

1. Das Auge des Gesetzes

Der zunehmenden Digitalisierung, gerade auch des unternehmerischen Schriftverkehrs Rechnung tragend, sind in den letzten Jahren durch den Bundesgesetzgeber vermehrt gesetzliche Regelungen in Kraft gesetzt worden, um traditionellen unternehmerischen Pflichten des Handels- und Steuerrechts auch im digitalen Zeitalter Geltung zu verschaffen.

Die Anforderungen:

International:

Hier gibt es die diversen Anforderungen für international aufgestellte Unternehmen.

National:

HGB = Handelsgesetzbuch

Hierin werden die grundsätzlichen Rahmenbedingungen definiert:

§§ 238, 239, 257, 258, 259, 261

AO = Abgabenordnung

Die AO konkretisiert und ergänzt das HGB.

§§ 145, 146, 147, 158

Das Problem: der individuelle Nachweis, dass die Vorschriften erfüllt werden, obliegt jeder einzelnen Buchführung

GoB / GoBS = Grundsätze ordnungsgemäßer Buchführung

Ergänzung zu HGB und zu AO.

GoB / GoBS ist Anwendungs- und Medienneutral und regelt die Verwendung elektronischer Dokumente (z. B. Verfahrensdokumentation)

GDPdU = Gesetz zur Durchführung der Prüfung von digitalen Unterlagen

Zugriff der Finanzbehörden auf digitale Daten und Unterlagen.

UStG = Umsatzsteuergesetz

SigG = Signaturgesetz

Die elektronische Signatur übernimmt die Rolle der handschriftlichen Unterschrift im elektronischen Geschäftsverkehr.

Prod.HaftG = Produkthaftungsgesetz

Ist es streitig, ob die Ersatzpflicht ausgeschlossen ist, trägt der Hersteller die Beweislast. Beweislastumkehr ist Bestandteil der EG-Produkthaftung.

Der Anspruch erlöscht nach 10 Jahren + Einspruchsfristen.

BDSG = Bundesdatenschutzgesetz

Wichtig u. a. bei E-Mail-Verkehr

ZPO = Zivilprozessordnung

KonTraG = Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Aus der Erkenntnis von KonTraG und Basel II besteht auch die Verpflichtung der Geschäftsführung zu einem effektiven Risikomanagementsystem (inkl. der Verfügbarkeit betriebswichtiger Informationen).

1.1 GoB und GoBS

Die GoBS (Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme) transformieren die handelsrechtlichen Grundsätze ordnungsgemäßer Buchführung (GoB, § 257 HGB) auf den Bereich der DV-gestützten Buchführung.

Insbesondere vor dem Hintergrund gesetzlicher Aufbewahrungsfristen (6-10 Jahre) muss bei Speicherung auf Datenträgern für die Dauer der gesamten Aufbewahrungszeit die Gewähr für die Unveränderlichkeit und Manipulationssicherheit des gesamten Verarbeitungs- und Archivierungsprozesses gegeben sein.

Im Einzelnen müssen beispielsweise alle in den Verarbeitungsprozess eingeführten Informationen vollständig und ordnungsgemäß erfasst, vor Veränderungen oder Fälschung geschützt, sowie gegen unberechtigte Nutzung gesichert werden.

Zugleich müssen die solchermaßen abgelegten Daten für die Dauer der gesetzlichen Aufbewahrungsfrist jederzeit verfügbar und innerhalb angemessener Frist (bei zwischenzeitlich erfolgtem Systemwechsel auch

auf Kosten des Aufbewahrungspflichtigen) unverzüglich lesbar gemacht werden können.

Die GoBS verpflichten den Anwender zur Erstellung einer umfangreichen Verfahrensdokumentation (Tz. 6 der GoBS), aus der sich einerseits die Sicherstellung der gesetzlichen Vorgaben und andererseits auch der Nachvollzug und die Prüfbarkeit der angewandten Verfahren und Funktionalitäten für einen sachverständigen Dritten in angemessener Zeit erschließen lassen. Eine ausführliche Beschreibung der gesetzlichen Anforderungen an die Verfahrensdokumentation siehe 1.3.

1.2 GDPdU

Seit dem 01.01.2002 sind die Finanzverwaltungen durch Änderungen der Abgabenordnung gesetzlich ermächtigt, die mit Hilfe eines DV-Systems erzeugten, empfangenen und in die Datenverarbeitung eingeflossenen steuerrelevanten Daten und Dokumente durch Datenzugriff beim Steuerpflichtigen zu prüfen.

Hierbei steht es im Ermessen des Steuerprüfers, ob er

Z 1 unmittelbarer Zugriff

unter Nutzung der unternehmenseigenen Hard- und Software unmittelbar auf die Daten des Steuerpflichtigen zugreift und selber Auswertungen vornimmt,

Z 2 mittelbarer Zugriff

die Auswertung durch unternehmenseigenes Personal nach seinen Anweisungen durchführen lässt oder

Z 3 Datenträgerüberlassung

sich die gespeicherten Unterlagen und Aufzeichnungen in maschinell auswertbarer Form auf einem Datenträger zur Verfügung stellen lässt. Die Analyse erfolgt dann mit der Prüfsoftware IDEA der Finanzverwaltung. Akzeptiert als Datenträger werden CD-ROMs und DVD im ISO Standard, oder aber Disketten sofern diese das Dateisystem MS-DOS oder FAT enthalten.

Für empfangene und im eigenen DV-System erzeugte steuerrelevante Daten und Dokumente gelten (vor dem Hintergrund steuerrechtlicher Aufbewahrungsfristen von ebenfalls 6-10 Jahren) grundsätzlich die gleichen Anforderungen, wie nach GoBS, einschließlich des Erfordernisses zur Erstellung einer Verfahrensdokumentation.

Darüber hinaus müssen die abgespeicherten steuerrelevanten Daten und Dokumente maschinell ausgewertet werden können. Das bedeutet, der Prüfer hat Anspruch auf (Mit)Überlassung der gleichen Auswertungsfunktionalitäten, wie sie den jeweiligen Anwendungen zur Verfügung stehen, innerhalb derer die Daten entstanden sind.

Diejenigen Dokumente und Unterlagen, die in elektronischer Form in das DV-System eingeführt wurden oder in diesem entstanden sind, sind in ihrer originären digitalen Form aufzubewahren,

z.B. Ausgangsrechnungen, Excel – Tabellen oder Faxe.

Excel ist ein Problemfeld, da selbst dann, wenn beispielsweise eine Spesenabrechnung eines Außendienstmitarbeiters nur in Form eines E-Mail – Anhangs eingeht oder eine Angebotskalkulation als E-Mail-Anhang, so muss diese elektronisch vorgelegt werden.

Bei einem Systemwechsel ist eine den Auswertungsfunktionalitäten des Ursprungssystems qualitativ und quantitativ entsprechende maschinelle Auswertbarkeit zu gewährleisten oder die zur Erstellung verwendete Hard- und Software für die Dauer der Aufbewahrungszeit (auf Kosten des Steuerpflichtigen) funktionsfähig vorzuhalten.

Da bereits ein entfernter, lockerer Zusammenhang mit betrieblichen Interessen genügt, um kaufmännische Korrespondenz zum Handelsbrief zu qualifizieren, und steuerrechtliche Aufbewahrungspflichten bereits ausgelöst werden, sobald Unterlagen allgemein für die Besteuerung bedeutsam sind, ist zu beachten, dass auch E-Mails per Definition aufbewahrungspflichtig in der von GoBS und GDPdU geforderten Form sein können.

Verstöße gegen gesetzliche Aufbewahrungsvorschriften können dazu führen, der Buchführung insgesamt ihre Ordnungsmäßigkeit zuzunehmen und können Sanktionen verschiedenster Intensität, vom Bußgeld, über Steuerschätzung, bis hin zum Vorwurf der Steuerhinterziehung oder der Verletzung anderer strafrechtlicher Vorschriften auslösen.

Zusammengefasst:

„Originär digitale Unterlagen .. sind auf maschinell verwertbaren Datenträgern zu archivieren“

Originär digitale Unterlagen sind:

in die Systeme digital eingehende Daten und
in den Systemen digital erstellte Daten.

Maschinell verwertbarer Datenträger:

muss maschinell lesbar und
muss maschinell auswertbar sein.

Für die Prüfung verwenden die Betriebsprüfer

IDEA (Interactive Data Extraction and Analysis)

Als offizielle Prüfsoftware des Bundesministeriums der Finanzen (BMF) ist IDEA spezialisiert auf die zuverlässige Prüfung von Datenbeständen nahezu beliebiger Größe aus unterschiedlichen Quellen.

1.3 Verfahrensdokumentation

Das Führen einer Verfahrensdokumentation ist konsequenterweise bei DV-gestützter Buchführung Pflicht seit 1995 und in den GoBS unter Tz.6 hinsichtlich seiner Anforderungen umfassend beschrieben.

Sie dient dem Nachweis der ordnungsgemäßen Umsetzung der gesetzlichen Vorgaben von GoBS und GDPdU und muss so gestaltet sein, dass sie einem sachverständigen Dritten sowohl die Überprüfung der Buchführung (hinsicht-

lich ihrer **formellen** und **sachlichen Richtigkeit**), als auch die Überprüfung interner Kontrollsysteme (vor dem Hintergrund der Sicherheit des Gesamtverfahrens) in angemessener Zeit ermöglicht.

Dies bezieht sich sowohl auf die Prüfbarkeit einzelner Geschäftsvorfälle, als auch auf die Prüfbarkeit des gesamten Abrechnungsverfahrens (Verfahrens- oder Systemprüfung).

Wie die erforderliche Verfahrensdokumentation formal gestaltet und technisch durchgeführt wird, kann das Unternehmen individuell entscheiden. Es gilt jedoch, dass die jeweilige Verfahrensdokumentation für einen sachverständigen Dritten verständlich sein muss.

Die Verfahrensdokumentation muss insbesondere beinhalten:

- Die Beschreibung der sachlogischen Lösung, d.h. die Darstellung der fachlichen Aufgabe aus Sicht des Anwenders;
- die Beschreibung der programmtechnischen Lösung, d.h. wo und wie die sachlogischen Lösungen in Programmen umgesetzt sind;
- eine Beschreibung, wie die Programm-Identität gewahrt wird, d.h. der Nachweis, dass die sachlogischen Forderungen durch die eingesetzten Programme erbracht werden;
- Beschreibung, wie die Integrität von Daten gewahrt wird, d.h. eine Beschreibung der Vorkehrungen, durch die erreicht wird, dass Daten und Programme nicht durch Unbefugte geändert werden können, sowie
- schriftlich fixierte Arbeitsanweisungen für den Anwender zur sachgerechten Erledigung und Durchführung seiner Aufgaben unter Berücksichtigung der Schnittstellen zu vor- und nachgelagerten Systemen.

Die Anforderungen an die Verfahrensdokumentation sind unabhängig von der Größe | Kapazität der genutzten DV-Anlage, gelten also gleichermaßen für Großrechnersysteme, wie auch für PC-Systeme.

Im Gegenzug eröffnet das Vorhandensein einer Verfahrensdokumentation dann u. U. jedoch auch Argumentationspotenziale hinsichtlich eines vorhandenen Sicherheitsmanagements, relevant für die Haftung nach dem KonTraG, bzw. für das Rating nach Basel II.

Wichtige Kriterien:

- Ordnungsmäßigkeit
- Vollständigkeit
- Sicherheit des Gesamtverfahrens
- Schutz vor Veränderung und Verfälschung
- Sicherung vor Verlust
- Nutzung nur durch Berechtigte
- Einhaltung der Aufbewahrungsfristen
- Dokumentation des Verfahrens
- Nachvollziehbarkeit
- Prüfbarkeit

1.4 Risikomanagement

Aus der Erkenntnis von KonTraG und Basel II heraus, besteht die Verpflichtung zu einem effektiven Risikomanagement

- Risikomanagementsystem (inkl. Verfügbarkeit betriebswichtiger Informationen)
- Verschuldensvermutung und persönliche Haftung des Managements
- Risikomanagement als zentraler Bestandteil aller neuen nationalen und internationalen Compliance-Gesetze, u.a. BDSG, GoBS, Basel II
- Risikomanagement auch als zentraler Bestandteil der allgemeinen kaufmännischen Sorgfaltspflichten.

1.5 revisionssichere Archivierung

Revisionssicherheit kann man nicht kaufen, das muss man machen!

Der Begriff Revisionssicherheit findet sich nicht in Gesetzestexten, nicht in Schreiben des BMF (Bundesfinanzministerium), nicht in der GoBS, noch wird der Begriff vom IDW (Institut der deutschen Wirtschaftsprüfer) offiziell verwendet.

Revisionssicherheit ist ein Schlagwort der Anbieter, unter dem unterschiedliche handels- und steuerrechtliche Aufbewahrungsvorschriften subsumiert werden.

Revisionssicherheit beschreibt die ganzheitliche Funktionalität eines ERP und / oder Dokumenten Management Systems (DMS) bezüglich der

- Technik
- Organisation
- Dokumentation

Hier noch einmal der Hinweis auf die Verfahrensdokumentation:

GoB § 6.2.2:

Die Beschreibung der programmtechnischen Lösung hat zu zeigen, wo und wie die sachlogischen Forderungen in Programmen umgesetzt sind.
Wichtig: Dokumentation und Prüfbarkeit

Die Praxis: 10 Regeln des VOI

1. Jedes Dokument muss unveränderbar archiviert werden.
 - Verfahren technisch und organisatorisch nachvollziehbar machen.
2. Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv verloren gehen.
 - Hier besteht die Nachweispflicht. Dokumentation!
3. Jedes Dokument muss mit geeigneten Retrievaltechniken wieder auffindbar sein.
 - Auswirkung auf die Verschlagwortung.
4. Es muss genau das Dokument wieder gefunden werden, das gesucht worden ist.
 - Eindeutigkeit der Verschlagwortung.

5. Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
 - Auswirkung auf das Löschkonzept und auf die Medien auch bei langen Aufbewahrungszeiten.
6. Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.
 - Inhaltliche und optische Übereinstimmung. Farbe kann zum Informationsträger werden.
7. Jedes Dokument muss zeitnah wieder gefunden werden können.
 - Relativer Begriff. Bei Prüfungen > sofort
8. Alle die Veränderungen in der Organisation und Struktur ziehen unter Umständen Veränderungen im Archiv nach sich.
 - Benötigt wird hier ein Protokoll, dass die Wiederherstellung des ursprünglichen Zustandes erlaubt.
9. Archive müssen auf neue Plattformen migrierbar sein.
 - Software, Medien und Komponenten müssen ohne Informationsverlust migrierbar sein.
10. Das System muss die Möglichkeit bieten, die gesetzlichen Anforderungen (BDSG; HGB; AO etc.) und die betrieblichen Anforderungen des Kunden bezüglich der Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.
 - Für die Unternehmen bedeutet das ein Spagat zwischen Flexibilität, Unveränderbarkeit und Dokumentation.

1.6 elektrische Signatur

1.6.1 Allgemein

Mit Inkrafttreten des „Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“ (SigG) wird zwischen vier Formen der elektronischen Signatur unterschieden.

- Die einfache elektronische Signatur z. B. eingescannte Unterschrift und Kontaktinformationen am Ende einer E-Mail mit Angaben zur Person, Firma etc.
- Die fortgeschrittene elektronische Signatur Privater Schlüssel lokal im Rechner. Der private Schlüssel wird zusammen mit dem öffentlichen Schlüssel auf der Festplatte oder einem anderen auslesbaren Medium, z. B. einer Diskette, gespeichert.
- Die qualifizierte elektronische Signatur Das qualifizierte Zertifikat enthält den öffentlichen Schlüssel des Zertifikatsinhabers (Unterzeichnender) und weitere Angaben, wie den Namen des Zertifikatsinhabers und den Gültigkeitszeitraum des Schlüssel-paares. Das Zertifikat (Nutzerzertifikat) ist durch einen Zertifizierungsdiensteanbieter (Trustcenter) signiert worden. Das Trustcenter selbst besitzt auch ein Zertifikat (Wurzelzertifikat), welches von ihm selbst signiert ist und mit dessen Hilfe wiederum die Integrität des Nutzerzertifikates geprüft werden kann.
- Die qualifizierte elektronische Signatur mit freiwilliger Anbieterakkreditierung

Der Signaturmarkt in Deutschland ist noch sehr wenig ausgeprägt. Die qualifizierte elektronische Signatur findet fast ausschließlich für Rechnungssignierung und Signierung von gescannten Dokumenten Anwendung. Es findet noch keine Verbreitung in den Bereichen B2B und B2C statt. Der Hinderungsgrund sind sicher die Registrierung und die Kosten. Dies wird sich aber in Zukunft schneller ändern.

Im Augenblick haben elektronische Rechnungen das größte Lösungspotenzial.

1.6.2 elektronische Rechnungen – digitaler Posteingang

„Endlich Schluss mit Rechnungen in Papierform“ ist die Devise einiger Anbieter und der Wunsch vieler Anwender.

Die aktuelle rechtliche Situation ermöglicht es Unternehmen, erstmals die Rechnungsbearbeitung vollständig in digitaler Form abzuwickeln. Mit Hilfe einer qualifizierten elektronischen Signatur können sie digitale Abrechnungen in Geschäftsprozesse integrieren und somit Zeit und Kosten sparen. Es werden Medienbrüche vom Empfang über die Verarbeitung bis zur Archivierung der Rechnung vermieden und die Aufträge vollständig digital abgewickelt.

Mit Hilfe der digitalen Signatur ist sichergestellt von welchem Partner die Informationen kommen und dass die Daten unverfälscht übertragen worden sind. Damit bei automatischem Datenaustausch die Signatur nicht von einer einzelnen Person erstellt werden muss, erlaubt es der Signaturserver Signaturen in großen Mengen schnell und performant zu bearbeiten.

Der Signaturserver eröffnet Versendern elektronischer Dokumente die Möglichkeit, Massensendungen in digitaler Form mit automatischen Signaturen zu unterschreiben – und dies ohne eigene Investition in teure Hardware und Konfiguration aufwendiger Softwareinstallationen.

Mit Hilfe des Signaturservers wird die Massensignatur nach den Regelungen aus dem Signaturgesetz (SigG) und der Signaturverordnung (SigV) sowie insbesondere nach dem BMF-Schreiben aus dem Jahre 2004 ermöglicht, wobei die Dokumente rechtsgültig signiert und weitergeleitet werden.

Eintreffende Daten, die mit einer digitalen Signatur versehen sind, müssen auf Ihre Unversehrtheit und Gültigkeit geprüft werden. Die Protokollierung der Prüfergebnisse muss für eine weitere Verarbeitung z. B. Archivierung, zur Verfügung gestellt werden. Die Prüfung der Signatur und des Zertifikates kann dabei über ein Onlineportal oder lokal über den digitalen Posteingang durchgeführt werden. Dabei wird eine Protokolldatei in Form eines LogFiles erstellt, um einen nachträglichen Beweis über die Gültigkeit der Signatur zu besitzen.

Der digitale Posteingang (dies sind auch Eingangsrechnungen) empfängt signierte Rechnungen vom Signaturserver und stellt dies übersichtlich dar, um eine einfache Weiterbearbeitung zu ermöglichen. Im Posteingang wird die Signatur anhand des öffentlichen Schlüssels (public key) der qualifizierten digitalen Signatur überprüft, um auf den unveränderten Inhalt des Dokumentes schließen zu können. Weiterhin nimmt der digitale Posteingang den Kontakt zum Verifikationsserver auf, um die Identität des Erstellers der Signatur und damit des Dokumentes zu verifizieren.

Der digitale Posteingang ermöglicht durch seine integrierten Schnittstellen eine leichte Integration in die Geschäftsprozesse des Unternehmens. Dazu zählen ERP-Systeme ebenso wie digitale Archive, die anhand der mitgelieferten Metadaten genutzt werden können.

1.7 E-Mail Archivierung

Die elektronische Archivierung von E-Mails steckt in Deutschland noch in den Kinderschuhen. Nur ein Viertel der von Dr. Haffa Expert Call befragten Entscheider gibt an, dass in ihrem Unternehmen E-Mails ordnungsgemäß archiviert werden. Über ein Drittel wusste bislang gar nicht, dass eine solche Verpflichtung überhaupt besteht. Siehe auch 1.4.

Unternehmen beziehen Archivierungspflichten nicht auf Mailkommunikation. Unternehmen übersehen dabei aber: Information und ihre Verfügbarkeit als essentielle Ressource (Know-how, Beweisführung) und wesentlich gefährlichere Haftungsquelle!

Es gibt bedeutende Fälle mit erheblichen Auswirkungen:

- SEC / Deutsche Bank (2004)
\$ 7.5 Millionen für nicht rechtzeitige Herausgabe interner Mails über Geschäftsvorfälle

- Ronald Perelman / Morgan Stanley Bank (2005)
\$ 1,45 Milliarden Schadenersatz, wegen Nichtverfügbarkeit von E-Mails und Beweislastumkehr wegen Nichtvorlage elektronischer Geschäftspost ebenso
- ERP Projekt Universitäten Stuttgart, Heidelberg (2001)
Verstoß gegen HGB und kaufmännische Sorgfaltspflicht
Nichtverfügbarkeit beweisheblicher Mailkorrespondenz

Worauf ist besonders zu achten:

OLG Karlsruhe 10.1.2005: Ablocken / Ausfiltern von E-Mails als Verstoß gegen das Fernmeldegeheimnis und Datenschutz.

Bei erlaubter oder geduldeter Privatmail gilt:

Ohne Mitarbeiter Zustimmung

- Keine Überwachung der Inhalte der Kommunikation
- gehört private Mail dem Mitarbeiter auch nach seinem Ausscheiden
- kein Unterdrücken / Ausfiltern privater Mail durch Spamfilter (Virenfilter erlaubt + geboten)

Was ist zu tun:

Individualvertrag und / oder betriebliche Policy zum Umgang mit Internet und E-Mail z. B.

- generelles Verbot mit Ausnahmeverbehalt
- betriebliche Mailstandards
- Vertretungs- und Ausscheidungsregelungen
- Ablagedefinitionen
- Kontrollbefugnisse
- Missbrauchssanktionen

Hier wird auch verwiesen auf die Ausführungen GOB Punkt 1.1 und GDPdU Punkt 1.2 sowie Verfahrensdokumentation Punkt 1.3.

Welche E-Mails sind zu archivieren?

Nach der GoB sind steuerrelevante E-Mails als originäre, digitale Dokumente mit einem unveränderbaren Index zu verschlagworten und die maschinelle Auswertbarkeit über mindestens 10 Jahre muss gegeben sein.

E-Mail bzw. Attachments können nicht nur kaufmännische sondern auch steuerrelevante Informationen enthalten.

Belegfunktion, Mittel der Fakturierung und / oder Auftragsabwicklung z. B.

- Reisekostenabrechnung im Tabellenkalkulationsprogramm
- digital signierte Mail mit Rechnung
- steuerrelevante Vertragsgestaltungen

Die Position des Bundesministeriums der Finanzen:

Unter welchen Voraussetzungen und in welchen Formaten müssen E-Mail archiviert oder für den Datenzugriff bereitgehalten werden? E-Mails, die für die Besteuerung von Bedeutung sind, sind nach den allgemeinen Vorschriften des § 147 Abgabenordnung aufzubewahren. Eine (elektronisch übersandte) E-Mail stellt ein originär digitales Dokument dar, das für den Datenzugriff im Originalformat maschinell auswertbar vorgehalten werden muss. Dies gilt beispielsweise für eine per E-Mail übermittelte Reisekostenabrechnung in einem Tabellenkalkulationsformat.

Nach den GoBS (Abschnitt VIII. „Wiedergabe der auf Datenträgern geführten Unterlagen“) sind auch E-Mails als originär digitale Dokumente mit einem unveränderbaren Index zu versehen, unter dem das archivierte digitale Dokument bearbeitet und verwaltet werden kann.

Hinsichtlich der maschinellen Auswertbarkeit ist jedoch nicht entscheidend, ob die per E-Mail übermittelten Daten automatisiert Eingang in das verwendete Buchhaltungssystem gefunden haben oder im betrieblichen DV-System

Importfunktionen zur Übernahme von steuerlich relevanten Daten aus dem Textkörper von E-Mails oder angehängter Dateien vorhanden sind. Als Beispiel sei eine E-Mail aufgeführt, die steuerlich relevante Vertragsgestaltungen enthält. Über den nach GoBS geforderten Index ist die maschinelle Auswertbarkeit – der wahlfreie Zugriff – auf die im Originalformat zu archivierende E-Mail auch in solchen Fällen sicher zu stellen.

E-Mails mit nicht steuerlich relevanten Inhalten müssen hingegen weder archiviert noch für den Datenzugriff vorgehalten werden.

Soweit das BMF.

Fazit:

E-Mail und GoBS / GDPdU

Entscheidet sich das Unternehmen für die elektronische Archivierung seiner Geschäftspost aus Gründen u. a.

- der Praktikabilität
- der internen Beweissicherung
- des Wissensmanagement
- des prozessunterstützten Informationsmanagement...

verzichtet es also auf die klassische vollständige Papierarchivierung, so sind wiederum die strengen Anforderungen des § 257 HGB und der GoBS zu beachten.

Daher gilt: Wer elektronisch archiviert, der muss dies auch richtig tun.

Ein Konglomerat aus Papierarchiv und elektronischem Archiv genügt diesen Anforderungen nicht.