Experten erläutern die GoBD

Ausgabe 4:

– Was bedeutet „Unveränderbarkeit“? –

20. Januar 2016

Peters, Schönberger & Partner mbB

Schackstraße 2, 80539 München

Tel.: +49 89 381720

Internet: www.psp.eu

Autoreninformationen:

- ***Stefan Groß**, Partner und Steuerberater*
  bei Peters, Schönberger & Partner mbB
- ***Dipl.-Fw. Bernhard Lindgens**,*
  Bundeszentralamt für Steuern[1]
- ***Bernhard Zöller**, Geschäftsführer*
  bei Zöller & Partner GmbH
- ***Thorsten Brand,** Senior Berater*
  bei Zöller & Partner GmbH
- ***Stefan Heinrichshofen**, Partner, Rechtsanwalt und Steuerberater*
  bei Peters, Schönberger & Partner mbB

[1] Der Beitrag wurde nicht in dienstlicher Eigenschaft verfasst.

Was bedeutet „Unveränderbarkeit“?

Mit dem Schreiben vom 14. November 2014, den „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (***GoBD***)“, hat das BMF dargelegt, welche Vorgaben aus Sicht der Finanzverwaltung an IT-gestützte Prozesse zu stellen sind.[2] Die GoBD sind für Veranlagungszeiträume anzuwenden, die nach dem 31. Dezember 2014 beginnen und betreffen grundsätzlich alle Steuerpflichtigen mit Gewinneinkünften i. S. d. § 5 EStG, § 4 Abs. 1 EStG sowie auch nicht buchführungspflichtige Unternehmen, wie insbesondere Einnahmen-Überschuss-Rechner[3]. Die ***Verantwortung*** für die Ordnungsmäßigkeit elektronischer Bücher und sonst erforderlicher elektronischer Aufzeichnungen, einschließlich der Verfahren, trägt allein der Steuerpflichtige. Dies gilt auch bei einer teilweisen oder vollständigen organisatorischen und/oder technischen Auslagerung von Buchführungs- und Aufzeichnungspflichten auf Dritte, wie auch etwa Steuerberater (***Outsourcing***).[4]

Nach § 146 Absatz 4 AO darf eine Buchung oder Aufzeichnung nicht in einer Weise ***verändert*** werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Dazu dürfen keine Veränderungen vorgenommen werden, die keinen Rückschluss darauf zulassen, ob sie ursprünglich oder erst später initiiert wurden.[5] Das zum Einsatz kommende DV-Verfahren muss Gewähr dafür bieten, dass alle Informationen (Programme und Datenbestände), die einmal in den Verarbeitungsprozess eingeführt werden (Beleg, Grundaufzeichnung, Buchung), nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden können. Bereits in den Verarbeitungsprozess eingeführte Informationen (Beleg, Grundaufzeichnung, Buchung) dürfen nicht ohne Kenntlichmachung durch neue Daten ersetzt werden.[6]

[2] BMF v. 14. November 2014 – IV A 4 – S 0316/13/10003, BStBl. I 2014, S. 1450.
[3] Steuerpflichtige, die ihren Gewinn nach den Vorschriften des § 4 Abs. 3 EStG ermitteln.
[4] GoBD (Fn. 2), Rn. 21.
[5] GoBD (Fn. 2), Rn. 107.
[6] GoBD (Fn. 2), Rn. 108.

Die Unveränderbarkeit der Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen kann sowohl hardwaremäßig (z. B. unveränderbare und fälschungssichere Datenträger) als auch softwaremäßig (z. B. Sicherungen, Sperren, Festschreibungen, Löschmerker, automatische Protokollierung, Historisierungen, Versionierungen) oder organisatorisch (z. B. mittels Zugriffsberechtigungskonzepten) gewährleistet werden.[7] Die Ablage von Daten und elektronischen Dokumenten in einem ***Dateisystem*** erfüllt die Anforderungen der Unveränderbarkeit regelmäßig nicht, soweit nicht zusätzliche Maßnahmen ergriffen werden, die eine Unveränderbarkeit gewährleisten.[8]

Gerade bei der Diskussion über die Umsetzung der Unveränderbarkeit ist aber auch der folgende Hinweis der GoBD wichtig: Technische Vorgaben oder Standards (z. B. zu Archivierungsmedien oder Kryptografieverfahren) können angesichts der rasch fortschreitenden Entwicklung und der ebenfalls notwendigen Betrachtung des organisatorischen Umfelds nicht festgelegt werden.[9]

Soweit die Formulierungen und Anforderungen aus den GoBD.
Doch was bedeuten diese Vorgaben im Einzelnen?

Bei der Auseinandersetzung mit den Vorgaben zur Unveränderbarkeit sind insbesondere die folgenden Aspekte in die Betrachtung einzubeziehen:

- Unveränderbarkeit vs. Nachvollziehbarkeit
- Technische Maßnahmen zur Sicherstellung der Unveränderbarkeit
- Formate der Aufbewahrung
- Nachvollziehbarkeit von Stammdaten und Systemeinstellungen

[7] GoBD (Fn. 2), Rn. 110.
[8] GoBD (Fn. 2), Rn. 110.
[9] GoBD (Fn. 2), Rn. 10.

Unveränderbarkeit vs. Nachvollziehbarkeit

„Eine Buchung oder Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Zudem dürfen keine Veränderungen vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind“.[10] Vor diesem Hintergrund fordern die GoBD, dass das eingesetzte DV-Verfahren so auszugestalten ist, dass alle Informationen, welche in den Verarbeitungsprozess Eingang gefunden haben (Beleg, Grundaufzeichnung, Buchung), nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden können.[11] Veränderungen und Löschungen von und an elektronischen Buchungen oder Aufzeichnungen müssen daher so protokolliert werden, dass die Voraussetzungen des § 146 Abs. 4 AO bzw. § 239 Abs. 3 HGB erfüllt sind. Für elektronische Dokumente und andere elektronische Unterlagen, die gemäß § 147 AO aufbewahrungspflichtig und keine Buchungen oder Aufzeichnungen sind, gilt dies sinngemäß.[12]

Technische Maßnahmen zur Sicherstellung der Unveränderbarkeit

Die geforderte Unveränderbarkeit und Nachvollziehbarkeit kann sowohl mittels geeigneter Hardware oder Software wie auch organisatorisch gewährleistet werden. Dabei darf sich die Sicherstellung der Unveränderbarkeit nicht isoliert auf den Speichervorgang beschränken. Vielmehr müssen an unterschiedlichen Komponenten und Prozessen Sicherheitsmechanismen zur Verfügung stehen, die eine unkontrollierte Veränderung von Informationen unterbinden[13] und die zeitliche Abfolge von Veränderungen nachweisen (z. B. durch Zeitstempel im Buchhaltungssystem oder der Warenwirtschaft). Im Kontext von Speichersystemen wird in den GoBD die zentrale Aussage getroffen, dass die bloße Ablage elektronischer Unterlagen in einem ***Dateisystem*** die Anforderungen der Unveränderbarkeit regelmäßig nicht erfüllt, soweit nicht zusätzliche Maßnahmen ergriffen werden.[14]

[10] GoBD (Fn. 2), Rn. 58.
[11] GoBD (Fn. 2), Rn. 108.
[12] GoBD (Fn. 2), Rn. 59.
[13] Vgl. Brand/Groß/Geis/Lindgens/Zöller, Steuersicher archivieren, S. 52 f.
[14] GoBD (Fn. 2), Rn. 110.

Damit erfüllt jedoch das gerade in der Unternehmenspraxis gängige Vorgehen, einzelne Dateien (z. B. ***PC-Dokumente mit steuerrelevanten Daten***) im Dateisystem abzulegen, nicht ohne weitere Maßnahmen die in den GoBD geforderten Ordnungsmäßigkeitsanforderungen.

Die Ablage in einem Dateisystem kann grundsätzlich zwar beibehalten werden, erfordert jedoch ergänzende Maßnahmen, wie z. B. eine Kombination aus regelmäßigen Sicherungen, Zugriffsschutzmechanismen, Kopien auf nur einmal beschreibbare Datenträger, Entzug von Schreibrechten sowie insbesondere eine Verfahrensdokumentation mit Erläuterung der spezifischen Kontrollmechanismen. Entsprechendes gilt für die reine Aufbewahrung von aufbewahrungspflichtiger ***E-Mail***-Korrespondenz innerhalb des Mail-Systems ohne jegliche zusätzliche Sicherungsmaßnahmen.

Bezogen auf Speichersysteme existieren Lösungen, welche die Unveränderbarkeit auf ***technischer Ebene*** sicherstellen. In der Vergangenheit basierten diese Systeme im Regelfall auf optischen WORM-Medien (z. B. UDO, CD, DVD etc.). Mittlerweile werden hierzu festplattenbasierte Systeme mit Softwareschutz eingesetzt (z. B. EMC Centera, Netapp Snaplock, FAST LTA etc.). Der Einsatz dieser Produkte ist zwar nicht gesetzlich vorgeschrieben, kann jedoch dazu beitragen, die Umsetzung der Vorgaben an die Unveränderbarkeit zu unterstützen.

Auf der Ebene von ***Software*** bietet sich in Abhängigkeit von der Unternehmensgröße und Komplexität der Einsatz dedizierter Aufbewahrungs- bzw. Archivsysteme (z. B. ***Dokumentenmanagementsysteme***) an, mit denen der Nachweis der Unveränderbarkeit bzw. der Nachvollzug von Änderungen entsprechend geleistet werden kann. Diese System unterstützen entweder die oben beschriebenen Archivspeicher oder sie besitzen eigene Sicherheitsmechanismen, die die Unveränderbarkeit und Nachvollziehbarkeit unterstützen. Dies sind beispielsweise:

- Berechtigungskonzepte und Änderungsschutz im Produkt (zusätzlich zum Betriebssystem), sodass keine unberechtigten Änderungen durchgeführt werden können,
- Versionierungsfunktionen, sodass Dokumente nicht überschrieben, sondern als neue Version abgelegt werden,
- Protokollierung von Änderungsaktion an Dokumenten, Daten und Systemeinstellungen,
- Zusatzfunktionen zur Nachvollziehbarkeit von Änderungen (z. B. Hashwerte, Zeitstempel) oder
- Anbindungsmöglichkeiten von unveränderbaren Speichersystemen.

Häufig findet sich auch eine Kombination aus WORM-Archivspeicher und weitergehenden Schutzfunktionen im DMS.

Die Software-basierten Schutzfunktionen sind dabei stets durch ***organisatorische Regelungen*** (z. B. Vier-Augen-Prinzip bei der Administration, regelmäßige Audits, Zugangskontrollen, Arbeitsanweisungen Systembetrieb etc.) zu ergänzen. Nur so kann im Rahmen der unternehmensindividuellen Implementierung sichergestellt werden, dass die getroffenen hard- und softwaretechnischen Maßnahmen auch umgesetzt werden.

Formate der Aufbewahrung

Die Anforderung der Unveränderbarkeit betrifft sowohl Daten als auch Dokumente, die originär elektronisch, inhaltlich oder bildlich identisch aufbewahrt werden müssen. Werden originär elektronische Dokumente als MS Word- oder MS Excel-Dokument ausschließlich im Dateisystem abgelegt, könnte bereits eine Unachtsamkeit dazu führen, dass unzulässige Änderungen vorgenommen werden. Insbesondere Excel-Formeln oder Word-Datumsfelder aktualisieren sich i. d. R. bereits beim Öffnen dieser Dateien. Wurden die elektronischen Unterlagen hingegen in eine PDF- oder TIFF-Datei umgewandelt, sind zwar ebenfalls „Manipulationen“ möglich – hierzu genügen Bordmittel eines normalen PCs – allerdings muss eine inhaltliche Manipulation absichtlich erfolgen. Damit wird letztlich auch deutlich, dass die Um-

wandlung in vermeintliche „Langzeitformate“ zwar der versehentlichen oder fahrlässigen Manipulation vorzubeugen vermag, nicht jedoch Veränderungen grundsätzlich ausschließt. Auch ist sicherzustellen, dass bei der Konvertierung in solche Formate nicht steuerrelevante, aufbewahrungspflichtige Informationen verloren gehen. Wird die Reisekostenabrechnung mit der Formel für die Verpflegungspauschale in PDF konvertiert, geht die Prüfbarkeit der Formel verloren und nur die Ergebnisse sind dauerhaft lesbar, jedoch nicht mehr deren Herleitung. Vorab sollte daher stets geprüft werden, ob einer Formatwandlung keine steuerrechtlichen Vorgaben – insbesondere im Kontext der digitalen Betriebsprüfung – entgegenstehen. Ist dies nicht der Fall, sind Formatumwandlungen grundsätzlich zulässig und in der Praxis – etwa beim Produktwechsel eines DMS-Produktes – sogar erforderlich. Beispiele für zulässige Formatumwandlungen in diesem Zusammenhang sind:

- Konvertierung von Single-Page TIF in Multi-Page TIF
- Konvertierung von TIF- oder JPG-Dateien in PDF
- Konvertierung von PDF-Dateien in PDF/A
- Änderung des Kompressionsverfahrens innerhalb eines Formates

Es geht bei der Sicherstellerung der Unveränderbarkeit u. E. damit nicht um die Unveränderbarkeit der binären Daten. Diese dürfen sich durchaus ändern, wenn es hierbei zu keinem Verlust an Informationen kommt (Lesbarkeit, maschinelle Auswertbarkeit etc.). Um dabei den Anforderngen an die Nachvollziehbarkeit und Nachprüfbarkeit zu entsprechen, sollte der Umwandlungsprozess dazu zwingend in der Verfahrensdokumentation beschrieben sein. Zu den ergänzenden Anforderungen der GoBD an die Konvertierung, insbesondere an die Aufbewahrung im Konvertierungsfall, verweisen wir auf unseren gesonderten Beitrag ***„Was bedeutet Konvertierung“***.[15]

Exkurs Signatur: In Bezug auf den Einsatz elektronischer ***Signaturen*** herrscht häufig die Meinung vor, Dokumente müssten im elektronischen Archiv mit einer elektro-

[15] Verfügbar unter: *https://www.psp.eu/media/in-public/Beitrag_Expertenerlaeuterungen_GoBD_Konvertierung.pdf*.

nischen Signatur versehen sein, um die Unveränderbarkeit zu garantieren. Tatsächlich kann eine elektronische Signatur jedoch keine Schutzfunktion übernehmen oder die Unveränderbarkeit sicherstellen. Sie bietet lediglich die nachträgliche Möglichkeit nachzuweisen, von wem die Signatur stammt und ob die signierte Datei verändert wurde (sofern sie nicht gelöscht wurde, weil sie nicht in einem entsprechenden Schutzsystem aufbewahrt wurde). Art und Inhalt der Änderung kann durch eine Signatur jedoch nicht nachvollzogen werden. Dies gilt auch für einen elektronisch ermittelten Fingerabdruck (engl. „Hashwert“), bei dem eine Prüfsumme für eine Datei erstellt wird, der sich bei einer Änderung der Datei verändert. Aus rein steuerlicher Sicht ist die elektronische Signatur für archivierte Dokumente nicht erforderlich. [16]

Nachvollziehbarkeit von Stammdaten und Systemeinstellungen

Die GoBD adressieren auch die Nachvollziehbarkeit von Änderungen an ***Stammdaten***, ***Einstellungen*** oder der ***Parametrisierung*** der Software. Bei der Änderung von Stammdaten (z. B. Abkürzungen oder Schlüssel) muss die eindeutige Bedeutung in den entsprechenden Bewegungsdaten erhalten bleiben.[17] Beispiele hierfür sind:

- Änderungen an Kunden- oder Lieferantenstammdaten führen auch zu Änderungen an den Daten, die nicht mehr verändert werden dürfen.
- Änderungen an Basisdaten im ERP-System, wie Steuersätze, Geschäftsführer etc. schlagen auf die alten Belege durch.

Gegebenenfalls müssen ***Stammdatenänderungen*** in bereits archivierten Unterlagen daher ausgeschlossen oder Stammdaten mit Gültigkeitsangaben historisiert werden, um eindeutige und korrekte Verknüpfungen zu gewährleisten. Auch die Änderungshistorie darf nicht nachträglich veränderbar sein.[18]

[16] Auch führen die GoBD im Kontext der Digitalisierung von Papierbelegen aus, dass für Besteuerungszwecke eine elektronische Signatur nicht erforderlich ist, GoBD (Fn. 2), Rn. 138.
[17] GoBD (Fn. 2), Rn. 111.
[18] GoBD (Fn. 2), Rn. 111.

Dieser Vorgabe ist insbesondere dann Rechnung zu tragen, wenn rückwirkend bestimmte Ausgangsbelege ***reproduziert*** werden sollen.[19] Hier bedarf es zwingend der historischen Stammdaten. Da die Nutzung historisierter Stammdaten jedoch nicht trivial ist, empfiehlt es sich in der Praxis, die entsprechenden Ausgangsbelege zum Zeitpunkt der Erstellung in einem Archivformat (z. B. PDF) der Aufbewahrung zuzuführen und insoweit auch eine Migrationsunabhängigkeit zu schaffen.

Weiter verlangt die Unveränderbarkeit eine ***Protokollierung*** sämtlicher Veränderungen und Löschungen von Daten und Datensätzen, sofern sich die Löschung/ Änderung auf aufbewahrungspflichtige Inhalte bezieht. Vor dem Hintergrund, dass hiervon auch sämtliche Vor- und Nebensysteme betroffen werden, geht damit im Ergebnis eine Protokollierung sämtlicher Datenveränderungen einher, was zu einem unverhältnismäßig hohen Aufwand auf Unternehmensseite führen kann. Jedenfalls sollte bei Änderungen zumindest erkannbar bleiben, durch wen (Benutzer, Prozess) eine Änderung vorgenommen wurde.

In Bezug auf die Nachvollziehbarkeit von Systemeinstellungen sind insbesondere die administrativen Bereiche und Berechtigungen ins Kalkül zu ziehen. Die entsprechenden Einstellungen und Parametrisierungen unterliegen dabei zumeist den entsprechenden ***Administratoren***, die stets mit besonderen Rechten ausgestattet sind. Dies können beispielsweise Administratoren für Datenbanken, Anwendungen, Filesysteme oder zentrale Berechtigungssysteme sein. Die Sicherstellung der Unveränderbarkeit und Nachvollziehbarkeit ist in diesem Bereiche grundsätzlich nur beschränkt mit hard- und/oder softwaretechnischen Mechanismen möglich. Die typischen Risiken sind insbesondere:

- Löschen von Dateien unter Umgehung des Berechtigungsystems und der Schutzmechanismen der verwaltenden Anwendung,
- Änderung von Datenbankeinträgen direkt im Datenbanksystem oder
- Änderung von Protokollen, die die Nachvollziehbarkeit sicherstellen.

[19] Gem. § 147 Abs. 2 Nr. 1 AO bedürfen Ausgangsbelege einer inhaltlichen Übereinstimmung mit dem Original, wenn sie lesbar gemacht werden.

Dabei gilt es zu beachten, dass Administratoren hier stets einen besonderen Vertrauensschutz besitzen. Dennoch sollten entsprechende Arbeitsanweisungen und Prozesse etabliert sein, welche dazu beitragen, die Vertrauenswürdigkeit des Prozesses zu gewährleisten. So kann etwa durch ein Vier-Augen-Prinzip eine unkontrollierte Änderung durch eine Person vermieden werden. Auch reduziert die Aufteilung von administrativen Tätigkeiten auf mehrere Personen das Risiko. Zuletzt kann über entsprechende Protokollierungen sowie deren regelmäßige Einsichtnahme eine kompensierende Kontrolle die Prozess-Sicherheit verbessern. Fehlen hierfür die personellen Kapazitäten (Kleinunternehmen), so sollte der Mangel durch technische Komponenten, die die Unveränderbarkeit sicherstellen können, kompensiert werden (kompensatorische Kontrollmaßnahmen).

Fazit

Die Umsetzung der in den GoBD beschriebenen Anforderungen an die Unveränderbarkeit ist stets in Abhängigkeit von den individuellen Rahmenbedingungen sowie der Umsetzung im Unternehmen zu beurteilen. Dabei gilt zunächst, dass es nicht die EINE Lösung zur Sicherstellung der Unveränderbarkeit gibt. Unveränderbare Speichersysteme sind dabei durchaus geeignet, die Umsetzung der Unveränderbarkeit zu unterstützen, sind aber weder zwingende Voraussetzung, noch für sich alleine genommen ausreichend, um den Vorgaben der GoBD vollumfänglich gerecht zu werden. Auch existieren keine unveränderbaren Formate, die isoliert eine tragfähige Lösung darstellen können. Die Formatwahl kann wiederum nur unterstützend wirken. Vielmehr sind die elektronischen Daten und Dokumente an sich stets mit zusätzlichen Mitteln zu sichern, die wiederum unternehmensindividuell ausgestaltet sein können. Über einen reinen Hard- und Softwareschutz hinaus, bedarf es insbesondere entsprechender organisatorischer Regelungen zur Sicherstellung der Prozess-Sicherheit, welche letztlich in Arbeitsanweisungen und einer Verfahrensdokumentation niedergelegt sind.

Bisherige Ausgaben der GoBD-Reihe „Experten erläutern die GoBD“:

- Was bedeutet „Zeitgerechtheit“?
- Was bedeutet „Konvertierung“?
- Was bedeutet „mobiles Scannen“?
- Was bedeutet „Unveränderbarkeit“?

Vorschau weiterer Themen der GoBD-Reihe „Experten erläutern die GoBD“:

- Was bedeutet „Ablage im File-System“?
- Was bedeutet „Maschinelle Auswertbarkeit“?
- Was bedeutet „Progressive und retrograde Prüfbarkeit“?
- Was bedeutet „Ersetzendes Scannen?“
- Was bedeutet „Migrationen und Systemabschaltungen?“

Die bereits veröffentlichten Ausgaben der GoBD-Expertenerläuterungen sind verfügbar unter: **www.gobd.de/expertenerlaeuterungen**