Interessengemeinschaft
EDI für
Telekommunikationsleistungen

Die rechtlichen Aspekte zum elektronischen Rechnungsdatenaustausch

Zu diesem Booklet haben viele Personen und Firmen aus der deutschen Wirtschaft beigetragen.

Unser besonderer Dank gilt:

Herrn Heiko Mehnen, GLI mbH, München
Herrn Carsten von Weschpfennig, Deutsche Telekom AG, Hannover
Herrn Marco Kock, T-Mobile, Bonn
Herrn Ralf Klöckner, T-Systems International GmbH, Frankfurt
Herrn Björn Bendisch, Arcor AG & Co. KG, Eschborn
Herrn Andreas Fessel, e-plus Service GmbH & Co. KG, Düsseldorf
Herrn Peter S. Oberhollenzer, Ingenieurbüro Oberhollenzer, Fischingen
Herrn Frank Siebert, TriNuts GmbH, München
Herrn Jörn Steinhauer, alphasystems GmbH, Augsburg
Herrn Tobias Wacker, WKS GmbH, Lüneburg

Informationsstand: November 2004

Inhalt

1 Einleitung

Der elektronische Austausch von Geschäfts- und Handelsdaten ist bei den meisten Unternehmen bereits heute eine Grundvoraussetzung für den wirtschaftlichen Erfolg. Jede Branche nutzt den elektronischen Datenaustausch für die verschiedensten Standardnachrichten wie Bestellungen, Lieferscheine, Überweisungen oder Rechnungen.

Die Vorteile des elektronischen Rechnungsdatenaustausches sind dabei unbestritten. Empfänger wie Absender elektronischer Rechungen profitieren u.a. durch Prozessoptimierung und Kostensenkungen in verschiedenen Bereichen, Lieferanten verbessern die Kundenbindung.

Eine Branche, die dabei in Deutschland eine Vorreiterrolle übernommen hat, ist die Telekommunikationsbranche. Bereits heute werden monatlich mehrere Millionen Telekommunikationsrechnungen von verschiedenen Carriern elektronisch versandt.
Beim Datenaustausch mit Geschäftskunden wird für die Übermittlung und Strukturierung der Rechnungen der Standard EDIFACT genutzt, eine ISO-Norm, die auch zur Strukturierung anderer Standardnachrichten genutzt wird.

Damit die Inhalte, Codierungen, usw. nicht zu variabel genutzt werden und somit die einheitliche Verarbeitung erschweren, wurde die INET gegründet.
Die INET (Interessengemeinschaft EDI für Telekommunikationsleistungen, siehe auch www.inet-org.de) hat sich zum Ziel gesetzt, den elektronischen Rechnungsdatenaustausch in der Telekommunikationsbranche aktiv zu fördern und zu koordinieren, ohne dass der Wettbewerb beeinflusst wird.

Manchen wird es vielleicht überraschen, dass nach mehr als 15 Jahren EDI und EDIFACT noch ein Booklet zum Thema 'Voraussetzung für die Anerkennung elektronischer Rechnungen' erstellt wird.
Als eines der größten Hemmnisse für die Einführung elektronischer Abrechnungsverfahren hat sich die Ungenauigkeit und fehlende Praktikabilität von Rechtsvorschriften erwiesen, die insbesondere auf Empfängerseite zu beachten sind. Innerhalb der Europäischen Union ist kein Land zu finden, dessen Finanzbehörden höhere Anforderungen an die Anerkennung, Verarbeitung und Archivierung elektronischer Rechnungen stellen als Deutschland.

Mit vorliegendem Booklet möchte die INET einen kurzen Überblick über die rechtlichen Voraussetzungen zur Anerkennung elektronischer Rechnungen geben. In Kapitel 2 finden Sie Informationen, unter welchen Voraussetzungen elektronische Rechnungen überhaupt von den Finanzbehörden akzeptiert werden. Und in Kapitel 3 sind die wichtigsten rechtlichen Voraussetzungen zusammengefasst, die bei der Verarbeitung und Archivierung elektronischer Rechnungsdaten auf Empfängerseite zu beachten sind.

Der Inhalt des Booklets beschränkt sich dabei auf Aspekte des elektronischen Rechnungsdatenaustausch zwischen Geschäftspartnern.

Bitte beachten Sie, dass dieses Booklet nur einen Überblick über die wichtigsten anzuwendenden Rechtsvorschriften beinhaltet und keinen Anspruch auf Vollständigkeit erhebt. Es wird keine Gewähr für eine vollständige und aktuelle Auflistung bzw. Interpretation der relevanten Rechtsvorschriften übernommen. Der Stand der Dokumente entspricht den Festlegungen Mitte 2004. Durch die Initiative der EU und des Europäischen Normungsinstituts CEN sind neue europäische Regelungen zu erwarten.

2 Voraussetzungen für die steuerrechtliche Anerkennung elektronischer Rechnungen

Sind elektronische Rechnungen überhaupt steuerrechtlich anerkannt?

Ja! - Die steuerrechtliche Anerkennung elektronischer Rechnungen ist, wie vieles im Steuerrecht, durch eine entsprechende EU-Richtlinie geregelt.
Damit müssen seit dem 01.01.2004 die nationalen Finanzbehörden aller EU-Mitgliedsstaaten elektronische Rechnungen akzeptieren, wenn diese bestimmte Anforderungen erfüllen.
In Deutschland sind die für die Anerkennung elektronischer Rechnungen maßgeblichen Regelungen im Umsatzsteuerrecht enthalten.

Unter welchen Voraussetzungen sind elektronische Rechnungen steuerrechtlich anerkannt?

Die wichtigsten Bestimmungen im Zusammenhang mit elektronischen Telekommunikations-Rechnungen sind:

- EU-Richtlinie 2001/115/EG des Rates vom 20.12.2001 zur Änderung der Richtlinie 77/388/EWG mit dem Ziel der Vereinfachung, Modernisierung und Harmonisierung der mehrwertsteuerlichen Anforderungen an die Rechnungsstellung (so genannte Rechnungsrichtlinie, siehe Rechnungsrichtlinie)
- §14 Umsatzsteuergesetz (UStG, siehe § 14 UStG)
- BMF-Schreiben zur Umsetzung der EU-Richtlinie 2001/115/EG, Aktenzeichen IV B 7 – S7280 – 19/04 vom 29.01.2004 (siehe BMF-Schreiben) und § 31 UStDV (siehe § 31 UStDV)

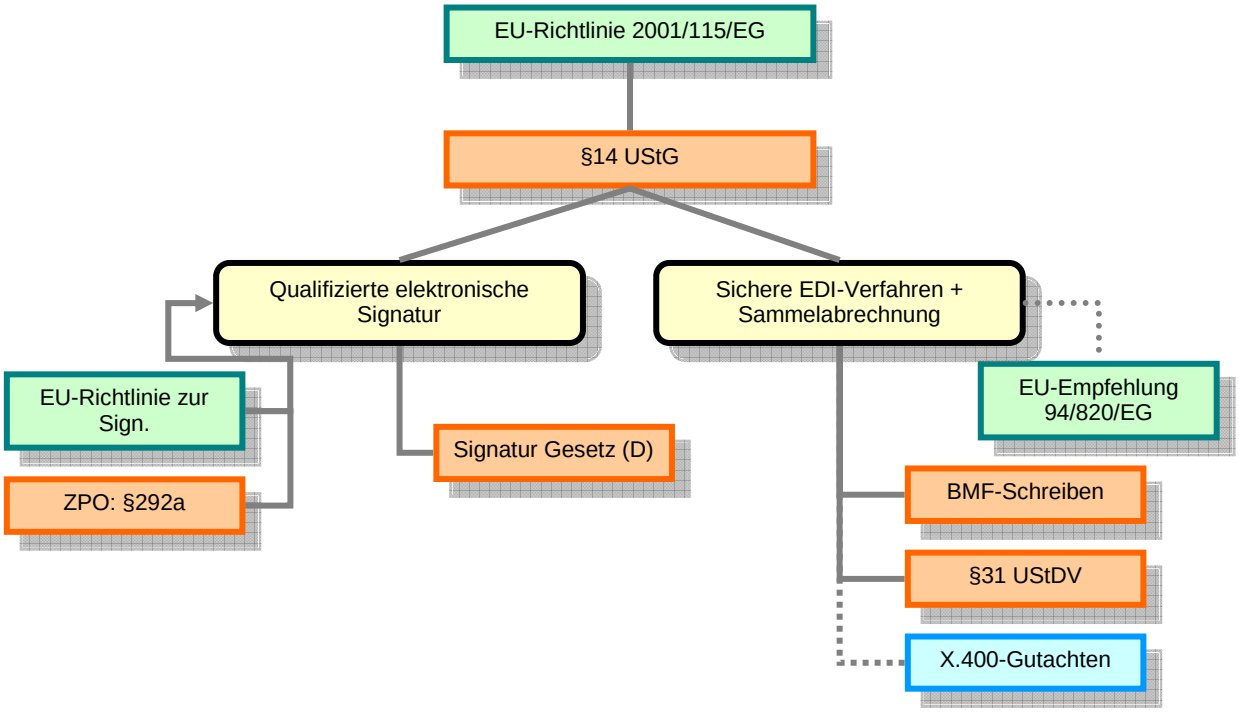
Nach der EU-Richtlinie 2001/115/EG (Rechnungsrichtlinie) akzeptieren die Mitgliedstaaten elektronische Rechnungen, wenn die Echtheit der Herkunft und die Unversehrtheit des Inhalts (Authentizität und Integrität) gewährleistet sind durch:

- Fortgeschrittene elektronische Signatur (die EU-Mitgliedsstaaten können jedoch zusätzlich eine qualifizierte Signatur verlangen) oder
- EDI-Verfahren gemäß Art.2 der EU-Empfehlung 94/820/EG (siehe EU-EDI-Empfehlung), wenn das verwendete EDI-Verfahren die Authentizität und Integrität der Daten gewährleistet. Zusätzlich können die EU-Mitgliedsstaaten verlangen, dass ein zusammenfassendes Dokument in Papierform erforderlich ist (im weiteren Sammelabrechnung genannt).

Die Gewährleistung der Lesbarkeit und Nachweis der Echtheit und Unversehrtheit während der gesamten rechtlich geforderten Aufbewahrungszeit wird zudem explizit erwähnt.

Mit der Neufassung des §14 UStG zum 01.01.2004 wurden die o.g. Anforderungen in Deutschland umgesetzt. Dabei hat der deutsche Gesetzgeber die höchsten Hürden an die Anerkennung elektronischer Rechnungen aufgestellt.
Elektronische Rechnungen werden von den deutschen Finanzbehörden danach akzeptiert, wenn diese mit einer qualifizierten elektronischen Signatur (wahlweise mit Anbieterakkreditierung) versehen sind oder sichere EDI-Verfahren mit einer Sammelabrechnung verwendet werden. Die Sammelabrechnung kann wahlweise ein Papierbeleg oder ein elektronisches Dokument mit einer qualifizierten elektronischen Signatur sein.
Da im B2B-Bereich im Zusammenhang mit dem Austausch elektronischer Rechnungsdaten die qualifizierte elektronische Signatur derzeit in der Praxis noch kaum verwendet wird, finden Sie nähere Informationen zur qualifizierten elektronischen Signatur im Exkurs.
In Deutschland werden im B2B-Bereich derzeit zumeist EDI-Verfahren mit Sammelabrechnungen (als Papierbeleg) eingesetzt. Hierbei wird hauptsächlich der EDIFACT-Standard, auf den auch die EU-Empfehlung 94/820/EG verweist, verwendet.
Die Bestimmungen des §14 UStG zur Anerkennung elektronischer Rechnungen werden durch das o.g. BMF-Schreiben konkretisiert. In diesem werden Anforderungen an die Sammelabrechnung

aufgeführt. Sie kann für mehrere Dienstleistungen periodisch (z.B. monatlich) erstellt werden. Eine Sammelabrechnung muss grundsätzlich alle Merkmale nach § 14 Abs. 4 und § 14a UStG (beinhalten die Pflichtangaben innerhalb einer Rechnung) enthalten. Sie muss für die Umsätze des abgebildeten Zeitraums das Entgelt in einer Summe und den darauf entfallenden Steuerbetrag bezeichnen. Sofern im Übrigen Angaben nicht enthalten sind, kann unter Bezugnahme auf § 31 UStDV auf ergänzende Dokumente und somit auch auf die zugrunde liegenden elektronischen Rechnungen hingewiesen werden.
Zwecks Sicherstellung der im Gesetz geforderten Authentizität und Integrität der Daten wird in Deutschland für den Versand von elektronischen Rechnungen häufig der X.400-Standard eingesetzt. Die Sicherheit des X.400-Standards wird durch ein Gutachten (siehe Gutachten) bestärkt, das für ein X.400-Produkt eines Anbieters erstellt wurde.



3 Verarbeitung und Archivierung elektronischer Rechnungsdaten auf Empfängerseite

In Kapitel 2 dieses Booklets wurden die Vorraussetzungen beschrieben, unter denen eine elektronische Rechnung ein anerkanntes, steuerrechtlich relevantes Dokument darstellt.

Damit ergeben sich für den Empfänger dieses Dokuments natürlich auch entsprechende Rechte und Pflichten, die vor allem den Empfang, die Verarbeitung der Daten in nachgeschalteten Softwaresystemen sowie die Archivierung der Dokumente betrifft.

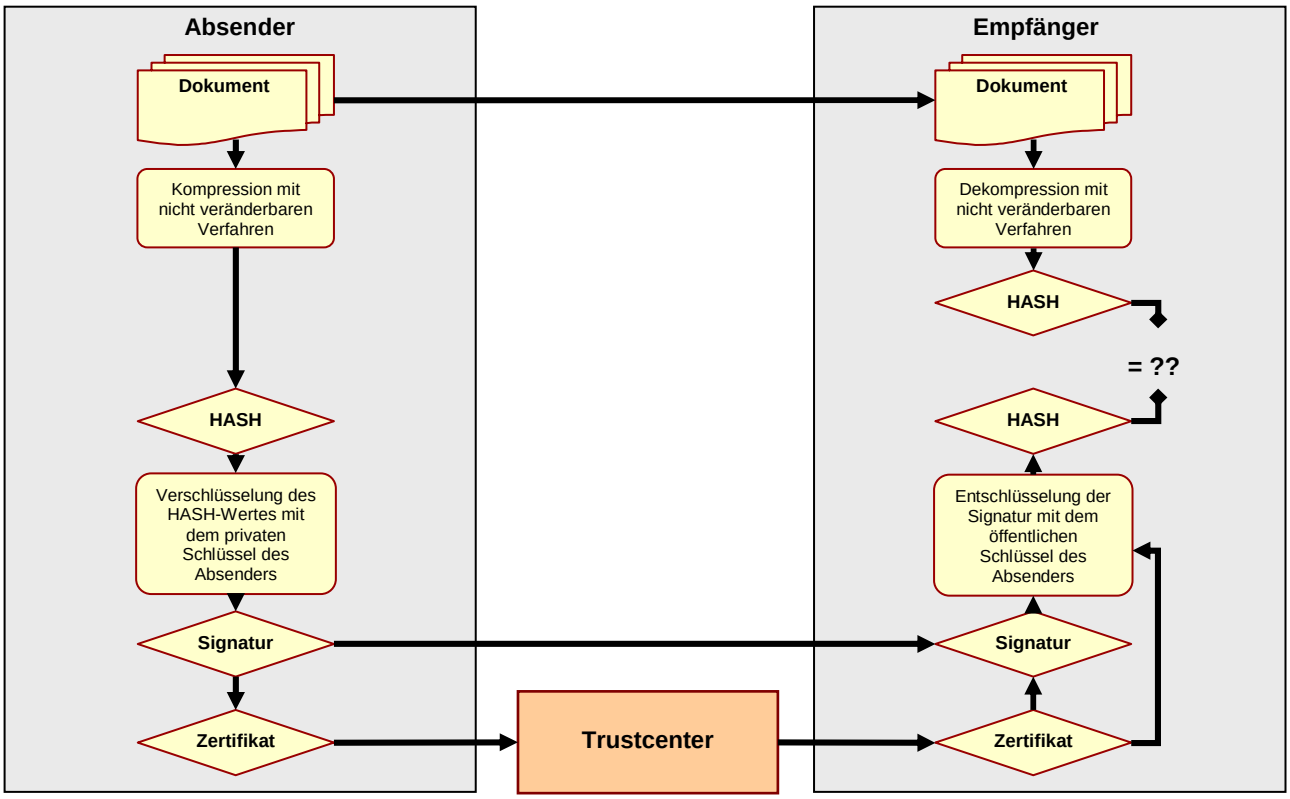
3.1 Empfang der Dokumente

Wie bereits erwähnt, ist eine elektronische Rechnung anerkannt, sofern die entsprechende Echtheit der Herkunft und die Unversehrtheit des Inhalts gewährleistet sind. Wer sich an elektronische Willenserklärungen von Abwesenden binden lassen will, muss sich darauf verlassen können, dass diese vom darin bezeichneten Absender stammen (Authentizität), unverfälscht erhalten bleiben (Integrität) und keinem Unbefugten bekannt werden (Vertraulichkeit). Hierfür gibt es technisch gesehen, verschiedene Möglichkeiten. Eine Variante ist die qualifizierte elektronische (digitale) Signatur, ein anderer Weg ist das bereits beschriebene EDI-Verfahren (über X.400) mit Sammelabrechnung.
In beiden Fällen erhält der Empfänger ein elektronisches Dokument übermittelt, dass diesen Voraussetzungen genügt. Der Empfänger muss nun seinerseits sicherstellen, dass dieses Original-Dokument technisch nicht verändert werden kann. Die Echtheit der Daten muss gewährleistet sein, da eine Veränderung auch in diesem Fall wie bei einem Stück Papier den Strafbestand der Urkundenfälschung (§ 267 StGB), bzw. der Fälschung technischer Aufzeichnungen (268 StGB) darstellt. Auch die verwendeten Softwareprodukte dürfen diese Originale nicht verändern oder erweitern.

3.2 Kommunikationssicherheit

Darunter sind alle Maßnahmen zu verstehen, die die Sicherheit beim Austausch elektronischer Dokumente sicherstellen und gewährleisten.
Beide Seiten (Sender und Empfänger) sind hierbei verpflichtet, entsprechende Vorkehrungen zu treffen, die diesen Datenaustausch so weit wie möglich absichern.
Beispiel für entsprechende Maßnahmen:

- Einrichtung von Firewall-Mechanismen und anderen Maßnahmen zum Schutz vor Hackern
- Festlegung der Verwendung und des Umfangs von Remote Access Services
- Einsatz von Virtual Private Networks (oder anderer spezieller Kommunikationskanäle) für sensible Systemzugriffe oder Transaktionen
- Einsatz von Verschlüsselungsverfahren (Kryptokonzept)
- Einsatz sicherer Protokolle zum Datenaustausch, z.B. SSL-Protokoll, X.400- oder SET-Verfahren (HASH-Wert-Verfahren)
- Sicherung der erforderlichen Bandbreiten und Ausfallsicherheit der Netzanbindungen.



3.3 Vertraulichkeit

Elektronische Rechnungen dürfen generell nur den berechtigten Personen zugänglich sein. Gespeicherte Nutzerdaten müssen ebenfalls geschützt sein und entsprechend den datenschutzrechtlichen Anforderungen behandelt werden. Es muss ausgeschlossen werden, dass z.B. Kundendaten einer bestimmten Person zugeordnet werden können. So sollten beispielsweise auch Mitarbeiter des Kundendienstes und des administratives Personals keinen Zugang zu unverschlüsselten Rechnungs- oder Kundendaten erhalten.
Zur Sicherstellung dieser Parameter müssen folgende Vorgehensweisen im Bereich der Organisations- und Personalsicherheit beachtet werden:

- Festlegung von sicherheitsrelevanten Arbeitsabläufen, Verfahrensweise bei Fehlern und Problemen festlegen.
- Gründliche Personalschulung und schriftliche Belehrung für die beteiligten Mitarbeiter.
- Aktualisieren von Administrationsrechten und Zugangsberechtigungen für Administratoren, Testpersonen und weiteren Mitarbeitern. Darunter fällt z.B. das regelmäßige Ändern wichtiger Passwörter oder auch das Löschen von Personen aus entsprechenden Verzeichnissen, die keinen Zugang zum System mehr erhalten sollen (z.B. nach Tests oder der Beendigung des Arbeitsverhältnisses).
- Schnelle Informationsauswertung von Billern und Kunden zu Anwendungs-Fehlern.
- Service Level Agreements zwischen Lieferant und Empfänger. Darin werden die beidseitig zu liefernden Services, Reporting-Anforderungen, Reaktionszeiten im Fehlerfall, Strafen bei Nichteinhaltung und bestimmte Geschäftsprozesse beschrieben.

3.4 Physikalische Sicherheit

Hierunter ist die Sicherheit und Unversehrtheit, bzw. Wiederherstellbarkeit der Daten auf physikalischer Basis zu verstehen. Darunter fallen Archivierungssysteme („Backup“), der Schutz der Daten vor Diebstahl, Vandalismus, Feuer, Wasser, etc.

Dies bedingt entsprechende Räumlichkeiten und eine entsprechende EDV- und Organisationsstruktur (z.B. externe Auslagerung von Backups).
Weiterhin sind darunter auch Mechanismen der bereits beschriebenen Vertraulichkeit (vor allem Zugangsberechtigungen und Sicherheitsroutinen) zu verstehen.

3.5 Applikationssicherheit

Dieser Sicherheitsaspekt betrifft vor allem die nachverarbeitenden Systeme. Hier müssen zum einen der möglichst fehlerfreie und reibungslose Betrieb sichergestellt werden, als auch die Möglichkeit der Wiederherstellung von Daten. Vor allem im Rahmen der GDPdU der Finanzbehörden (siehe 3.7) werden hier einige Anforderungen an die Nachverarbeitungssysteme und –mechanismen gestellt.

- Funktionssicherheit der eingesetzten Software durch Tests und geeignete Anbieterauswahl gewährleisten.
- Schutz vor Datenverlusten durch Raid-Systeme (Festplatten-Ausfallsystem), Datenspiegelung oder Backupsysteme.
- Methoden und Protokollverfahren zum Fehlerhandling bei fehlerhafter Soft- oder Hardware.
- Sicherung der Verfügbarkeit durch Loadbalancing (Lastverteilung) und Skalierbarkeit der Systeme. Der Austausch oder die Erweiterung bestimmter Komponenten muss auch im laufenden Betrieb möglich sein.
- Absicherung vor unbefugtem Systemzugang zu Daten oder Programmen durch User-Authentifizierung bzw. Nutzerverwaltung, durch Einsatz von Virenschutzsoftware, Firewall-Systemen, Verschlüsselungsmechanismen, usw. .
- Sensible Daten sind sowohl innerhalb als auch außerhalb der Systeme verschlüsselt zu speichern (Beispiel: USB-Sticks).
- Die Protokollierung wichtiger System- bzw. Anwendungsvorgänge muss festgelegt werden.

3.6 Archivierung

3.6.1 Haftung für verlorene Daten

Nach der aktuellen Rechtsprechung haftet der Unternehmer persönlich dafür, dass kein für die Erhebung von Steuern bedeutsames Dokument oder Datensatz in seinem Unternehmen verloren geht. Dies gilt nicht nur für Dateien sondern vor allem auch für E-Mails. Diese müssen inklusive der angehängten Dokumente über zehn Jahre lückenlos abgespeichert sein. Nach Auffassung des Finanzgerichtshofes kann es sich bei jeder E-Mail um eine für die Steuer bedeutsame Information bzw. relevantes Dokument handeln. Im Zusammenhang damit ist der Steuerpflichtige dafür verantwortlich, vor Löschung von E-Mails zu prüfen, ob der Inhalt der E-Mail steuerrechtlich relevant ist oder nicht.

3.6.2 Prüfung durch die Finanzbehörden

Generell darf der Betriebs- oder Wirtschaftsprüfer grundsätzlich alle digitalen Dokumente des Betriebes einsehen, die in den letzten zehn Jahren erstellt worden sind.
Dabei spielt es keine Rolle, ob es sich um ein per E-Mail übermitteltes Angebot, einen Vertrag oder um sonstige auf dem Computer abgespeicherte Hintergrundinformation handelt.
Dieses Recht der Einsichtnahme wird nur durch die generellen und allgemeinen Daten- und Persönlichkeitsschutzrechte eingeschränkt. Diese Maßgabe birgt jedoch für das Unternehmen

einige Fallen. Denn die Daten müssen, auch wenn sie 10 Jahre alt sind, noch „sichtbar“ gemacht werden. D.h. neben den eigentlichen elektronischen Daten müssen auch die entsprechenden Softwaresysteme verfügbar sein, die diese Daten auch wieder sicht- und auswertbar machen.

3.6.3 Revisionssichere Archivierung

Unter revisionssicherer Archivierung versteht man Archivsysteme, die entsprechend den gesetzlichen Vorgaben die Daten und Dokumente des Unternehmens sicher, unverändert, vollständig ordnungsgemäß verlustfrei reproduzierbar und datenbankgestützt recherchierbar verwalten. Es gibt bis jetzt jedoch noch keine genauen Vorgaben oder Festlegungen, wie die Ausgestaltung dieser Revisionssicherheit auszusehen hat. Hier spielen die Gewohnheiten, die Organisationsstrukturen und die Menge der zu archivierenden Daten im jeweiligen Unternehmen eine wichtige Rolle.

Um die revisionssichere Archivierung zu gewährleisten sind einige Schritte (zwingend oder optional) notwendig, die beim Aufbau eines Archivsystems beachtet werden sollten.

1. Selektion (notwendig)
Der Datenbestand (steuerrelevante und Stammdaten) wird aus den Datensystemen (siehe Abschnitt GDPdU) extrahiert, inklusive der Strukturdefinitionen und Attributen und als Datei gespeichert

2. Validierung (optional)
Die gespeicherten Daten werden nochmals manuell oder automatisiert auf Vollständigkeit und Korrektheit validiert

3. Übergabe (notwendig)
Die extrahierten Daten werden an das Archivsystem übergeben. Dies kann ebenfalls wieder manuell oder automatisiert erfolgen. Die Automatisierung hat den Vorteil, dass die Daten nicht mehr verändert werden.

4. Indizierung der Daten (notwendig)
Die Daten werden im Archivsystem so indiziert, dass sie zu jedem Zeitpunkt eindeutig auffindbar sind. Sollten bestimmte Daten mehrfach übertragen werden, muss eine Versionierung erfolgen.

5. Speicherung (notwendig)
Die Daten werden inkl. Index und einem Zeitstempel (optional) auf entsprechenden Medien gespeichert. Dabei muss gewährleistet sein, dass die eindeutige Identifizierbarkeit, Vollständigkeit und Unveränderbarkeit gewährleistet bleibt.

6. Migration (konditional)
Sollte im Laufe der Zeit eine Migration der Daten in ein anderes Archivsystem notwendig werden, sind die Daten, die Strukturinformationen und auch der Index verlust- und veränderungsfrei zu überführen. Der Migrationsprozess muss mit einer entsprechenden Protokolldatei dokumentiert werden.

7. Zugriff auf die Daten (notwendig)
Im Falle eine Prüfung muss das Archivsystem die Daten für den auszuwertenden Zeitraum suchen und korrekt sowie vollständig anzeigen. Entsprechende Strukturinformationen oder Migrationsprotokolle sind ebenfalls mitzuliefern.

8. Prüfung auf Vollständigkeit und Korrektheit (empfohlen)
Die Indizierung hat sicherzustellen, dass entsprechend der Suchanfrage die gefundenen Daten vollständig und richtig sind. Ein Zeitstempel nach Signaturgesetz kann hier die Aussagekraft des Protokolls verbessern. Die Protokolle sollten für den Nachweis auch druckbar und exportierbar sein.

9. Bereitstellung (notwendig)
Die gefundenen Daten müssen nun bereitgestellt werden. Dies kann entweder durch Export, Bereitstellung in den Hauptsystemen (sofern möglich) oder über ein universelles Auswertungsprogramm (siehe Abschnitt GDPdU) erfolgen.

3.6.4 Umfang der Archivierung bei elektronischen Rechnungen

Der Umfang der Archivierung bei elektronischen Rechnungen ist u.a. in einem BMF-Schreiben (siehe BMF-Schreiben zu GDPDU) aufgeführt.

Insbesondere folgende Sachverhalte müssen bei dem Empfang und der Verarbeitung elektronischer Rechnungen unbedingt archiviert werden:

- Dokumentation, dass qualifizierte elektronische Signatur entsprechend geprüft wurde.
- Signaturprüfschlüssel.
- Elektronische Originalrechnung **und** die konvertierte Rechnung (Inhouse-Format).

Protokollierung des Eingangs der elektronischen Rechnung, ihrer Archivierung und ggf. Konvertierung sowie der weiteren Verarbeitung.

Des Weiteren ist bei EDI-Verfahren unbedingt darauf zu achten, dass auch die Sammelabrechnung (siehe Kapitel 2) entsprechend den steuerrechtlichen Vorschriften zu archivieren ist.

3.7 GDPdU

Ein Betriebsprüfer bekommt den Auftrag, einen Betrieb oder ein Unternehmen zu prüfen. Für bestimmte Prüfungsfelder und Prüfungszeiträume beschließt der Betriebsprüfer, die Daten unter Zuhilfenahme von Prüfungssoftware zu analysieren. Entsprechend gibt der Betriebsprüfer dem Unternehmen die Prüfung an sich und die Prüfungsschwerpunkte bekannt.
Da der Betriebsprüfer die behördeneigene Prüfsoftware (z.B. IDEA) nicht auf der EDV des Unternehmens installieren darf, die Prüfung also auf dem eigenen Computer durchführen muss, verlangt er, die Daten per Datenträgerüberlassung bereitzustellen. Er beruft sich dabei auf die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“, kurz GDPdU.

3.7.1 elektronische Unterlagen

Neben den „steuerrelevanten Daten“ – ein durchaus dehnbarer Begriff - hat innerhalb der GDPdU der Begriff der „originär elektronischen Unterlagen“ eine wichtige Bedeutung (siehe auch 3.3).
Bei originär elektronischen Unterlagen handelt es sich in erster Linie um Daten, die in einem kaufmännischen System selbst durch Verarbeitungsschritte entstanden sind. Bei der Entstehung dieser Daten sind unterschiedliche Quellen zu berücksichtigen. Sie können aus anderen Datenverarbeitungssystemen importiert (siehe Nebensysteme und vorgelagerte Systeme), von Dritten durch Datenübertragung übermittelt (z.B. EDI, E-Mail) oder aber durch manuelle Eingaben erfasst worden sein. Durch die Verarbeitung, d.h. im wesentlichen durch die Zuweisung zu Vorgängen, Konten, Lieferanten oder Kunden, durch Berechung von abgeleiteten Werten, Zuordnung von Stammdaten und andere Operationen der Programmlogik entstehen erst die originär elektronischen, steuerrelevanten Daten. Erst durch die Verarbeitung und die Zuweisung im buchhalterischen Sachzusammenhang entstehen die steuerrelevanten Daten. Die Rohdaten vor der Verarbeitung haben daher einen Belegcharakter, der die Nachvollziehbarkeit der durchgeführten Operationen der Software sicherstellen muss.

3.7.2 Datenverarbeitungssystem im Sinne der GDPdU

Durch die Vorgaben der GDPdU in Bezug auf Bereithaltung, Archivierung und Originalität von Daten sind natürlich auch die verschiedenen Datenverarbeitungssystemen betroffen. Je nach dem, in welchem Umfang steuerrelevante Daten in ihnen entstehen und gespeichert werden ist ihre Relevanz für eine elektronische Steuerprüfung verschieden. Daher wurden hier verschiedene

Differenzierungen geschaffen, um die Qualität und die Wichtigkeit der Daten und der Systeme zu unterscheiden.

Zugriffsdifferenzierung:

1. Unmittelbarer Datenzugriff (Z1): Der Prüfer darf zur Prüfung direkt auf die im Unternehmen zur Buchhaltung eingesetzten Systeme (Hard- und Software) zugreifen. Das Unternehmen muss ihn in die Bedienung der Systeme einweisen und alle notwendigen Hilfsmittel zur Verfügung stellen.

2. Mittelbarer Datenzugriff (Z2): Der Prüfer kann verlangen, dass die notwendigen Daten für die Prüfung durch eigene Systeme mit entsprechendem Personal nach den behördlichen Vorgaben ausgewertet und zur Verfügung gestellt werden.

3. Datenüberlassung in elektronischer Form (Z3): Die Daten werden aus den Systemen in ein elektronisch verwertbares Format exportiert und können durch die finanzbehördlichen Systeme ausgewertet werden. Dies gilt vor allem für Daten der Lohn-, Finanz- und Anlagenbuchhaltung.

Systemdifferenzierung:

1. "Hauptsystem"
Unter einem Hauptsystem ist dasjenige System, bestehend aus Software und benötigter Hardware zu verstehen, in dem die originär steuerrelevanten Daten verarbeitet und gespeichert werden. Dies sind in der Regel kaufmännische Anwendungen, ERP-Systeme, Buchhaltungssysteme etc. Solange dieses Hauptsystem im Betrieb ist spricht man auch vom operativen, Produktiv- oder Produktionssystem um es von stillgelegten, redundanten Sicherheits- oder im Testbetrieb befindlichen Systemen zu unterscheiden. Das Hauptsystem mit seiner Programmfunktionalität und seinen Auswertungsmöglichkeiten erfüllt auch die Voraussetzungen des unmittelbaren Zugriffs (Z1) und des mittelbarer Zugriffs (Z2) sowie die Erstellung von Datenträgern (Datenträgerüberlassung, Z3).

2. "Vorgelagertes System"
Vorgelagerte Systeme sind Lösungen, mit denen steuerrelevante Daten und Belege erfasst und verarbeitet werden (z.B. Scannen mit Übertragung ins ERP), deren Ergebnisse jedoch in ein Buchführungs-, ERP- oder vergleichbares System übertragen werden und dort für den Zugriff bereitstehen. Dabei ist sicherzustellen, dass die Verarbeitung und Übertragung verlustfrei, nachvollziehbar und ohne Veränderung der originären Daten und Belege geschieht. Die Daten dieser Systeme gehören auch zum Umfang einer digitalen Außenprüfung. Bei vorgelagerten Systemen ist im Regelfall kein (un)mittelbarer Zugriff möglich und diese besitzen meist auch keine Möglichkeit der Datenträgerüberlassung. Hier sind häufig die Datenmengen so groß, dass eine vollständige Datenübergabe technisch gar nicht möglich ist.

3. "Nebensystem"
Unter Nebensystemen versteht man Systemlösungen, in denen steuerrelevante Daten entstehen, gespeichert und verarbeitet werden, die nicht oder nur sehr stark verdichtet im Buchhaltungs- oder ERP-System vorliegen. Hierbei kann es sich um Materialwirtschafts-, Zeiterfassungs- oder E-Business-Anwendungen handeln, die eine eigenständige Logik und Speicherung besitzen. Die Daten dieser Systeme dürfen auch der elektronischen Steuerprüfung unterworfen werden. Sofern die steuerrelevanten Daten in diesen Systemen qualifiziert und identifiziert werden können, kann auch ein direkter Zugriff über die Anwendung möglich sein. Der unmittelbare und mittelbare Zugriff, sowie die Datenüberlassung sind bei Nebensystems häufig beschränkt oder gar nicht möglich.

4. "Archivsystem"
Archivsysteme kommen erst dann ins Spiel, wenn in den operativen Haupt-, Neben- und vorgelagerten Systemen die steuerrelevanten Daten des Prüfungszeitraums nicht mehr auswertbar vorliegen. Angesichts der Aufbewahrungsfristen von 6 oder 10 Jahren ist die

Auslagerung von Datenbeständen aus den Produktivsystemen besonders bei mittleren und größeren Anwendungen der Regelfall. In Archivsystemen entstehen jedoch selbst keine steuerrelevanten Daten, sondern sie dienen lediglich der Speicherung und der Bereitstellung der Daten. Die Auswertbarkeit und die Vollständigkeit müssen von den Hauptsystemen und den Nebensystemen bereits bei der Übergabe der Daten an das Archivsystem sichergestellt sein.

5. "Universelles Auswertungsprogramm für steuerrelevante Daten"
Wenn Archivsysteme selbst nicht mehr über die Auswertungslogik des Hauptsystems verfügen müssen, wenn es nur noch vollständige, auswertbare steuerrelevante Daten übernimmt und auf Anforderung wieder bereitstellt, muss die Auswertbarkeit der steuerrelevanten Daten mit anderen Mitteln sichergestellt werden (siehe hierzu auch 3.6). Die Finanzbehörden arbeiten derzeit an Systemen für die Prüfung von elektronischen Daten (z.B. IDEA oder ACL). Die Systeme im Unternehmen sollten dann in der Lage sein, die Daten für ein solches universelles Auswertungsprogramm zur Verfügung zu stellen.

(Quelle: www.gdpdu-portal.de)

4 Exkurs: Qualifizierte elektronische Signatur in der Praxis

Für die elektronische Rechnungsstellung wird im UStG gefordert, dass die Unversehrtheit des Inhalts und die Echtheit der Herkunft gewährleistet werden muss. Gemäß §14 UStG kann in der Praxis hierfür die qualifizierte elektronische Signatur genutzt werden. Elektronische Signaturen sind im Signaturgesetz (SigG, siehe Signaturgesetz) definiert. Beispielsweise wird für die Erstellung einer qualifizierten elektronischen Signatur u.a. gefordert, dass diese mit einer sicheren Signaturerstellungseinheit erzeugt wird und zum Zeitpunkt der Erzeugung auf einem gültigen qualifizierten Zertifikat beruht. Im Zusammenhang mit der steuerrechtlich geforderten Unversehrtheit des Inhalts und der Herkunft der Daten erfüllt die qualifizierte elektronische Signatur die höchsten Sicherheitsanforderungen, die im SigG aufgeführt werden.

Unversehrtheit des Inhalts: Die Signatur eines elektronischen Dokumentes ist eine verschlüsselte Prüfsumme, die mittels definierter mathematischer Verfahren berechnet wird. Jede Veränderung des Dokumentes führt bei Anwendung des mathematischen Verfahrens zu einem anderen Ergebnis. Die Verschlüsselung dieser Prüfsumme stellt darüber hinaus eine eindeutige Beziehung zwischen der berechneten Prüfsumme und dem Unterzeichner her und garantiert, dass die Prüfsumme in der Signatur nachträglich nicht mehr verändert werden kann.
Folgendermaßen erfolgt die Überprüfung einer elektronischen Signatur:

- Die Prüfsumme des Dokuments wird berechnet
- Die Prüfsumme in der Signatur wird entschlüsselt
- Die beiden Prüfsummen werden verglichen

Sofern die beiden Prüfsummen gleich sind, ist die Authentizität und damit also die Unversehrtheit des Inhalts nachgewiesen.

Echtheit der Herkunft: Zur Erstellung einer Signatur wird ein Zertifikat genutzt, welches unter anderem die Feststellung der Identität des Unterzeichners ermöglicht.
Um die Identität eines Zertifikatsinhabers zu prüfen, existiert eine dritte Stelle, die sicher feststellt und mittels Verzeichnisdienste öffentlich zugänglich macht, wem dieses Zertifikat gehört. Diese dritte Stelle nennt sich Trustcenter. Die Trustcenter in Deutschland unterstehen der RegTP, die als staatliche Behörde für die Einhaltung der rechtlichen Rahmenbedingungen verantwortlich ist.

Eine mit einer qualifizierten elektronischen Signatur unterzeichnete elektronische Rechnung erfüllt daher alle Anforderungen des UStG und wird vom Finanzamt zum Vorsteuerabzug anerkannt.

Zwei weitere Begriffe sind in diesem Umfeld noch von wesentlicher Bedeutung. Der Begriff des „Attribut-Zertifikates“ und die „Akkreditierung“.

Gemäß dem BGB (§126a) ist die elektronische Signatur der eigenhändigen Unterschrift gleich gestellt. Mit einem Attribut-Zertifikat kann der Geltungsbereich einer Signatur eingeschränkt werden. Dort könnte z.B. geregelt sein, dass nur Rechnungen signiert werden dürfen. Somit wäre eine solche Signatur unter einem Vertragsdokument rechtlich nicht bindend.

Die Akkreditierung ist laut SigG eine freiwillige Prüfung eines Zertifizierungsdiensteanbieters. Wenn sich ein Trustcenter als Zertifizierungsdiensteanbieter akkreditieren lässt, wird geprüft, ob alle rechtlichen Vorschriften erfüllt sind. Akkreditierte Zertifikate müssen von dem Trustcenter für 30 Jahre zur Verifikation bereitgehalten werden. Die RegTP garantiert die Einhaltung dieser Fristen.
Die elektronische Rechnung, also das Dokument und die Signatur unterliegen den normalen Vorschriften für die Rechnungslegung und müssen somit für zehn Jahre archiviert werden.
Als Empfänger einer Rechnung ist man gemäß der GDPdU neben der normalen inhaltlichen Prüfung verpflichtet, die Signaturen zu prüfen und die Prüfung zu dokumentieren. Es empfiehlt sich, diese Dokumentation zusammen mit der Rechnung im Archiv abzulegen.
Ein qualifizierter Zeitstempel ist rechtlich nicht erforderlich.