

Newsletter Competence Center Steuern & Recht

Ausgabe 2/2007

Finanzgerichte weiten Datenzugriff aus

Stefan Groß, Steuerberater/CISA, Peters, Schönberger & Partner GbR, München

Vernichtung der Originale beim Scannen von Eingangsrechnungen aus handels- und steuerrechtlicher Sicht

Wolfgang Heinrich, EASY Software AG

IDW RS FAIT 3 - Neue Prüfungsrichtlinie für DMS-Lösungen

Thorsten Brand, Senior-Berater Zöller & Partner GmbH

Nachsignieren

Oliver Berndt, B&L Management Consulting GmbH

Veranstaltungen des CC Steuern und Recht am 26. September 2007 im VOI-Forum der DMS Expo

Peter Seiler, GID GmbH

Impressum

Herausgeber: VOI – Verband Organisations- und Informationssysteme e.V., Heilsbachstr. 25, 53123 Bonn, Postfach 140 231, 53057 Bonn, Telefon +49 228 9082089, Fax +49 228 9082091, voi@voi.de, www.voi.de

Redaktionelle Auswahl: Peter Seiler, (pseiler@gid-it.de), Stefan Groß (s.gross@pspmuc.de)

Der VOI-Newsletter gibt die gesetzlichen Neuregelungen, Rechtsprechung und Finanzverwaltungsanweisungen nur auszugsweise wieder. Für etwaige Informationsfehler übernehmen wir keine Haftung. Die Inhalte der einzelnen Beiträge sind nicht zu dem Zweck erstellt, abschließende Informationen über bestimmte Themen bereitzustellen oder eine Beratung im Einzelfall ganz oder teilweise zu ersetzen.

Finanzgerichte weiten Datenzugriff aus

Stefan Groß, Steuerberater/CISA, Peters, Schönberger & Partner GbR, München

Während die Urteile der Finanzgerichte Rheinland-Pfalz und Hamburg aus dem Jahr 2006 das Recht auf Datenzugriff noch an vielen Stellen eingeschränkt und damit dem Steuerpflichtigen entgegen kamen, weisen zwei aktuelle Urteile des Finanzgerichts Düsseldorf in eine andere Richtung. Beide Entscheidungen vom 5. Februar 2007 beschäftigen sich im Kern mit der Reichweite des Datenzugriffs, also mit dem Umfang, welcher einer digitalen Betriebsprüfung zu Grunde zu legen ist und interpretieren diesen in einer Art, welche über das bisherige Verständnis von Literatur und Verwaltung hinausgeht. Dazu haben die Richter teilweise eigenständige Definition von GDPdU-Begrifflichkeiten vorgenommen und damit neue Diskussionspunkte eröffnet.

FG Düsseldorf vom 5. Februar 2007 – Steuerrelevanz vs. Steuerauswirkung

Die Finanzbehörde darf im Rahmen des steuerlichen Datenzugriffs auch auf solche Konten der handelsrechtlichen Finanzbuchhaltung zugreifen, auf denen steuerlich nicht abzugsfähige Betriebsausgaben verbucht werden.

Sachverhalt

Das FG Düsseldorf hatte sich in einer Entscheidung zur Aussetzung der Vollziehung mit der Frage zu beschäftigen, inwieweit der Ausschluss bestimmter Konten vom Datenzugriffsrecht zulässig ist (FG Düsseldorf vom 5. Februar 2007 – Az.: 16 V 3457/06 A(AO)). Im vorliegenden hatte das Finanzamt eine Betriebsprüfung für die Jahre 2001 bis 2003 bei einer deutschen Aktiengesellschaft (AG) angeordnet, die ihre handelsrechtliche Finanzbuchhaltung in diesem Zeitraum über das FiBu-System „R3“ abgewickelt hatte. Da keine eigenständige steuerliche Buchführung bestand, wurden abweichende Bilanzansätze auf Grundlage des § 60 Abs. 2 EStG in eine Steuerbilanz bzw. eine steuerliche Gewinn- und Verlustverrechnung übergeleitet. Im Rahmen der Betriebsprüfung verweigerte das Unternehmen dem Finanzamt nun den Datenzugriff auf ausgewählte FiBu-Konten mit der Begründung, dass nur solche Daten als steuerrelevant i. S. d. § 146 Abs. 7 AO einzustufen seien, die auch letztlich in die Besteuerung eingehen. Auf Grundlage dieser Argumentation wurden Konten

im Zusammenhang mit der Bildung von Drohverlustrückstellungen aus schwebenden Geschäften, nicht abzugsfähigen Betriebsausgaben sowie Aufwendungen für handelsrechtliche Steuerumlagen im Rahmen der körper- und gewerbesteuerlichen Organschaft vom Zugriffsrecht des Betriebsprüfers ausgeschlossen.

Das Finanzamt gab sich damit nicht zufrieden und entgegnete, dass als Prüfungsgegenstand stets die gesamte Buchführung des Steuerpflichtigen anzusehen sei. Die in Frage stehenden Konten seien der steuerlichen Gewinnermittlung, ohne welche die eigentliche Ausgangsgröße Gewinn und auch dessen spätere (steuerbilanzielle oder außersteuerbilanzielle) Korrektur nicht hinreichend prüfbar sei. Weiter bemängelte das Finanzamt, dass es das Unternehmen zunächst unterlassen habe darauf hinzuweisen, dass bestimmte Konten nicht freigeschaltet waren. Dies sei dem Finanzamt erst aufgefallen, als beim Versuch, eine nicht verdichtete Summen- und Saldenliste zu erzeugen, in Folge der nicht freigeschalteten Konten erhebliche Differenzen aufgetreten seien.

Entscheidung

Das zur Entscheidung herbeigerufene Finanzgericht Düsseldorf schloss sich der Auffassung des Finanzamts an und sah keine ernstlichen Zweifel an der Rechtmäßigkeit auf den Datenzugriff der von Seiten des Unternehmens zunächst gesperrten Konten. Bei den fraglichen digitalen Kontoaufzeichnungen handele es sich um „Bücher“ i.S.d. § 147 Abs. 1 Nr. 1 AO, die – anknüpfend an das Handelsrecht – die Funktion erfüllten, für einen Kaufmann seine Handelsgeschäfte und die Lage seines Unternehmens zu dokumentieren. Da zu den Büchern letztlich auch die einzelnen Buchungssätze und deren Übertragung auf die Sachkonten rechneten und die Unterlagen mit Hilfe eines Datenverarbeitungssystems (R3) erstellt wurden, liege im Streitfall das für den Datenzugriff maßgebliche Kriterium der „maschinell auswertbaren Daten“ vor. Weiter führte das Gericht aus, dass die im Rahmen der GDPdU geforderte „steuerliche Relevanz“ nicht mit der vom betroffenen Unternehmen angeführten „steuerlichen Auswirkung“ gleichgesetzt werden dürfe. Dabei habe sich die eigentliche Steuerrelevanz stets auch daran zu orientieren, inwieweit die in Frage kommenden Unterlagen einen Bezug zur Buchführung aufwiesen und mithin zu deren Verständnis erforderlich seien. Inwieweit sich aus den Unterlagen eine konkrete Gewinnauswirkung ergebe, hielten die Richter hingegen für unbeachtlich. Im Übrigen sei die handelsrechtliche Buchführung, da die Steuerbilanz im Ergebnis als abgeleitete Handelsbilanz zu verstehen sei, stets zur Feststellung oder Überprüfung der Besteuerungsgrundlagen geeignet und folglich auch für die Besteuerung von Bedeutung. Die in Frage stehenden FiBu-Konten

seien damit vom Umfang des Datenzugriffs gedeckt, das Finanzamt brauche sich insoweit nicht auf andere Unterlagen, etwa in Papierform, verweisen zu lassen.

Praxishinweis

Die Klarstellung des FG Düsseldorf, dass alle Konten der handelsrechtlichen Finanzbuchhaltung vom Datenzugriff betroffen sind, kommt nicht wirklich überraschend, waren die in Frage stehenden Unterlagen wohl doch auch schon für die steuerliche Außenprüfung in Papierform maßgeblich. Es bleibt indes abzuwarten, ob das Zugriffsrecht auch gelten soll, wenn beispielsweise ein IFRS-Abschluss seitens des Unternehmens erstellt wird. Interessant ist darüber hinaus, dass die Richter der Auffassung sind, der Begriff der Steuerrelevanz sei derzeit noch weitestgehend ungeklärt. Insbesondere konnten die Richter dem im Fragen- und Antwortenkatalog der Finanzverwaltung unternommenen Definitionsversuch nur ungenügende Praxistauglichkeit attestieren, da es sich dabei um eine bloße Begriffsumschreibung handele.

FG Düsseldorf vom 5. Februar 2007 – GDPdU-Begrifflichkeiten neu definiert

Werden Eingangsbelege beim Steuerpflichtigen gescannt, gespeichert und die Originale anschließend vernichtet, so erstreckt sich das Zugriffsrecht im Rahmen der elektronischen Steuerprüfung auch auf derart erzeugte Datenbestände. Der Steuerpflichtige muss diese Datenbestände so organisieren, dass bei einer zulässigen Einsichtnahme keine geschützten Bereiche des Unternehmens tangiert werden.

Sachverhalt

Das FG Düsseldorf hatte sich in einer Entscheidung zur Aussetzung der Vollziehung mit der Frage zu beschäftigen, ob sich der Datenzugriff der Finanzverwaltung auch auf digitalisierte Eingangsbelege erstreckt, deren Original vernichtet wurde (Beschluss v. 05.02.2007 - Az.: 16 V 3454/06 A(AO)). Betroffen war eine Aktiengesellschaft (AG) mit Sitz im Inland, die eine softwaregestützte Belegarchivierung im Einsatz hatte. Dabei wurden sämtliche Eingangsrechnungen eingescannt und die Originalbelege anschließend vernichtet. Während in diesem Zusammenhang bei 90% der eingehenden Rechnungen eine Trennung in steuerlich relevante und steuerlich nicht relevante Unterlagen vorgenommen wurde, galt dies nicht für die übrigen 10% der Fälle. Im Rahmen der steuerlichen Außenprüfung für die Veranlagungszeiträume 2001 bis 2003 wollte die AG den Zugriff der Finanzverwaltung auf jene 90% begrenzen, die eindeutig als steuerlich relevant klassifiziert werden konnten. Eine rückwirkende Trennung der übrigen 10% sei, so

das Unternehmen, nur mit einem unverhältnismäßigen Kostenaufwand möglich. Jedoch könnten diese Belege ausgedruckt und dann in Papierform vorgelegt werden. Außerdem handele es sich bei den Belegen weder um originär digitale, noch um maschinell auswertbare Daten im Sinne der GDPdU, da sie durch den Scan-Vorgang von analoger Form in digitale Form (z. B. PDF-Dateien) transformiert worden waren. Das Finanzamt war damit nicht einverstanden und forderte, den Zugriff auf alle digitalisierten Belege freizugeben.

Entscheidung

Das FG Düsseldorf sah keine ernstlichen Zweifel daran, dass dem Finanzamt nach § 147 Abs. 6 Satz 1 AO das Recht zustehe, auf die fraglichen Belege zuzugreifen. Zunächst sei klar, dass es sich bei Eingangsrechnungen (und auch Ausgangsrechnungen) um Unterlagen im Sinne des § 147 Abs. 1 AO handele. Diese Belege seien zudem „mit Hilfe eines Datenverarbeitungssystems“ erstellt worden und damit auch „maschinell auswertbar“. Wenn Belege in Papierform in elektronische Form überführt würden, komme es, so die Ansicht der Richter, nicht darauf an, ob originär digitale Daten vorlägen. Die digitalisierten Daten würden damit an die Stelle der Originale treten. Auch müsse das Merkmal der maschinellen Auswertbarkeit weiter ausgelegt werden, als dies bisher in Literatur und Verwaltungsanweisungen geschehen sei. Die Auslegung könne sich nicht einseitig aus der Perspektive des Datenzugriffs (respektive aus den derzeitigen Einsatzmöglichkeiten der Prüfsoftware der Finanzverwaltung) ergeben, sondern müsse vielmehr auch nicht-mathematische Operationen, die eine Prüfung von Unterlagen im weitesten Sinne ermöglichen, berücksichtigen. Gemeint sind damit etwa Bildschirmabfragen, die Nachverfolgung von Verknüpfungen und Verlinkungen oder Textsuchen nach bestimmten Eingabekriterien.

Weiter entschieden die Richter, dass es stets Aufgabe des steuerpflichtigen Unternehmens sei, seine Datenbestände so zu organisieren, dass bei einer zulässigen Einsichtnahme in die steuerlich relevanten Datenbestände keine geschützten Bereiche des Unternehmens tangiert würden (vgl. FG Rheinland-Pfalz, Urteil v. 20.01.2005 – Az. 4 K 2167/04).

Praxishinweis

Nach Ansicht der Verfasser geht es im vorliegenden Urteil nicht um Daten, sondern um Belege. Diese sind in der Regel schwach strukturierte oder unstrukturierte Dokumente (non coded Information) und gerade nicht maschinell auswertbar. Der Versuch, über nicht-mathematische Operationen dennoch eine maschinelle Auswertbarkeit zu erreichen, erscheint konstruiert. Nicht zuletzt deshalb bewegt sich das Urteil außerhalb der bislang herrschenden Literaturmeinung. Wenngleich diese Definitionserweiterung noch für Diskussionsstoff sorgen wird, so sei angemerkt, dass das eigentliche Zugriffsrecht nachvollziehbar und verhältnismäßig erscheint. Dies gilt schon alleine deshalb, weil die vorzulegenden Original-Dokumente vernichtet wurden.

Eine endgültige Entscheidung des BFH steht indes noch aus. Nichts desto trotz sollten Unternehmen, die Originalbelege digitalisieren und anschließend vernichten, ihre jeweilige GDPdU-Strategie gegebenenfalls anpassen, um einen adäquaten Zugriff auf alle steuerrelevanten Daten zu gewährleisten. Was man in diesem Zusammenhang nicht vergessen sollte, ist das Thema der Verfahrensdokumentation. Gerade das Digitalisieren von papierbasierten Eingangsrechnungen verlangt vom Steuerpflichtigen gewisse Sorgfaltspflichten, nicht zuletzt um den Vorsteuerabzug aus den entsprechenden Rechnungen sicherzustellen.

Fazit

Wenngleich die beiden Entscheidungen des Finanzgerichts Düsseldorf nicht rechtskräftig sind und noch eine endgültige Entscheidung seitens des Bundesfinanzhofs aussteht, werden diese nicht ohne Resonanz bleiben. Während die bisherige Rechtsprechung eher in Richtung Unternehmensseite tendierte, verschaffen die beiden nun vorliegenden Entscheidungen der Finanzverwaltung einen deutlichen Rückenwind. Die Unternehmen sollten insbesondere das Urteil betreffend die digitalisierten Originalbelege in ihre künftige GDPdU-Strategie einbeziehen und einen adäquaten Datenzugriff nebst Trennung in steuerlich relevante und irrelevante Unterlagen einplanen.

Vernichtung der Originale beim Scannen von Eingangsrechnungen aus handels- und steuerrechtlicher Sicht

Wolfgang Heinrich, EASY Software AG

Viele Unternehmen scannen ihre in Papierform eingehenden Eingangsrechnungen, archivieren sie elektronisch und vernichten dann die Papieroriginale. Obwohl mitunter Bedenken geäußert werden, ist dieses Verfahren in Deutschland aus handels- und steuerrechtlicher Sicht zulässig, wenn dabei die allgemeinen Regeln zur elektronischen Archivierung kaufmännischer Belege beachtet werden.

Nur in sehr speziellen Ausnahmefällen, z. B. wenn der Unternehmer keine Inlandsumsätze tätigt und dennoch in Deutschland Vorsteuer abziehen will, gilt das so genannte Vorsteuer-Vergütungsverfahren. Dabei müssen dann zwingend die Rechnungsoriginale vorgelegt werden. (§ 62 Abs. 2 UstDV).

Ansonsten ist die elektronische Form der Aufbewahrung von Rechnungen und den anderen Buchführungsunterlagen im Gesetz ausdrücklich gestattet (§§ 239 Abs. 4, 257 Abs. 3 HGB, § 147 Abs. 2 AO); lediglich Bilanzen und Abschlüsse müssen im Original aufbewahrt werden.

Auch aus umsatzsteuerlichen Gesichtspunkten ergibt sich nichts anderes. Das Bundesfinanzministerium stellt dazu in einem Schreiben ausdrücklich fest:

„Die Rechnungen können unter bestimmten Voraussetzungen als Wiedergaben auf einem Bildträger (z. B. Mikrofilm) oder auf anderen Datenträgern (z. B. Magnetband, Diskette, CD-Rom) aufbewahrt werden (vgl. § 147 Abs. 2 AO). Das bei der Aufbewahrung angewandte Verfahren muss den Grundsätzen ordnungsgemäßer Buchführung, insbesondere den Anforderungen des BMF-Schreiben vom 1. Februar 1984 (BStBl I S. 155) und den diesem Schreiben beigefügten „Mikrofilm-Grundsätzen“ sowie den „Grundsätzen DV-gestützter Buchführungssysteme - GoBS-“ (Anlage zum BMF-Schreiben vom 7. November 1995 - BStBl S. 738), entsprechen. Unter dieser Voraussetzung können Originale der Rechnungen grundsätzlich vernichtet werden (vgl. Abschnitt 255 Abs. 2 UStR).“ (BMF-Schreiben vom 29. Januar 2004 - IV B 7 - S 7280 - 19/04 - Randziffer 72).

Bei der elektronischen Archivierung sind allerdings einige wesentliche Punkte unbedingt zu beachten:

- Die Dokumente müssen während der gesamten Aufbewahrungszeit (in der Regel 10 Jahre) jederzeit verfügbar sein und unverzüglich lesbar gemacht werden können. Sie sind vor Verlust und Verfälschung zu schützen. Die Originale dürfen z. B. erst vernichtet werden, nachdem eine Datensicherung der neu archivierten Dokumente erfolgt ist.
- Das gesamte Archivierungsverfahren muss ordnungsmäßig sein, also den Grundsätzen ordnungsmäßiger Buchführung entsprechen. Dies bezieht sich sowohl auf die eingesetzte Technik („revisions-sicheres Archivsystem“) wie auch auf die Organisation der Archivierung beim Anwender. Zur Ordnungsmäßigkeit gehört insbesondere auch eine Verfahrensdokumentation, welche die Technik und die Abläufe nachvollziehbar beschreibt. Die Vorschriften der GoBS und der GDPdU sind zu beachten.
- Eine Abnahme der Archivierungslösung durch einen Wirtschaftsprüfer oder durch eine andere Prüfungsorganisation ist gesetzlich nicht erforderlich, wird aber oft freiwillig zur Erhöhung des Vertrauens in das Verfahren vorgenommen.

Das Finanzministerium vertritt derzeit die Auffassung, dass auch eingescannte Belege dem vollen Datenzugriff gemäß GDPdU unterliegen („Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung“, Stand 15. Januar 2007, Abschnitt I Frage 8). Damit muss der Steuerpflichtige dann auch für die gescannten Belege den Datenzugriff in allen Varianten Z1, Z2 und Z3 ermöglichen, zumindest so lange es keine anderslautenden Gerichtsurteile gibt.

Abschließend muss noch einmal betont werden, dass sich die obigen Aussagen ausschließlich auf gescannte Papierbelege beziehen und nicht auf „originär digitale“ Dokumente im Sinne der GoBS und der GDPdU, bei denen noch weitere Aspekte zu beachten sind. Außerdem geht es hier nur um die handels- und steuerrechtliche Beurteilung nach deutschem Recht.

Eine ganz andere Frage ist der zivilprozessrechtliche Beweiswert einer gescannten Rechnung in Abgrenzung zum Beweiswert des Papieroriginals. Unter diesem Aspekt ist eine gescannte Rechnung genau wie ein Mikrofilm oder eine Fotokopie ein „Beweismittel des Augenscheins“ und unterliegt der „freien Beweiswürdigung“ des Richters; sie ist also keine „Urkunde“. Allerdings ist auch ein Rechnungsoriginal, das nicht von Hand unterschrieben ist (wie dies ja heute meistens der Fall ist), keine Urkunde im Sinne des Gesetzes. Es ist daher jeweils im Einzelfall zu prüfen, ob und ggf. in welchem Ausmaß die Vernichtung der Originale die Beweislage in einem eventuellen Zivilprozess wirklich verschlechtert.

In der Praxis sind zivilgerichtliche Auseinandersetzungen um die Echtheit von Rechnungen höchst selten. Man wird daher sinnvollerweise eine Abwägung zwischen dem wirtschaftlichen Risiko eines geminderten Beweiswerts und den Einsparungen vornehmen, die durch

Vernichtung der Originale erreicht werden. Oft wird es dann in der Praxis zu der Entscheidung kommen, die meisten Originale zu vernichten und allenfalls ausgewählte Rechnungen mit hohen Rechnungsbeträgen zusätzlich als Original in Papierform aufzubewahren.

IDW RS FAIT 3 - Neue Prüfungsrichtlinie für DMS-Lösungen

Thorsten Brand, Senior-Berater Zöller & Partner GmbH

Der IDW RS FAIT 3 ist erschienen. Es handelt sich hierbei um eine Sammlung von Anforderungen an den Betrieb einer DMS-Lösung aus Sicht der Deutschen Wirtschaftsprüfer. Im Gegensatz zu Gesetzen und Verordnungen wurden hier konkrete und DMS-spezifische Regelungen zusammengestellt.

Der erste Entwurf des IDW RS FAIT 3 war bereits seit Mitte 2005 auf der Homepage der IDW verfügbar. Dann dauerte es aber noch fast ein Jahr, bis die endgültige Version verabschiedet wurde. Eine Veröffentlichung in den Fachnachrichten des IDW erfolgte dann im November 2006. Eine Beschaffung über die eigene Wirtschaftsprüfungsgesellschaft sollte aber leicht möglich sein.

Die Inhalte des IDW RS FAIT 3

Die neuen Grundsätze für Wirtschaftsprüfer sind abgeleitet aus dem Handelsgesetzbuch, es werden aber auch andere rechtliche Grundlagen wie die Abgabenordnung, das Umsatzsteuerrecht und die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Lösungen (GDPdU) berücksichtigt. Grob gliedert sich das Dokument in die Abschnitte:

- Darstellung der heutigen Archivierungsverfahren
- Komponenten einer DMS-Lösung
- Rechtliche Grundlagen, wie HGB, AO, GDPdU oder BDSG
- Beschreibung von typischen Einsatzszenarien, wie frühe oder späte Erfassung, Datenarchivierung oder E-Invoicing
- Darstellung der rechtlichen, technischen und organisatorischen Risiken beim Betrieb einer DMS-Lösung
- Anforderungen für den sicheren DMS-Betrieb

Somit ist der IDW RS FAIT 3 keine reine Kriterienammlung oder Prüfliste, sondern eine Mischung von beschreibenden Texten und Anforderungsdefinitionen. Für einen DMS-erfahrenen Anwender sind sicher nur die letzten beiden Abschnitte von Interesse, da hier konkrete Vorgaben für das eigene System vorhanden sind.

Typische Risiken beim DMS-Betrieb

Rechtlich:

- Sicherstellung des Beweiswertes von Dokumenten
- Langfristige Lesbarmachung
- Vernichtungsregeln

Steuerlich:

- Zugriffsmöglichkeiten auf GDPdU-Archive

Organisatorisch:

- Festlegungen für den Betrieb (Erfassung, Administration)
- Falsche oder unzureichende Indizierung
- Falsche oder fehlende Berechtigungen

Technisch:

- Vollständigkeit und Korrektheit von Prozessen
- Nachvollziehbarkeit und Protokollierung
- Sicherstellung der Unveränderbarkeit
- Inkompatibilitäten aufgrund technischer Änderungen während der Aufbewahrungsfrist
- Unzureichende Migrationskonzepte

Von den Grundlagen zu den Details

Aus den in den Grundsätzen ordnungsgemäßer Buchführungssysteme (GoBS) definierten Kriterien für die Ordnungsmäßigkeit der Buchführung und eines Buchführungssystems werden entsprechende Sicherheits- und Betriebsanforderungen für ein DMS abgeleitet. Diese allgemeinen Anforderungen sind:

- Richtigkeit
- Vertraulichkeit und Autorisierung
- Integrität und Authentizität
- Verfügbarkeit
- Unveränderbarkeit

- Nachvollziehbarkeit

Diese Kriterien sind in den GoBS nur sehr allgemein und von wenigen Ausnahmen abgesehen nicht DMS-spezifisch konkretisiert, so dass der sorgfältige Anwender nicht genau weiß, was hier zu tun ist. Sie werden im RS FAIT 3 interpretiert und detailliert.

Beispielsweise wird für das Kriterium Richtigkeit die bildliche und inhaltliche Gleichheit definiert. Auch werden Anforderungen an das Farbscannen und die Brutto-Netto-Image-Verarbeitung beschrieben. Die Problematik des Scannens von AGBs ist ein weiteres praxisnahes Beispiel.

Für das Kriterium Integrität wird auf das Zusammenspiel zwischen Buchhaltungsanwendung und DMS eingegangen, da für die Ordnungsmäßigkeit des DMS häufig auch Teile der Buchhaltungs-anwendung relevant sind. Beispielsweise sind bei der Dokumentenarchivierung mit SAP R/3 die Zugriffskriterien auf Dokumente in den Standard-Archivierungsszenarien nur in den SAP-Tabellen vorhanden, so dass die obigen DMS-relevanten Anforderungen auch für eine Buchhaltungs-anwendung gelten.

Die GoBS aus 1995 leistet hier nichts Vergleichbares, da das Werk mit dem Fokus Buchführung erstellt wurde. Hier wurde allerdings Handlungsbedarf erkannt und im Rahmen einer AWV-Arbeitsgruppe erfolgt eine Überarbeitung dieser Grundsätze. Auch hat sich der VOI e.V. (Verband Organisations- und Informationssysteme) mit der Veröffentlichung der Prüfkriterien für DMS-Lösungen (PK-DML) ebenfalls dem Thema angenommen.

WORM oder nicht WORM: Sicherstellung der Unveränderbarkeit

Mit besonderer Spannung wurden die Regelungen für die Sicherstellung der Unveränderbarkeit erwartet. WORM oder nicht WORM war hier die Frage. Werden also konkrete Anforderungen an die Speichertechnologie formuliert oder überlässt man die Ausgestaltung der Unveränderbarkeit durch Hardware, Software und Organisation dem Betreiber eines DMS?

Die relevante Formulierung ist: Das Kriterium der Unveränderlichkeit verlangt, dass mit Hilfe von technischen und organisatorischen Maßnahmen sichergestellt wird, dass keine nachträglichen Änderungen an elektronisch archivierten Dokumenten und Daten vorgenommen werden.

Es ist also nicht ausschließlich eine Hardware-Technologie gefordert, wie dies die GDPdU für elektronisch signierte Rechnungen fordern. Somit steht es dem Anwender frei, ob er dies durch Hardware-Komponenten wie WORM-Jukeboxen oder WORM-Festplattensysteme oder die DMS-Software selbst sicherstellt.

Eine einfache Speicherung von archivierten Objekten

auf File-Servern ohne besondere Sicherheitsmechanismen ist hier sicher nicht ausreichend, aber kombiniert mit softwaretechnischen Verfahren wie Prüfsummenbildung oder elektronischen Signaturen kann die Unveränderbarkeit gewährleistet werden. In jedem Fall sind organisatorische Regelungen zusätzlich erforderlich, beispielsweise für das Medienhandling, die Erstellung von Sicherheitskopien oder die Berechtigungsvergabe.

DMS-Betrieb konkret

Am Ende des Dokumentes wird dann schließlich der Konkretisierungsgrad erreicht, an dem sich Anwender und Administratoren gut orientieren können. Hier sind interessante Hinweise und Empfehlungen für die Einrichtung und den Betrieb einer DMS-Lösung aufgeführt. Auf wichtige DMS-Prozesse wie Erfassung, Indizierung oder Speicherung/Archivierung wird konkret eingegangen. Hier einige Beispiele:

- Es sind die aufbewahrungspflichtigen Daten und Dokumente inkl. deren Aufbewahrungsfrist, Index- und Erfassungsprofil zu definieren.
- Das Archivierungsverfahren ist für jede Dokumentenart festzulegen (z. B. vor oder nach der Sachbearbeitung) sowie der Archivierungsprozess selbst (z. B. Scanverfahren, Indexierung, Konvertierung).
- Regelungen und technische Verfahren zur Sicherstellung der Vollständigkeit sind zu definieren bzw. zu implementieren. Hierzu zählen beispielsweise eine Doppeleinzugskontrolle bei Scannern, Stapelprotokolle, Konsistenzprüfungen zwischen Buchführungsanwendung und DMS, aber auch technische Protokolle mit Prüfsummen und Job-Informationen.
- Sicherstellung der Lesbarkeit beim Einsatz von automatischen Bildkorrekturverfahren wie Perfect Page oder VRS.
- Bei Systemen mit Eingangs-Cache, bei denen ein zu archivierendes Dokument vor der endgültigen Archivierung beispielsweise in einem Datei-Verzeichnis auf dem Archivserver liegt, müssen entsprechende Sicherheits- und Zugriffsregeln vorhanden sein.
- Für Medien-Handling, Software-Updates, Löschen und Vernichtung von Dokumenten, Datensicherung, Berechtigungsvergabe und Notfallbetrieb werden konkrete Regelungen gefordert.
- Wiederanlauf und Wiederherstellung müssen geregelt, aber auch getestet worden sein.

- Es müssen regelmäßige dokumentierte Tests erfolgen, insbesondere bei hochverfügbar ausgelegten Systemen oder für die Lesbarkeit von Archivmedien.
- Beim Outsourcing muss die Auslagerung von einzelnen Dienstleistungen (z. B. Scannen) oder des gesamten DMS-Betriebes unterschieden werden. Je nach Grad der Auslagerung müssen unterschiedlich umfangreiche Prüfungs- und Kontrollmechanismen vertraglich vereinbart sein.

Bei den obigen Anforderungen geht es nicht immer um Produkteigenschaften, die entwickelt oder hinzugekauft werden können. Vielmehr ist die Festlegung der Verantwortlichkeiten und Kompetenzen in Archivierungsprozessen erforderlich. Schnell kommt man hier auch wieder auf das Thema Verfahrensdokumentation, die bereits in den GoBS von 1995 gefordert wurde. Auch im RS FAIT 3 wird erneut darauf verwiesen, ohne aber die exakten Inhalte zu definieren. Hier hilft meist ein Blick in Veröffentlichungen des VOI e.V. (www.voi.de).

Nachsignieren

Oliver Berndt, B&L Management Consulting GmbH

Immer wieder wird – auch von so genannten Spezialisten – behauptet, dass elektronische Signaturen nur begrenzt gültig wären. Z. T. ergänzt mit der Konkretisierung einer Gültigkeit von 5 Jahren laut Signaturgesetz. Somit müssten Signaturen kontinuierlich erneuert, d.h. nachsigniert werden. Diese Aussage ist jedoch in dieser Form nicht richtig:

Nicht die Signatur, sondern das Zertifikat (der elektronische Personalausweis) ist – meist auf zwei oder drei Jahre – begrenzt. Auf die bereits geleisteten Signaturen hat der Zertifikatablauf keinen Einfluss. So wie traditionell unterschriebene Verpflichtungen und Willenserklärungen auch nicht deshalb ungültig werden, weil der Personalausweis mit dem man sich ursprünglich identifiziert hat, durch ein neues Exemplar ersetzt wurde, gilt auch hier die Signatur weiterhin.

Warum ist das Zertifikat nun begrenzt gültig? Dies ist durch die Verbindung zu den mathematischen Verschlüsselungsverfahren begründet, mit denen die Si-

Fazit

Bei RS FAIT 3 handelt es sich um eine kompakte und konkrete Darstellung zum Thema elektronische Archivierung aus Sicht der Wirtschaftsprüfung. Neben den technischen Anforderungen sind wichtige organisatorische Aspekte (Verfahrensdokumentation, Test-Szenarien, Notfallkonzepte oder das Change-Management) gut berücksichtigt und sinnvoll konkretisiert.

Es ist somit ein klarer Rahmen, der die Diskussion über den ordnungsgemäßen Betrieb sicher erleichtert. Der RS FAIT 3 geht über die allgemeinen Anforderungen der GoBS hinaus und liefert einen ähnlichen Konkretisierungsgrad, wie die Prüfkriterien für DMS-Lösungen (PK-DML) des VOI.

Kritische oder unverhältnismäßige Anforderungen sind im RS FAIT 3 nicht enthalten. Ein vertretbares Maß an IT-Sicherheit und die Beachtung von einigen wichtigen Betriebsregeln sind immer die Voraussetzung für einen ordnungsgemäßen Betrieb. Wenn der Anwender dann noch eine Muster-Verfahrensdokumentation vom DMS-Anbieter bekommt und hier seine eigenen organisatorischen Regelungen einfügt, kann man einer Systemprüfung durch die Wirtschaftsprüfer gelassen entgegen sehen.

gnatur erstellt wird. Durch die Fortschritte der Informationstechnologie wird befürchtet, dass die Algorithmen gebrochen werden und damit unentdeckte Manipulationen der Originaldaten möglich werden könnten. In der Praxis wäre die Vertuschung einer gezielten Manipulation auch mit einem gebrochenen Verschlüsselungsalgorithmus bei weitem nicht trivial, aber eben möglich.

Der Gesetzgeber fordert daher in §17 der Signaturverordnung eine Nachsignatur mitsamt einem Zeitstempel, „wenn diese [Daten] für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind.“ Dabei ist dieser §17 der Signaturverordnung eine offensive Interpretation des §6 des Signaturgesetzes, bei dem es eigentlich um die Unterrichtsverpflichtung der Trust Center gegenüber ihren Kunden geht. Darin heißt es, das Trust Center „hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.“

Es lässt sich trefflich darüber streiten, ob sich daraus eine generelle Verpflichtung zur Nachsignierung ableiten lässt und ob die Vorgabe sinnvoll oder gar notwendig ist. Elektronische Archive sichern ihre Bestän-

de schon seit Jahrzehnten auch ohne Signatur gegen nachträgliche Änderungen. Bei einer der wichtigsten Anwendungen, dem Signatureinsatz bei elektronischen Rechnungen, wird zwar die revisions sichere Archivierung über 10 Jahre, aber kein Nachsignieren verlangt. Trotz alle dem: Wegdiskutieren lässt sich der §17 SigV damit nicht. Als Anwender müssen wir damit leben. Sofern man also signierte Dokumente hat, die längerfristig aufzubewahren sind und über diesen Zeitraum auch einer Signaturprüfung standhalten müssen, muss man sich mit dem Nachsignieren beschäftigen.

Dabei sind die folgenden Punkte wichtig:

1. Nachsignieren verlängert nicht die Signatur, z. B. die Willenserklärung, sondern „friert“ das Gesamt-konstrukt – mitsamt Signatur – ein.
2. Erneute Signatur muss rechtzeitig und mit geeigneten Verfahren erfolgen.
3. Erneute Signatur muss die gleiche Qualitätsstufe haben, wie die Ausgangssignatur.
4. Es ist kein personenbezogenes Zertifikat notwendig, sondern es reicht ein qualifizierter Zeitstempel.
5. Erneute Signatur muss alle vorherigen Signaturen eines elektronischen Dokuments umschließen.
6. Es muss nicht jedes Dokument separat nachsigniert werden, sondern es können komplette Bestände gemeinsam signiert werden.
7. Das Verfahren kann beliebig oft für dieselben Bestände wiederholt werden.
8. Das Verfahren muss vollkommen automatisch ablaufen und auch für sehr große Dokumentmengen geeignet sein.

In der Praxis finden sich derzeit primär zwei Verfahren, die ihre Eignung nachweisen konnten. Einerseits wurden im Rahmen der europäischen und der IETF-Standardisierung die Spezifikationen ETSI TS101733 bzw.

RFC 3126 geboren und andererseits wurde über ein gefördertes Projekt das Konzept „ArchiSig“ geboren.

Das ETSI-Verfahren sichert prinzipiell jede Signatur mit einem Zeitstempel. Es ist somit auch tolerant bezüglich Änderungen der Bestände. Dokumente/Akten können hinzukommen oder gelöscht bzw. ausgelagert werden. Allerdings führt das Verfahren bei sehr großen Beständen zu einem großen Aufwand, der sich zumindest in der Performance niederschlägt. Weiterhin ist es für eingebettete Signaturen schlecht geeignet, was gerade für die beliebten PDF-Signaturen problematisch sein kann. Die genannten Nachteile vermeidet das ArchiSig-Verfahren, in dem es so genannte Hashbäume verwendet. Das heißt es wird nicht das Dokument selbst erneut signiert, sondern der das Dokument kennzeichnende Hashwert (eine Art Prüfsumme). Es wird dabei wiederum ein Hashwert über die Hashwerte vieler Dokumente gebildet, so dass eine Baumstruktur entsteht. Lediglich der oberste Hashwert wird mit einem Zeitstempel gesichert.

ArchiSig bietet damit ein elegantes und performantes Verfahren zum Nachsignieren an. Probleme ergeben sich jedoch bei Veränderungen in den Beständen, weil dann Teile des Baumes ihre Gültigkeit verlieren und neu verarbeitet werden müssen.

Weiterhin hängt das ArchiSig-Verfahren von der längerfristigen Gültigkeit des Hash-Algorithmus ab. Wird somit nicht ein Signatur-Algorithmus, sondern ein Hash-Algorithmus „schwach“, so muss auch ArchiSig direkt auf das Dokument zugreifen und alle abhängigen Werte neu berechnen.

Egal welches Verfahren Verwendung findet, bei den unterschiedlichen Zertifikatslaufzeiten sowie den verschiedensten Algorithmen für Signaturen und Hashwerte, muss dies bei größeren Beständen ein kontinuierlich laufender Prozess sein. Auch wenn das technische Verfahren automatisiert ist, so ist klar, dass es nicht ohne einen organisatorischen Rahmen und Betriebsaufwand funktionieren kann. Damit stellt sich wieder die Eingangsfrage nach dem Sinn. Leider lässt sie sich nur über eine Änderung oder zumindest Konkretisierung der Signaturverordnung beantworten. Hier sind die diversen Interessengruppen gefordert. Als einzelner Anwender bleibt uns leider nur die Bewertung des Risikos einerseits und des Aufwandes andererseits.



Veranstaltungen des CC Steuern und Recht am 26. September 2007 im VOI-Forum der DMS Expo

Peter Seiler, GID GmbH

12:00-12:45

GDPdU – Finanzgerichte erweitern Recht auf Datenzugriff. Aktuelle Urteile. Was sind steuerlich relevante Daten? Welche Mindestauswertungsmöglichkeiten sind bereitzustellen?

Stefan Groß, Peters Schönberger & Partner GbR

Martin Lamm, Peters Schönberger & Partner GbR

12:50-13:35

E-Mail – Haftungsfragen des Informationsmanagements. Welche rechtlichen Auswirkungen haben E-Mails? Rechtsverbindliche Verträge über E-Mail? Haftungsfragen. Fragen des Datenschutzes.

Dr. Jens Bücking, esb Rechtsanwälte

Thorsten Brand, Zöller & Partner GmbH

13:40-14:25

Elektronische Abrechnung – Chancen und Risiken aus praxisorientierter Sicht. Thesen zur Signatur und Abrechnung, werden auf ihre Fakten und die Bedeutung in der Praxis hin überprüft.

Oliver Berndt, B& L Management Consulting GmbH

Walter Steigauf, UnITeK GmbH