der Beteiligten abzuwägen. Auf der Seite des Anlagenbetreibers muss die Datensicherheit gewährleistet und die IT-Systeme vor Schäden durch Viren geschützt werden, auf der Seite des Empfängers muss der Schutz von dessen personenbezogenen Daten sichergestellt werden. Der damit gebotene Grundsatz der Verhältnismäßigkeit gebietet, das am wenigsten belastende Mittel zu wählen. Unter diesem Gesichtspunkt der Verhältnismäßigkeit ist es problematisch, virenverseuchte Mails zu löschen. Einen zulässigen Weg bietet die Quarantänelösung, die die virenverseuchte E-Mail nicht zustellt, sondern in einen gesonderten Ordner umleitet und den Adressaten darüber informiert, dass eine an ihn gerichtete Nachricht Viren enthält und wie die Mail für ihn zugänglich ist. Dieses Verfahren bietet den Vorteil, dass es ausschließlich automatisiert abläuft und damit datenschutzrechtlich unbedenklich ist, da die Inhalte der E-Mail durch eine Kontrollinstanz, wie etwa Administratoren, nicht zur Kenntnis genommen werden.

## 1.2 Betriebsvereinbarung und E-Mail-Policy

Wegen dieser kritischen Rechtslage bei der SPAM-Abwehr und beim Virenschutz ist eine Betriebsvereinbarung oder, wenn ein Betriebsrat nicht besteht, eine E-Mail-Policy zu empfehlen. In einer Betriebsvereinbarung oder E-Mail-Policy sollte das Recht des Unternehmens bestimmt werden,

- Nachrichten auszufiltern, die nicht dem Unternehmenszweck noch der angemessenen privaten Nutzung entsprechen,
- Kontrollen durchzuführen, ob die private Nutzung des Mitarbeiters auf einen angemessenen Umfang und rechtmäßige Inhalt beschränkt ist und
- für die Abwesenheit des Mitarbeiters einen Vertreter zu bestellen, der aus organisatorischen und betriebsbedingten Gründen berechtigt ist, auf den E-Mail-Account zuzugreifen.

Hierbei sollten nach dem Prinzip der Verhältnismäßigkeit die Unternehmensinteressen und das Recht des Mitarbeiters auf seine Privatsphäre möglichst berücksichtigt werden. So sollten Filterprogramme auf rechtswidrige und eindeutig überflüssige Nachrichten beschränkt sein, Kontrollen aus Anlässen durchgeführt werden und Vertreter auf den E-Mail-Account zugreifen dürfen, um geschäftsrelevante Nachrichten abzurufen.

# 2 Datenschutz: Zugriffsschutz und Verschlüsselung

Die E-Mail-Kommunikation unterliegt dem Datenschutz, da sie personenbezogene Daten enthält. Die durch den Datenschutz geforderte Datensicherheit wird durch Zugriffsschutz (2.1) und Verschlüsselung erreicht (2.2).

## 2.1 Zugriffsschutz

Der entscheidende datenschutzrechtliche Aspekt der elektronischen Archivierung ist die Zugriffskontrolle nach Nr.3 der Anlage zu § 9 BDSG. Unter Zugriffskontrolle werden technische und organisatorische Maßnahmen verlangt, die „gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegend Daten zugreifen können, und dass personenbezogene Daten bei Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert verändert oder entfernt werden können“. Danach umfasst Zugriff jede Aktivität in Bezug auf die gespeicherten Daten, die den Informationswert verfügbar macht, insbesondere seine Kenntnisnahme oder seine Nutzung ermöglicht. Zugriff ist gegeben, wenn das Datenverarbeitungssystem veranlasst wird, dass die Daten auf dem Bildschirm lesbar gemacht, ausgedruckt und auf einen Datenträger übertragen werden. Beispiele für Maßnahmen der Zugriffskontrolle sind das Festlegen der Zugriffsbefugnisse, die Identifikation der Zugreifenden und die Protokollierung der Zugriffe und Verschlüsselung.

## 2.2 Verschlüsselung

Hochgradige Sicherheit der Dokumente vor dem Zugriff Unberechtigter wird durch die asymmetrische Verschlüsselung (Public-Key-Verfahren) erreicht. Bei einer asymmetrischen Datenverschlüsselung werden verschiedene Schlüssel zum Verschlüsseln und Entschlüsseln verwendet. Zum Verschlüsseln dient der öffentliche Schlüssel (public key), der von einem potenziellen Empfänger bekannt gegeben wird. Zum Entschlüsseln dient der private Schlüssel (private key), der von seinem Besitzer verwahrt wird und auf den kein anderer Zugriff haben darf. Aus dem öffentlichen Schlüssel lässt sich der private Schlüssel nicht ableiten und allein aus dem öffentlichen Schlüssel lässt sich die verschlüsselte Nachricht nicht dechiffrieren. Damit sind die Dokumente wie in einem virtuellen Container dem Zugriff Unberechtigter entzogen.

## 2.3 Technikneutralität

Zugriffsschutz und Verschlüsselung sind Funktionalitäten, die von dem Gesetzgeber mit dem Bundesdatenschutzgesetz technikneutral ausgestaltet sind. E-Mail-Archivierungssysteme sind damit nicht auf eine bestimmte Lösung für den Zugriffsschutz und die Verschlüsselung festgelegt. Wichtig ist alleine der Effekt, dass der Zugriff Unberechtigter verhindert wird.

# 3 Rahmenbedingungen der E-Mail-Archivierung

Nach der Kommunikationsphase ist die geschäftsrelevante E-Mail-Kommunikation nach Handelsrecht und Steuerrecht aufzubewahren (3.1). Das Bundesfinanzministerium hat mit den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) (3.2) und mit den „Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) (3.3) die Anforderungen an die elektronische Aufbewahrung steuerlich relevanter Dokumente bestimmt. Basel II, Sarbanes Oxley Act (SOX) und die EuroSOX-Richtlinien wirken sich auf die Dokumentationspflicht aus: Die Anforderungen können nur durch möglichst lückenlose Dokumentation erfüllt werden (3.4). Es ist zwingend anzunehmen, dass diesen komplexen Anforderungen an die ordnungsmäßige Archivierung der E-Mail-Kommunikation Archivierungssysteme entsprechen, die hierauf spezialisiert sind (3.5).

## 3.1 Die E-Mail als Handelsbrief und die Pflicht zur Archivierung

Nach der Kommunikationsphase ist die geschäftsrelevante E-Mail zu archivieren, denn nach § 257 Handelsgesetzbuch (HGB) sind empfangene Handelsbriefe (§ 257 Abs.1 Nr. 2 HGB), die Wiedergabe abgesandter Handelsbriefe (§ 257 Abs.1 Nr. 3 HGB) und Buchungsbelege (§ 257 Abs.1 Nr. 4 HGB) geordnet aufzubewahren. Handelsbriefe sind nach § 257 Abs. 2 HGB nur Schriftstücke, die ein Handelsgeschäft betreffen. Dieser historische Wortlaut des HGB ist an die elektronische Kommunikation anzupassen und umfasst damit nicht nur papiergebundene Schriftstücke, sondern auch die E-Mail-Kommunikation, denn mit einer E-Mail kann wie mit einem Schriftstück eine rechtswirksame Willenserklärung abgegeben werden, mit der Rechte und Pflichten begründet werden. Rechtlich kritisch ist das Wirksamwerden der E-Mail gegenüber dem Empfänger. Hierzu muss die E-Mail dem Empfänger nach § 130 Bürgerliches Gesetzbuch (BGB) zugegangen sein. Zugang liegt vor, wenn die Erklärung so in den Machtbereich des Empfängers gelangt ist, dass er unter gewöhnlichen Umständen Kenntnis nehmen kann. Dies ist ihm möglich, wenn die E-Mail auf der von ihm bereitgehaltenen Empfangseinrichtung angekommen ist. Als solche Einrichtung gilt das E-Mail-Postfach des Empfängers. Das gilt für den Fall, dass die E-Mail direkt an den Empfänger übermittelt wird und auf dessem lokalem Mail-System gespeichert wird und für den Fall, dass die Mailbox auf dem Server eines Providers angelegt ist. Das Rechtsrisiko für den Empfänger besteht darin, dass die Nachricht ihm auch dann zugerechnet wird, wenn er die Nachricht nicht abgerufen hat. Deshalb sollte organisatorisch sichergestellt werden, dass in dem E-Mail-Postfach bereitgestellte Nachrichten während der Geschäftszeiten abgerufen werden. Die Aufbewahrung muss den Grundsätzen ordnungsmäßiger Buchführung entsprechen (§ 257 Abs. 3 Satz 1 HGB) und es muss sichergestellt sein, dass die Daten währen der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können (§ 257 Abs. 3 Satz 1 Nr. 2 HGB). Die

Buchungsbelege sind 10 Jahre, die empfangenen und die Wiedergabe der abgesandten Handelsbriefe sind 6 Jahre aufzubewahren (§ 257 Abs. 4 HGB). Die Aufbewahrungspflichten sind von dem Bundesfinanzministerium durch die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ und die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ konkretisiert worden.

## 3.2 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

Dokumente, die für die Besteuerung von Bedeutung sind, sind für die Prüfung durch die Finanzbehörde zu archivieren. Dies sind nach Ziffer I. Nr. 1 GDPdU Daten der Finanzbuchhaltung, der Anlagenbuchhaltung und der Lohnbuchhaltung. Damit sind alle Dokumente erfasst, die für das Buchen von Geschäftsvorfällen relevant sind. Hierzu zählt die steuerlich relevante E-Mail-Kommunikation. Dies hat das Bundesfinanzministeriums in seiner Veröffentlichung „Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung“ (Stand 23. Januar 2008) unter Ziffer III. Nr. 9 festgestellt (www.Bundesfinanzministerium.de) (Suchbegriff: Datenzugriff). Nach § 147 AO muss der Steuerpflichtige sicherstellen, dass die Daten während der Dauer der sechsjährigen Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können. Damit ist die E-Mail-Kommunikation auf maschinell auswertbaren Datenträgern während der gesamten Aufbewahrungsfrist zu archivieren. Wenn originär digitale Unterlagen auf maschinell auswertbaren Datenträgern zu archivieren sind, dann dürfen sie nicht, so die Schlussfolgerung des Bundesfinanzministeriums in Ziffer III. Nr. 1 der GDPdU, ausschließlich in ausgedruckter Form oder auf Mikrofilm aufbewahrt werden. Im Ergebnis bedeutet dies, dass der Steuerpflichtige zur elektronischen Archivierung der E-Mail-Kommunikation verpflichtet ist und die Prüfer der Finanzbehörden unterstützen muss, damit sie auf die elektronischen Dokumente zugreifen und sie auswerten können.

## 3.3 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

Allgemeingültige Regeln für die ordnungsmäßige Archivierung elektronischer Dokumente hat das Bundesfinanzministerium mit Schreiben vom 7.11.1995 “Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme” (GoBS), formuliert. Mit der Aufbewahrung entsprechend diesen Grundsätzen soll die elektronische Dokumentation gegen Änderungen geschützt werden. Diese Änderungssicherheit soll durch archivtaugliche Speichermedien und Speicherformate erreicht werden. Zulässig und damit ordnungsmäßig im Sinne der handelsrechtlichen und steuerrechtlichen Aufbewahrungsvorschriften sind alle Speichermedien: die CD-Rom, die nicht wiederbeschreibbare Platte, die wiederbeschreibbare Platte und das Speicherband.

Entscheidend für die Ordnungsmäßigkeit sind die hardwaremäßigen, softwaremäßigen und organisatorischen Sicherheitsfunktionen, die für das jeweilige Speichermedium gesondert ausgeprägt sein können. Unter den Speicherformaten gilt für Worddateien das Format PDF/A als die ideale Lösung, da dieses Format eine ausgeprägte Integritätsfunktion hat. Um den Zugriff auf das Dokument sicherzustellen, muss das Dokument mit einem Index versehen sein, unter dem es aufgefunden werden kann. Diese Sicherheit des Zugriffs ist bei den Massen archivierter E-Mails ein kritisches Problem, das durch Metadaten gelöst wird, die elektronische Objekte formal und inhaltlich beschreiben und identifizieren.

## 3.4 Basel II, Sarbanes Oxley Act und EuroSOX

Die europäische Regel für Kreditinsitute „Basel II“ (3.4.1), das US-Gesetz „Sarbanes Oxley Act“ (3.4.2) und die „EuroSOX-Richtlinien“ (3.4.3) betonen die Pflicht der Unternehmen, die Organisation, wozu die IT-Organisation und damit die E-Mail-Archivierung gehören, zu dokumentieren.

### 3.4.1 Basel II

Zweck der „Internationalen Konvergenz der Kapitalmessung und Kapitalanforderung (Basel II)“ ist die wirtschaftliche Sicherheit von Kreditinstituten. Der kritische Punkt sind die „operationellen Risiken“: die Gefahr von Verlusten, die durch das Versagen interner Systeme oder durch externe Ereignisse eintreten. Als operationelle Risiken gelten Rechtsrisiken, da sie zu Bußgeldern, Geldstrafen und Strafzahlungen führen können. Die Abwehrstrategie gegen solche Risiken ist die elektronische Dokumentation, um die Erfüllung der Pflichten in einem Streitfall beweisen zu können. Dies ist ein allgemeingültiger Grundsatz unternehmerischen Handelns und nicht auf Kreditinstitute beschränkt. Deshalb strahlt “Basel II“ mit der Konsequenz der Dokumentationspflicht auch auf andere Unternehmen als Kreditinstitute aus.

### 3.4.2 Sarbanes Oxley Act

Wie Basel II so zeigt auch der „Sarbanes Oxley Act“ indirekte Rechtswirkungen. Das zentrale Anliegen des „Sarbanes Oxley Act“ ist die „compliance“ des Finanz- und Rechnungswesens, um Investoren zu schützen. Nach der zentralen Vorschrift des Sec. 404 haben Unternehmen jährlich ihr internes Kontrollsystem prüfen zu lassen und über das Ergebnis in ihrem Abschluss zu berichten. Hierfür ist eine vollständige Dokumentation Grundlage. Von den Regelungen des Sarbanes Oxley Act sind in Deutschland Unternehmen betroffen, die auf Grund der Inanspruchnahme des US-amerikanischen Kapitalmarktes an US-amerikanischen Börsen registriert sind und mit diesen gesellschaftsrechtlich verbundene Unternehmen. Dies zwingt dazu, rechtserhebliche Dokumente nach den Grundsätzen der Ordnungsmäßigkeit vollständig elektronisch zu archivieren. Dies entspricht den Anforderungen des deutschen Archivierungsrechts durch GDPdU und GoBS.

### 3.4.3 EuroSOX

An die US-amerikanische SOX-Gesetzgebung knüpft EuroSOX an, eine Umschreibung für die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006, geändert durch die Richtlinie 2008/30/EG vom 11. März 2008 für die Aktionärssicherheit sowie die Rechnungs- und Abschlussprüfung. Die EuroSOX-Richtlinien sind noch nicht in nationales Recht umgesetzt worden. Es ist geplant, sie in das Bilanzmodernisierungsgesetz aufzunehmen. Die Richtlinien wirken indirekt auf die E-Mail-Archivierung. Nach Art. 29 der Richtlinie 2006/43/EG werden für die Abschlussprüfung Qualitätsstandards verlangt, die nur durch eine Dokumentation der IT-Infrastruktur, zu der auch die E-Mail-Archivierung gehört, erfüllt werden können. Hiermit wird die Bedeutung der sicheren IT-Infrastruktur für Unternehmen und deren Aktionäre betont. Dieses Risikomanagement der IT-Infrastruktur ist bereits durch das „Gesetz zur Kontrolle und Transparenz im Geschäftsbereich“ (Kontra- Gesetz) vom 27. April 1998 gefordert worden. Das Gesetz, das in das Aktiengesetz integriert worden ist, bezweckt, dass durch Selbstorganisation das Unternehmen vor Schäden geschützt wird. Nach § 91 Abs. 2 AktG hat der Vorstand ein Überwachungssystem einzurichten, um Schäden, die dem Unternehmen drohen, möglichst früh zu erkennen. Tritt ein Schaden ein, so wird nach 93 Abs. 2 AktG das Verschulden des Vorstands vermutet. Unter diese Organisationspflichten fällt auch die IT-Infrastruktur. Sie erfordert ein hochentwickeltes Spezialwissen. Die Organisationspflichten der Geschäftsleitung können deshalb durch Delegation an Spezialisten reduziert werden. Dies sind gesetzliche Anforderung, die in ihrer Allgemeingültigkeit für alle Unternehmen unabhängig von ihrer Rechtsform gelten und die Pflicht zur Dokumentation der IT-Infrastruktur einschließlich der Archivierungssysteme bestätigen, wie sie nach Basel II, dem Sarbanes Oxley Act und den EuroSOX-Richtlinien verlangt wird.

## 3.5 Das E-Mail-Archivierungssystem als Faktor ordnungsmäßiger Archivierung

E-Mail-Archivierungssysteme sind ein entscheidendes Argument für die ordnungsmäßige Archivierung der E-Mail-Kommunikation. Hierin besteht auch der Wert der E-Mail-Archivierungssysteme für die Beweisqualität der archivierten E-Mail-Kommunikation.

# 4 Beweisqualität der E-Mail-Kommunikation

In einem Rechtsstreit muss sich die archivierte E-Mail als beweissicher bewähren. Das deutsche Beweisrecht bietet die Wahl zwischen freier Beweiswürdigung des Gerichts und Urkundenqualität (4.1). Die Geschäftsbeziehungen zwischen deutschen Unternehmen und US-Unternehmen begründen das Risiko eines Rechtsstreits in den USA. Nach den eDiscovery Rules ist die prozesserhebliche E-Mail-Kommunikation zu archivieren (4.2). Im Ergebnis erweist sich ein E-Mail-Archivierungssystem nach deutschem Recht und nach US-Recht als Indiz für die Beweissicherheit (4.3).

## 4.1 Das deutsche Beweisrecht

Durch die elektronische Archivierung der E-Mail-Kommunikation nach den Anforderungen der Ordnungsmäßigkeit werden Indizien für die Integrität und damit die Beweissicherheit der elektronisch archivierten Dokumente begründet. Hierdurch besteht Beweissicherheit im Rahmen der freien Beweiswürdigung des Gerichts nach § 286 Zivilprozessordnung (ZPO). Im Rahmen der freien Beweiswürdigung bewertet das Gericht inwieweit die Qualität der elektronischen Archivierung die Integrität der Dokumente sicherstellt. Urkundenqualität, durch die das Gericht an den Inhalt des Dokuments gesetzlich gebunden ist, wird nur erreicht, wenn der Aussteller seine elektronische Erklärung mit einer qualifizierten elektronischen Signatur abgegeben hat. Die qualifizierte elektronische Signatur muss nach § 2 Nr. 3 Signaturgesetz (SigG) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein und mit den Daten, auf die sie sich bezieht, verknüpft sein, damit eine nachträgliche Veränderung der Daten erkannt werden kann. Für elektronische Dokumente mit qualifizierter elektronischer Signatur gelten nach § 371a Abs. 1 S. 1 ZPO die Vorschriften zur Beweiskraft privater Urkunden entsprechend. Damit sind diese Dokumente zwar Objekte des Augenscheins, begründen aber in entsprechender Anwendung des § 416 ZPO vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von dem Aussteller abgegeben und damit authentisch sind. Dieser Standard der qualifizierten elektronischen Signatur hat in der E-Mail-Kommunikation nur geringe Resonanz gefunden. Üblich ist die E-Mail-Kommunikation ohne qualifizierte elektronische Signatur. Dies hat die Bundesregierung erkannt. Deshalb sollen unter dem Namen „De-Mail“ künftig E-Mails zuverlässig und vor Veränderungen geschützt in einem sicheren Kommunikationsraum zwischen registrierten Nutzern versendet werden können. De-Mail-Anbieter müssen dazu in einem staatlichen Zertifizierungsverfahren nachweisen, dass sie hohe Anforderungen an Sicherheit und Datenschutz erfüllen. Das Konzept wird ergänzt durch eine sichere Dokumentenablage und einen benutzerfreundlichen Identitätsnachweis. De-Mail wird in Bürgerportalen für die Kommunikation mit Behörden zur Verfügung gestellt. Wie der Website des „Beauftragten der Bundesregierung für Informationstechnik“ (www.cio.bund.de) zu entnehmen ist, sind erste Projekte für das Jahr 2009

geplant. In der E-Mail-Kommunikation, in der nicht qualifizierte elektronische Signaturen oder das De-Mail-Verfahren genutzt werden, ist die Beweissicherheit von der Initiative des Einzelnen abhängig, durch ordnungsmäßige Archivierung nachweisbare Indizien für die Integrität der gespeicherten Dokumente zu schaffen. Hierfür ist die Aufbewahrung der E-Mail-Kommunikation in einem E-Mail-Archivierungssystem ein unterstützendes Argument.

## 4.2 Geschäftsbeziehungen mit den USA und die Pflicht zur E-Mail-Archivierung

Die internationale elektronische Kommunikation weist über den Raum des deutschen Rechts hinaus. So ist der Beweiswert elektronischer Dokumente im Austausch mit den USA wegen der E-Mail-Kommunikation zwischen deutschen und US-Geschäftspartnerschaften ein aktuelles Thema. Ist für ein Unternehmen absehbar, dass es zu einem Rechtsstreit kommt, so darf ein Unternehmen entsprechend den US-amerikanischen eDiscovery Rules potentielles Prozessmaterial nicht löschen. Bewahrt ein Unternehmen die Informationen nicht auf, gilt dies als Beweisvereitelung, die zu prozessualen Sanktionen und Geldstrafen führen kann. Im Falle eines Rechtsstreits in den USA muss die deutsche Prozesspartei archivierte elektronische Dokumente, die prozessrelevant sind, in die USA übermitteln. Auch aus diesem Aspekt der eDiscovery-Rules ist es notwendig, dass die E-Mail-Kommunikation zwischen deutschen Unternehmen und den US-amerikanischen Geschäftspartnern archiviert wird.

## 4.3 Das E-Mail-Archivierungssystem als Garant für die Beweissicherheit

Das entscheidende Indiz für die Beweissicherheit archivierter E-Mail-Dokumente ist ein E-Mail-Archivierungssystem. Dies gilt gleichermaßen im deutschen Beweisrecht und im US-Beweisrecht. Damit ist ein E-Mail-Archivierungssystem auch in einem Rechtsstreit in den USA das entscheidende Argument für die Beweisqualität der dem Gericht im eDiscovery-Verfahren vorgelegten E-Mails.

## 5 Pflichtangaben in geschäftlichen E-Mails

Nach dem „Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister“ (BGBl. S. 2553) gelten die Pflichtangaben für Geschäftsbriefe „gleichviel in welcher Form“, also auch für elektronische Briefe. Geschäftsbrief ist grundsätzlich jedes Schreiben über geschäftliche Angelegenheiten, das an einen bestimmten Empfänger gerichtet ist. In allen E-Mails müssen neben der Anschrift und der Gesellschaftsform die Handelsregisternummer, das zuständige Registergericht und Geschäftsführer/Vorstand/Aufsichtsrat angegeben werden. Betroffen sind Unternehmen, die im Handelsregister eingetragen sind: der Einzelkaufmann, die offene Handelsgesellschaft (oHG), und Kommanditgesellschaft (KG), die Gesellschaft mit beschränkter Haftung (GmbH), die GmbH & Co.KG, GmbH & Co, oHG, AG & Co. KG und AG & Co. oHG und die Aktiengesellschaft (AG). Die Normen, die die Pflichtangaben auf Geschäftsbriefen regeln, sind Ordnungs- und keine Formvorschriften. Insofern hat ein Verstoß auf die Gültigkeit der in einem Geschäftsbrief enthaltenen rechtsgeschäftlichen Erklärung keinen Einfluss. In der Nichtmitteilung der erforderlichen Angaben ist auch nicht ohne weiteres ein Wettbewerbsverstoß zu sehen. Das Registergericht kann jedoch bei Nichtbeachtung der Ordnungsvorschrift ein Zwangsgeld von bis zu € 5.000,-- festsetzen.

## 6 Ergebnis

Die Nutzung des E-Mail-Accounts durch Mitarbeiter für private Zwecke ist ein zentrales Thema der Unternehmenskultur, das durch Betriebsvereinbarung oder E-Mail-Policy geregelt werden sollte. Datenschutz der E-Mail-Kommunikation wird durch Zugriffsschutz und Verschlüsselung erreicht. Die Archivierung der E-Mail-Kommunikation nach den Grundsätzen der Ordnungsmäßigkeit sichert die Integrität der elektronischen Dokumente und damit deren Beweisqualität. Diese Argumentation unterstützt ein E-Mail-Archivierungssystem.

Hamburg, den 29. Mai 2009

Dr. Ivo Geis
Rechtsanwalt

Hinweis: Dieses Dokument stellt einen generellen Leitfaden dar, kann aber eine rechtsverbindliche, individuelle Beratung nicht ersetzen. Für die Angaben kann keine Garantie und Gewährleistung bzgl. der Genauigkeit übernommen werden.

# 7 GROUP Technologies – Ein Geschäftsbereich der GROUP Business Software AG

*Der GROUP Geschäftsbereich für E-Mail, Archivierung und Administration*

Durchgängige Kommunikation ist ein wesentliches Kriterium für den Erfolg von Unternehmen. Effiziente E-Mail-Korrespondenz mit Kunden und Geschäftspartnern, aber auch intern entscheidet darüber, ob sich ein Unternehmen von der großen Masse erfolgreich absetzen kann oder ob es lediglich standardisierte Kommunikationsprozesse anwendet.

E-Mail ist nicht mehr nur Mittel zum Zweck der Kommunikation, sondern längst das wichtigste Instrument zur konstruktiven Zusammenarbeit über eine zeitliche bzw. räumliche Distanz hinweg. Gerade diese Tatsache macht E-Mail-Management zu der unternehmenskritischsten Anwendung überhaupt. Zahlreiche interne und externe Risiken, gesetzlichen Vorgaben, Unternehmenspolicies und -standards sind damit verbunden.

GROUP Technologies hat sich deshalb auf die Entwicklung prozessorientierter, zentraler und wartungsfreundlicher E-Mail-Management-Lösungen für die weit verbreiteten Plattformen Lotus Domino und Microsoft Exchange spezialisiert und sich als Anbieter dieser Lösungen weltweit etabliert.

*GROUP Technologies – Kompetenzen*

**Kompetent:** GROUP Technologies ist für seine Kunden der alleinige Ansprechpartner, wenn es im Bereich E-Mail um Sicherheit, Compliance oder IT-Effizienz geht. Alle unternehmerischen Herausforderungen werden auf Basis eines zentralen und regelbasierten E-Mail-Managements zuverlässig gelöst.

**Zentral:** Umfassender Viren- und Spam-Schutz, automatische Ver- und Entschlüsselung, Durchsetzung von unternehmerischen sowie gesetzlichen Vorgaben und die Realisation einer Echtzeit-Archivierung im kompletten Unternehmen – GROUP Technologies macht die Verwaltung all dieser Prozesse an zentraler Stelle möglich.

**Unkompliziert:** Die E-Mail-Lösungen von GROUP Technologies zeichnen sich durch eine hohe Benutzerfreundlichkeit und einzigartige Effizienz aus. Die serverbasierten Lösungen reduzieren Aufwand und Interaktion seitens der E-Mail-Anwender auf ein absolutes Minimum. Denn die unternehmensweite Einbeziehung der E-Mail-Aktivitäten aller Nutzer geschieht serverseitig und kann auf diese Weise zentral über nur eine einzige Konsole administriert werden.

**Konform:** Zentral definierte Prozesse gewährleisten die Einhaltung von unternehmenseigenen Policies und gesetzlichen Vorgaben bei der E-Mail-Kommunikation. Intuitive Konfigurationsmöglichkeiten erlauben es, die E-Mail-Infrastruktur ohne weiteres an die Anforderungen des Marktes, des Unternehmens oder neuer Gesetze anzupassen.

*GROUP Technologies – Kunden*

Zu den Kunden des Geschäftsbereiches GROUP Technologies zählen weltweit namhafte Konzerne, wie die Deutsche Bank, Ernst & Young, Honda, Heineken, Allianz und Miele. Mehr als drei Millionen Anwender und über 3.000 Unternehmen weltweit vertrauen die Sicherheit und die Organisation ihrer Systeme den Lösungen der GROUP Technologies an.

**European Headquarters**
**GROUP Business Software AG**
MesseTurm
60308 Frankfurt/Germany
Phone: +49 69 789 8819-0
Fax: +49 69 789 8819-99

**North American Headquarters**
**GROUP Business Software Corporation**
40 Wall Street, 33rd Floor
New York, NY 10005/USA
Phone: +1 212 995-2900
Fax: +1 212 995-2206

**Email Main Office**
**GROUP Technologies**
Ottostrasse 4
76227 Karlsruhe /Germany
Phone: +49 721 4901-0
Fax: +49 721 4901-199

**UK Office**
**GROUP Business Software Ltd.**
97 Buttermarket Street
Warrington WA1 2NL/UK
Phone: +44 1925 624950
Fax: +44 1925 240211

info@group-technologies.com
http://www.group-technologies.com


*A Division of GROUP Business Software*