White Paper

We make sure

FUJITSU COMPUTERS SIEMENS

Compliance

bei E-Mails und digitalen Dokumenten: Rechtsfragen der Archivierung und Beweisbarkeit

Ausgabe Januar 2005

Seiten 10

Inhalt

Compliance bei E-Mails und digitalen Dokumenten: Rechtsfragen der Archivierung und Beweisverwertbarkeit

Von Dr. jur. Jens Bücking*

Vorbemerkung

Unternehmer tragen eine zunehmend schwere Bürde: Nicht allein, dass steuerrelevante Dateien ggf. 10 Jahre und länger in revisionssicherer Form archiviert werden müssen. Hinzu kommt, dass die Geschäftsführung für die Sicherheit der betriebswichtigen Daten und Systeme persönlich haften kann. Eine geordnete, jederzeit verfügbare Aufbewahrung der elektronischen Geschäftspost ist aber auch aus Gründen der strategischen Rechtssicherheit unabdingbar, insbesondere um das Unternehmen für eine etwaige juristische Auseinandersetzung beweisrechtlich zu positionieren. Indessen greift die uneingeschränkte Archivierung der gesamten Kommunikation ohne geeignete betriebliche Regelungen schnell in die Rechte der Mitarbeiter ein. In diesem Spannungsfeld diametral gegenläufiger Interessen und Rechtspflichten geht der Überblick allzu leicht verloren. Das hat nicht selten die fatale Folge, dass Unternehmensführung und Belegschaft ohne erkennbare Organisation der elektronischen Geschäftsabläufe „vor sich hinwursteln“. Der Staat versteht freilich, wenn es um seine fiskalischen Interessen geht, keinen Spaß. Die Sanktionen für Verstöße gegen archivierungsrelevante Buchführungs- und Datenschutzpflichten sind erheblich. Dieser Artikel soll dem Leser einen ersten Überblick über die Rechtslage und die hieraus abzuleitenden technisch-organisatorischen Verpflichtungen geben:

Gibt es eine Rechtspflicht zu IT-Sicherheit?

In unserem Privatbereich sind wir es längst gewohnt, beispielsweise durch Alarmanlagen, Tresore, Banken und Versicherungen umfassend Vorsorge gegen den Verlust oder die Beschädigung unseres Hab und Gut zu treffen. Ganz ähnliche Sicherheitsbedürfnisse erleben wir nun im IT-Umfeld. Hier trifft den Unternehmer unter dem rechtlichen Gesichtspunkt der Schutz- und Verkehrssicherungspflichten[1] die Obliegenheit zur Bereitstellung einer dem Stand der Technik entsprechenden Infrastruktur und der dazugehörenden geeigneten Organisationsrichtlinien.

Dies betrifft namentlich den besonders schadensanfälligen Bereich der Kommunikations- und DV-Systeme, häufig die wichtigste Ressource im Unternehmen. Während die IT- und Beschaffungsabteilung hier über die erforderlichen Budgets für Firewalls, Filtersysteme (Viren, Spam, URL- und Content) und geeignete Backup- und Archivierungsmaßnahmen verfügen sollte, ist die Unternehmensführung in organisatorischer Hinsicht zu einem effizienten Risikomanagement verpflichtet[2]. Rechtssicherheit schaffen weiterhin IT-Versicherungen sowie die diversen

* Der Autor ist Gründungspartner der Rechtsanwaltskanzlei Emmert Schurer Buecking (http://www.kanzlei.de), zugleich Fachbuchautor im IT-Recht und Lehrbeauftragter an der Hochschule für Technik in Stuttgart.

1 Integrität und bestimmungsgemäße Verfügbarkeit geordneter, betriebswichtiger Daten stehen unter dem Schutz der Rechtsordnung. Im vertraglichen Bereich (insbes. Schutz von Kunden und Mitarbeitern) sind hier die §§ 311, 241 II Bürgerliches Gesetzbuch (BGB) einschlägig; außerhalb vertraglicher Bindungen gilt § 823 I BGB.

2 Spezielle Vorschriften hierüber finden sich z.B. im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG, in Kraft seit 01.05.1998), in der Anlage zu § 9 Bundesdatenschutzgesetz (BDSG), im Kreditwesengesetz (§ 25a KWG), in der neuen Baseler Eigenkapitalvereinbarung (Basel II) und in den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) Tz. 5.

Möglichkeiten der Zertifizierung und der Etablierung betrieblicher User- und Security-Policies nebst regelmäßiger Schulung der Mitarbeiter bei der Anwendung elektronischer Medien.

Bedeutsam wird das Erfordernis einer Konvergenz zwischen Technik und Recht, das uns im Fachjargon unter dem Stichwort „Compliance“[3] begegnet, insbesondere unter dem Gesichtspunkt der Haftungsentlastung. Werden die gesetzten Grenzen verletzt, haftet primär das Unternehmen für die vom Staat angeordneten Rechtsfolgen. Gegebenenfalls trifft eine solche Haftung indes auch die für das Unternehmen tätigen Organe (Vorstand, Geschäftsführung) persönlich.

IT-Risikomanagement

Ist von IT-Sicherheit die Rede, wird es zumeist um die Integrität und Vertraulichkeit von Daten gehen. Rechtspflichten, die Unternehmen insofern zu beachten haben, betreffen daher beispielsweise den sicheren Eingang und Ausgang von elektronischen Informationen (Mails, Buchungen, Bestellungen)[4] sowie die Verwahrung und den Schutz von Kunden- und Mitarbeiterdaten[5].

Über diese allgemeinen Anforderungen hinaus verlangt das Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr (KonTraG) ein effizientes Risikomanagementsystem[6], das nach einhelliger Ansicht eine Überwachung und Früherkennung sowie entsprechende Reaktionsszenarien im Schadensfall umfasst. Die Organe von Aktiengesellschaften und größeren Kapitalgesellschaften[7] trifft die Verpflichtung, geeignete Schutzmaßnahmen in Bezug auf die IT-Sicherheit ihres Unternehmens, gerade auch für betriebswichtige Systeme und Daten, zu konzipieren und umzusetzen. Im Falle des Schadenseintritts wird ihr Verschulden vermutet[8]. Besonders bemerkenswert ist, dass das KonTraG als Sanktion die persönliche Haftung der geschäftsführenden Organe zur Kompensation eines durch IT-Missmanagement hervorgerufenen Schadens beim Unternehmen vorsieht[9].

Auch die Rechtsprechung geht wie selbstverständlich von einer Rechtspflicht zu einer zeitnahen, umfassenden und zuverlässigen Datensicherung aus[10]. Versäumnisse in diesem Zusammenhang können zum Verlust des Versicherungsschutzes führen.

Speziellere Gesetze und Richtlinien für die Datensicherung ergeben sich aus dem Handelsgesetzbuch[11] und der Abgabenordnung[12] in Verbindung mit den Grundsätzen

3 „Compliance“ meint im Wesentlichen die Einhaltung der rechtsverbindlichen Mindestanforderungen in Bezug auf die Sicherheit und Verfügbarkeit von Informationen. Diese wurden in neuen Regelwerken wie den aktuellen SEC-Regeln (Sarbanes-Oxley-Act) in den USA, der neuen Baseler Eigenkapitalübereinkunft (Basel II) oder dem deutschen KonTraG weiter verschärft.

4 Die entsprechenden Rechtspflichten werden abgeleitet aus den Bestimmungen des Gewerberechts, den Anforderungen an den elektronischen Geschäftsverkehr (§ 312e BGB) sowie wiederum den allgemeinen Schutz- und Sorgfaltspflichten der §§ 823 I bzw. 311, 241 II BGB.

5 Schutzvorschriften finden sich hier in einer Vielzahl von Vorschriften, so etwa dem BDSG (dort z.B. die §§ 5, 7, 8, 43, 44 und die Anlage zu § 9,) § 89 KG, § 17 UWG sowie die im Strafgesetzbuch die §§ 202, 202a, 203 bis 206 StGB.

6 Vgl. dazu die verschärften Anforderungen an den Lagebericht, §§ 289, 264 HGB, sowie § 91 II Aktiengesetz (AktG).

7 Siehe § 267 I HGB zu den Größenklassen.

8 § 93 II AktG.

9 § 93 II bis V AktG.

10 Oberlandesgericht Hamm, Urteil vom 01.12.2003, 13 U 133/03.

11 §§ 257, 239 IV HGB.

12 §§ 146 V, 147 AO.

ordnungsgemäßer DV-gestützter Buchführungssysteme (GOBS von 1995)[13] und den Grundsätzen zum Datenzugriff und zur Prüfbarkeit originär digitaler Unterlagen (GDPdU von 2002)[14], die von allen Buchungspflichtigen zu beachten sind.

Die genannten Rechtspflichten betreffen somit die sichere Informationsverbreitung und Informationsaufbewahrung. Stets geht es um sensible Information in Datenform und ihre Verfügbarkeit in bestimmter Form für eine bestimmte Dauer, kurz – und um abermals im Jargon zu bleiben – um „Information Lifecycle Management“. Gehaftet wird hier unter anderem für die technisch und rechtlich sichere Aufbewahrung und die jederzeitige Integrität und Verfügbarkeit solcher Daten. Die Haftungsfolge tritt ein bei Fehlen oder Ungeeignetheit eines auf ihren Schutz, notfalls auf ihre Wiederherstellung gerichteten Konzepts.

Fokus rechtssichere E-Mail-Archivierung

Die im Rahmen der IT-Sicherheit geforderte Datensicherung betrifft insbesondere auch E-Mails. Deren Rechtsnatur kann vielfältig sein:

E-Mails als rechtsrelevante elektronische Erklärungen

Zum einen kann es sich um elektronische Erklärungen handeln, weshalb es im Geschäftsverkehr erforderlich ist, täglich seine Accounts zu überprüfen[15]. Denn bereits der Zugang, d.h. die Abrufbarkeit vom Mailserver, kann auf Seiten des unternehmerisch tätigen Empfängers (bzw. seiner Mitarbeiter) Rechtsfolgen auslösen, ohne dass es der tatsächlichen Kenntnisnahme vom Inhalt der E-Mail bedarf[16]. Vorsicht ist daher geboten bei der Verwendung von Mailadressen auf Visitenkarten, im Internet oder auf Geschäftsbriefen. Geht etwa eine elektronische Rechnung[17] oder Mahnung zu, werden hierdurch bereits Zahlungs- bzw. Verzugsfolgen ausgelöst. Und im Handelsverkehr zwischen Kaufleuten gilt, dass der Vertragspartner auf ein ihm unterbreitetes Angebot unverzüglich mit einem so genannten kaufmännischen Bestätigungsschreiben reagieren, also ggf. widersprechen muss. Tut er dies nicht, muss er sich an dem vom Vertragspartner bestätigten Vertragsinhalt festhalten lassen, auch wenn er von ganz anderen Abmachungen ausgegangen war. Sein Schweigen gilt hier kraft Handelsbrauchs als Zustimmung[18]. Wer also bei seinem geschäftlichen Auftritt eine Erreichbarkeit über seine geschäftliche Mailadresse suggeriert, muss auch für die tägliche Kontrolle dieser Mailbox sorgen.

13 http://www.bundesfinanzministerium.de/Anlage1408/GoBS.pdf

14 http://www.bundesfinanzministerium.de/Anlage8440/BMF-Schreiben-vom-16.07.01.pdf

15 Dieses Erfordernis ergibt sich u.a. aus der Telefax-Rechtsprechung des Bundesgerichtshofs: Mit der Kenntnisnahme einer via Fax übermittelten Erklärung ist stets während der Geschäftsstunden zu rechnen. Beim Faxempfänger besteht eine entsprechende Überprüfungspflicht in Bezug auf Faxeingänge (vgl. Urteil vom 21.01.2004, Az. XII ZR 214/00).

16 § 312e I 2 BGB.

17 § 14 III Umsatzsteuergesetz (UStG).

18 §§ 346, 362 HGB.

E-Mails als Beweismittel bei der Dokumentation betriebswichtiger Vorgänge

Über die vertragliche Komponente hinaus ist die E-Mail zum anderen aber insbesondere auch Gegenstand notwendiger (oder zumindest kaufmännisch gebotener) Dokumentation. Gerade am Beispiel der E-Mail zeigt sich besonders deutlich das Interesse des Unternehmens, zu seiner eigenen Rechtssicherheit und beweisrechtlichen Positionierung so viele Informationen wie möglich zu sammeln, abzuspeichern, auszuwerten und für die Zukunft verfügbar zu halten. Dies beinhaltet häufig den Wunsch, bis zur Auslastungsgrenze der Speicherkapazität sämtliche Geschäftskorrespondenz automatisiert zu erfassen und über einen längeren Zeitraum zu sichern. Denn in einem Prozess muss jede Partei die ihr günstigen Tatsachen darlegen und beweisen. Und wenngleich die E-Mail im Grundsatz keinen höheren Beweiswert hat als beispielsweise ein Ausdruck aus dem Internet, die Kopie eines Papierdokuments oder die Vorlage einer Fotografie (etwas anderes gilt nur für E-Mails, die mit einer qualifizierten elektronischen Signatur nach Signaturgesetz versehen sind)[19] und daher als Gegenstand der freien Beweiswürdigung[20] nur dem Augenschein des Gerichts unterliegt, bietet sie jedoch in der Regel einen beweisrechtlichen „Wettbewerbsvorteil“. Denn der Ausdruck einer E-Mail ist häufig das einzige Beweismittel, das dem Gericht zu seiner Entscheidungsfindung vorliegt. Sie schafft mithin Indizien für den Aussteller, den Empfänger, das Absende- und Zugangsdatum und die Richtigkeit des in ihr niedergelegten Inhalts. Darüber hinaus kann sie eine wertvolle Gedächtnishilfe für die Zeugenvernehmung bilden. Die jeweils andere Partei, die sich gegen den mit der E-Mail begründeten Sachverhalt wehren will, ist wegen ihrer prozessualen Wahrheitspflicht[21] daran gehindert, die in der E-Mail dokumentierten Angaben pauschal zu bestreiten. Einwände, die Mail stamme nicht vom Aussteller, sei beim Empfänger nicht zugegangen, enthalte falsche Datumsangaben oder sei inhaltlich verfälscht worden, wären daher von der dies einwendenden Partei genauestens zu substantiieren.

Grenzen der Dokumentation: E-Mails und Mitarbeiterschutz

Die Maximalschwelle solcher Vorsorge bildet hier, wie eingangs angedeutet, jedoch das Datenschutzrecht und das Fernmeldegeheimnis der Mitarbeiter[22]. So gilt bei erlaubter oder geduldeter Privatmail im Grundsatz, dass ohne die Zustimmung der Mitarbeiter oder ihrer Vertretung (Betriebsrat/Personalrat) eine Überwachung der Inhalte der Kommunikation unzulässig ist. Wichtig ist ferner, dass private Mail dem Mitarbeiter gehört und von ihm herausverlangt werden kann, dies prinzipiell auch nach seinem Ausscheiden. Auch ist es problematisch, Privatmail durch Spamfilter zu unterdrücken oder gar zu löschen[23]. Zur Überwindung dieser Interessenkonflikte sind rechtlich-organisatorische Maßnahmen letztlich unabdingbar. Gemeint sind individualvertragliche Vereinbarungen mit dem Arbeitnehmer, Betriebsvereinbarungen, Security- und User-Policies sowie fortwährende Schulungs- und Qualifizierungsmaßnahmen der Belegschaft.

19 Die „elektronische Form“ ist 2001 der Schriftform gleichgestellt. Seitdem sind bspw. Verträge via E-Mail, sofern sie mit einer qualifizierten elektronischen Signatur (§ 2 Nr. 3 des Signaturgesetzes) versehen sind, rechtswirksam. Parallel dazu normiert der neue § 292a der Zivilprozessordnung einen Anscheinsbeweis für die Echtheit solcher Erklärungen , und § 130a ZPO eröffnet den prozessualen Rahmen für die Zulässigkeit und Verwertbarkeit elektronischer Dokumente.

20 § 286 ZPO.

21 § 138 I ZPO.

22 § 206 StGB, § 85 TKG.

23 Strafbar ggf. nach § 206 II StGB.

E-Mails als Gegenstand der gesetzlich zwingenden Dokumentation von Geschäftsvorfällen

Wenig verbreitet ist die Erkenntnis, dass Unternehmen nach handelsrechtlichen und steuerrechtlichen Grundsätzen verpflichtet sind, ihre Geschäftskorrespondenz („Handels- oder Geschäftsbriefe“) aufzubewahren. Dies betrifft Unterlagen, die für die Übersicht über einen bestimmten Geschäftsvorfall (im Sinne von Vorbereitung, Durchführung, Rückgängigmachung) bedeutsam sein können, gleichgültig in welcher Form (Briefe, Telefaxe, E-Mails) diese vorliegen. Gemeint sind also bspw. Aufträge und deren Bestätigung, Lieferpapiere, Rechnungen und Rechnungskopien, Reklamationen samt dazugehöriger Stellungnahmen, Gutschriften und Zahlungsbelege, Kontoauszüge, Bescheide über Steuern oder Gebühren, Kassenunterlagen, Produkt- und Preislisten (inkl. entsprechender Rundmailings zur Kundeninformation), Verträge, Gehaltsunterlagen etc. Hintergrund dieser weit reichenden Verpflichtung sind die Erfordernisse der Transparenz und Revisionssicherheit, d.h. die Archivierung aller Belege und Dokumente, die für eine betriebliche Überprüfung Bedeutung, aber auch vor den ordentlichen Gerichten Bedeutung erlangen können[24].

Zulässige Archivierungsformen

Nach den Bestimmungen des Handels- und Steuerrechts[25] können die empfangenen und abgesandten Geschäfts- und Handelsbriefe und die Buchungsbelege auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsgemäßer Buchführung (GOBS) entspricht und sichergestellt ist,

- dass die Wiedergabe oder die Daten mit den empfangenen Handelsbriefen und den Buchungsbelegen *bildlich* und mit den anderen Unterlagen *inhaltlich* übereinstimmen, wenn sie lesbar gemacht werden,
- dass sie während der Dauer der Aufbewahrungsfrist verfügbar sind,
- und dass sie jederzeit innerhalb angemessener Frist lesbar gemacht und für die Besteuerung maschinell ausgewertet werden können.

Handels und Steuerrecht verlangen vom Unternehmer mithin Transparenz sowie Revisions- und Datensicherheit. Die GOBS bilden dabei den Regelungsrahmen für die handelsrechtlichen Grundsätze der Ordnung, Nachvollziehbarkeit und Fälschungssicherheit, während die im Zuge der Abgabenordnungsänderung entstandenen GDPdU diese Grundsätze letztlich auf alle originär hergestellten digitalen Unterlagen von steuerrechtlicher Relevanz erstrecken.

Neben geeigneten Sicherheitsvorkehrungen gegen die unberechtigte Kenntnisnahme, Unauffindbarkeit, Vernichtung und den Diebstahl von gesicherten Programmen und Datenbeständen stellen GOBS und GDPdU insbesondere Vorschriften für die Archivierung digitaler Dokumente und für den Zugriff auf diese Dokumente im Rahmen von Betriebsprüfungen auf. Gewährleistet muss dabei die Prüfbarkeit und Belegbarkeit sämtlicher Geschäftsvorfälle sein, die Nachvollziehbarkeit etwaiger Stornierungen und Änderungen, die Datensicherheit, die interne Kontrolle und die Einhaltung der gesetzeskonformen Aufbewahrungsfristen. Notwendig ist ferner

24 Gemäß § 258 HGB kann im Laufe eines Rechtsstreits das Gericht auf Antrag oder von Amts wegen die Vorlegung der Handelsbücher einer Partei anordnen.

25 Siehe §§ 257, 239 HGB und §§ 146, 147 AO.

eine umfassende Verfahrensdokumentation in Ansehung dieser Abläufe, die nachvollziehbar beschreibt, wie die relevanten Informationen angelegt, geordnet, gespeichert, indiziert und geschützt wurden und später wieder gefunden und verlustfrei reproduziert werden können[26]. Die archivierten Daten müssen in wiedergabefähiger, maschinell lesbarer und auswertbarer Form zur Verfügung gestellt werden können. Ihre periodengerechte Auswertung durch die jeweils aktuelle Prüfsoftware der Finanzverwaltung muss gewährleistet sein. Der Steuerpflichtige ist insoweit zur Kooperation verpflichtet[27]. Bei der Archivierung von E-Mails ist außerdem darauf zu achten, dass auch die Attachements und - im Falle der Signierung und Verschlüsselung - auch die verschlüsselten und entschlüsselten Dokumente nebst Schlüsseln mit aufbewahrt werden.

Betroffen sind zum einen alle steuerrelevanten Unterlagen, also sämtliche Informationen, die für eine steuerliche Veranlagung im Sinne von Entstehen, Entfallen oder Minderung einer Steuerlast Bedeutung erlangen können. Andererseits geht es bei den Aufbewahrungspflichten freilich - wie bereits dargestellt - nicht allein um die im engeren Sinne steuerrelevanten Unterlagen. Gemeint sind darüber hinaus die nach Handelsrecht aufbewahrungspflichtige „bloße“ Geschäftskorrespondenz und die einschlägigen Organisationsunterlagen des Unternehmens (beispielsweise Gründungsprotokolle, Prüfberichte, Aufsichtsratsbeschlüsse, ferner aber auch die Arbeitsverträge, Lohn- und Sozialversicherungsunterlagen der Arbeitnehmer oder die im laufenden Geschäftsbetrieb abgeschlossene Verträge mit der in diesem Zusammenhang angefallenen Korrespondenz, gleichgültig in welcher Form)[28].

Die Problematik der Archivierungsfristen

Rechnungen[29] und andere Buchungsbelege, bestimmte Zollunterlagen und Handelsbücher nebst aller Aufzeichnungen[30] sind zehn Jahre, die sonstigen handels- und steuerrechtlich relevanten Unterlagen (Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind) sechs Jahre aufzubewahren[31].

Eine Abgrenzung der Handels- oder Geschäftsbriefe und sonstigen steuerrelevanten Unterlagen (Archivierung über mindestens 6 Jahre) insbesondere zu den Buchungsbelegen, für die eine wenigstens zehnjährige Aufbewahrungsfrist besteht, ist im automatisierten Verfahren jedoch kaum möglich. Und auch eine qualifizierte individuelle Prüfung, wird sie nicht fachmännisch durch den Steuerberater oder Wirtschaftsprüfer vorgenommen, wird mit erheblicher Rechtsunsicherheit behaftet bleiben. Aus praktischen Erwägungen heraus empfiehlt sich daher, eine entsprechende Einteilung in „steuerrelevante belegartige“ und „übrige“ Handels- oder Geschäftsbriefe nicht vorzunehmen, sondern generell von der strengeren zehnjährigen Aufbewahrungsfrist auszugehen. Alles andere wäre mit einem organisatorisch unangemessenen Mehraufwand und mit der erheblichen Gefahr von Irrtümern verbunden.

26 Es besteht also eine Indexierungspflicht. Der Erhalt der Verknüpfung zwischen Index, digitalem Dokument und Datenträger muss während der gesamten Aufbewahrungsfrist gewährleistet sein.

27 Nach § 200 I AO 200 hat der Steuerpflichtige u.a. Aufzeichnungen, Bücher, Geschäftspapiere und andere Urkunden zur Einsicht und Prüfung vorzulegen. Dies gilt unabhängig von der Aufbewahrungsform (elektronisch, Papier).

28 § 147 I Nr. 5 AO.

29 § 14b I UStG.

30 So auch Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zum Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen.

31 § 147 III AO, § 257 IV HGB.

Gerade bei E-Mails kann aber die Grenze zu den steuerrelevanten Buchhaltungsunterlagen in den Fällen, in denen der E-Mail zugleich Belegfunktion zukommen kann, weil sie nicht nur als Informationsträger sondern beispielsweise auch zur Fakturierung oder zur Auftragsabwicklung eingesetzt wird, fließend sein, so dass im Zweifel auch alle elektronisch archivierten Maildokumente in revisionssicherer Form über die Zehnjahresfrist verfügbar gehalten werden sollten.

Wichtig bei der Berechnung der sechs- bzw. zehnjährigen Aufbewahrungsfrist ist, dass der Fristenlauf erst mit dem Ende des Kalenderjahres beginnt, in welches der betreffende Geschäftsvorfall fällt. Es ist also danach zu fragen, wann der Buchungsbeleg entstanden ist bzw. wann die geschäftsrelevante E-Mail gesendet oder empfangen wurde. Eine Verlängerung durch offene Veranlagungszeiträume, für die noch kein bestandskräftiger Steuerbescheid vorliegt, ist möglich und daher vom Unternehmen bei der Berechnung seiner Aufbewahrungsfristen gleichfalls zu berücksichtigen[32]. Daraus kann sich im Einzelfall eine deutliche Erstreckung der Aufbewahrungsfristen um mehrere Jahre ergeben.

Folgen einer Verletzung der Archivierungspflicht

Werden jedoch, wie in der Praxis häufig anzutreffen, die Ordner und Mailboxen in regelmäßigen Abständen „auf eigene Faust“ analysiert, Altbestände in Archivordner verschoben und Mails, die für überholt (und daher nicht mehr geschäftsrelevant) gehalten werden, gelöscht, steht dies häufig im Gegensatz zu den oben genannten Vorschriften. Verstöße sind mit Zwangsmaßnahmen, Schätzung, straf- und bußgeldrechtlicher Ahndung und der Versagung gesetzlicher Steuervergünstigungen sanktioniert.

Die Verletzung der Aufbewahrungspflichten kann aber auch Folgen haben, die über die Besteuerung weit hinausgehen. Wenn beispielsweise der Verlust oder die Unauffindbarkeit einer E-Mail den Finanzbehörden eine vollständige und lückenlose Übersicht über die Vermögensverhältnisse des Unternehmens (und damit zusammenhängende Geschäftsvorfälle) erschwert, ist eine Haftung des Unternehmens und seiner Organe nicht ausgeschlossen. So wird etwa wegen Verletzung der Buchführungspflicht mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft, wer Handelsbücher oder sonstige Unterlagen, zu deren Aufbewahrung er nach Handelsrecht verpflichtet ist, vor Ablauf der Aufbewahrungsfrist beiseite schafft, verheimlicht, zerstört oder beschädigt und dadurch die Übersicht über seinen Vermögensstand erschwert[33]. Vergleichbare Sachverhalte können mit Freiheitsstrafe von jeweils bis zu fünf Jahren oder mit Geldstrafen verfolgt werden, wenn Buchführungsunterlagen vernichtet, beschädigt oder vorenthalten werden (Urkundenunterdrückung)[34] oder die Finanzbehörden pflichtwidrig über steuerlich erhebliche Tatsachen in Unkenntnis gelassen und dadurch Steuern verkürzt oder nicht gerechtfertigte Steuervorteile erlangt werden (oder Steuerhinterziehung)[35]; die leichtfertige Steuerverkürzung ist immerhin noch mit Ordnungsgeldbußen bis zu 50.000 Euro sanktioniert.

32 § 257 V HGB, § 147 III, IV AO.

33 § 283b StGB.

34 § 274 StGB.

35 § 370 AO.

Fazit

Backup und Archivierung sind aus dem Unternehmensalltag nicht mehr wegzudenken. Welche Bestimmungen dabei in Bezug auf geschäftliche Mails zu beachten sind, war Gegenstand dieses Artikels. Diese Bestimmungen rechts- und revisionssicher umzusetzen und praktikabel in den Arbeitsalltag einzubinden, gehört zu den Herausforderungen des Unternehmens. Die Wahl des Archivsystems und die Komplexität der betrieblichen Umsetzungsorganisation müssen dem Wert der Information gerecht werden. Aus Unternehmersicht essentiell ist dabei jedoch nicht allein die Erfüllung gesetzlicher Vorgaben in Bezug auf die Aufbewahrung handels- und steuerrechtlich relevanter Daten. Dies ist nur ein Aspekt des Wertes von Information. Ebenso wichtig ist die vollständige Dokumentation von Geschäftsvorgängen unter den Gesichtspunkten der Beweisrelevanz und des unternehmensinternen Informationsmanagements. Leistungsfähige und revisionssichere Archivsysteme zeigen ihre besondere Effizienz daher vor allem dann, wenn sie nicht allein kaufmännisch sondern zur Speicherung und Dokumentation sämtlicher elektronischen Informationen eines Unternehmens eingesetzt werden.

Maßgeschneiderte Komponenten für eine E-Mail Infrastrukturlösung
easyXchange von Fujitsu Siemens Computers

easyXchange ist eine Komplettlösung, die aus Servern, Speichersystemen, Software und Services für die Konsolidierung von Mail-Servern und Speicherumgebungen in Unternehmen besteht. Sie verfügt über Schlüsselkomponenten für die Applikationsverfügbarkeit, Datenverfügbarkeit und umfassendes Lifecycle-Management für die Archivierung von E-Mails und Anhängen. *easyXchange* stellt Funktionen bereit, die Unternehmen helfen, gesetzliche Anforderungen der E-Mail Aufbewahrung zu erfüllen.

easyXchange Backup – zuverlässig und einfach

Mit Ausfallsicherungssystemen, Snapshot-Zwischenspeicherlösungen und kürzeren Wiederherstellungszeiten wird verhindert, dass E-Mail Datensicherung zu einer Schwachstelle im Arbeitsablauf wird. Inhalte einzelner Mailboxen oder ganze Datenbanken lassen sich wiederherstellen, ohne das der Betrieb unterbrochen werden muss. Eine Reihe von Mechanismen sorgen dafür, E-Mails vor Zerstörung/Löschung durch Hardware-, Software- oder Bedienungsfehler zu schützen.

easyXchange Lebenszyklus-Management – mehr als nur Archivierung

Mit speziellen Prüf- und Kontrollfunktionen wird für eine automatisierte Lösung im Umfeld des E-Mail Lebenszyklus-Managements gesorgt. Unternehmen werden damit bei ihren Archivierungspflichten unterstützt, ohne das dies eine komplizierte Implementierung voraussetzt. Zugriff mit hoher Effizienz, auch auf ältere E-Mails, wird duch Volltextsuche gewährleistet. Ergänzend steht eine hierarchische Speicher-Management-Software (HSM) zur Verfügung, die E-Mail Daten automatisch auf preiswertere Speicherebenen verschiebt.

easyXchange – mit weniger mehr erreichen

easyXchange von Fujitsu Siemens Computers ist eine umfassende, vorgestestete Infrastrukturlösung für Mailserver- und Speicherkonsolidierungsprojekte. Dank der modularen Struktur (Bausteinkonzept) kann die Konfiguration an die individuellen Bedürfnisse der Kunden angepasst werden. Die Implementierung lässt sich auch stufenweise vornehmen oder einzelne easyXchange Bausteine in der vorhandene IT-Architektur jederzeit ergänzen.

easyXchange stellt die Verfügbarkeit der Applikation sicher, verbessert die Leistung, reduziert Kosten und Komplexität und stellt Funktionen bereit, die Unternehmen helfen, gesetzliche Anforderungen der Archivierung zu erfüllen. Kurz: Mail-Infrastruktur der nächsten Generation.

Herausgegeben durch:

Jürgen Heidegger
Telefon: +49 89 636 42535
Fax: +49 89 636 46349
Juergen.Heidegger@fujitsu-siemens.com
http://www.fujitsu-siemens.com/easyXchange

Extranet:

http://extranet.fujitsu-siemens.com/easyXchange