CB-BEITRAG

Dipl.-Wirtschaftsinformatiker Rüdiger Giebichenstein und Dipl.-Ing. Carsten Alexander Schirp

Die GoBD – neue Verwaltungsvorschriften für die IT-gestützte Buchführung

Die seit dem 1.1.2015 geltenden Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (kurz GoBD) beschreiben, wie sich die Finanzverwaltung eine zeitgemäße IT-gestützte Rechnungslegung und die Verwaltung von steuerlichen und außersteuerlichen Aufzeichnungen vorstellt. Es ist zu erwarten, dass die neuen Vorgaben mit nicht zu unterschätzenden Anpassungen der rechnungslegungsrelevanten Geschäftsprozesse und IT-Systeme für weite Teile der deutschen Unternehmenslandschaft einhergehen werden. Der folgende Artikel erläutert die wesentlichen Neuerungen und Herausforderungen der GoBD und liefert Empfehlungen, um diesen erfolgreich zu begegnen.

I. Was sind die GoBD?

Die am 14.11.2014 veröffentlichten GoBD stellen eine Meinungsäußerung des Bundesministeriums der Finanzen (kurz BMF) in Form eines Schreibens dar.[1] Durch sie formuliert das BMF seine Vorgaben und Regelungen an eine ordnungsmäßige IT-gestützte Buchführung. Gegenüber den nachgeordneten Dienststellen sind die GoBD als eine Verwaltungsvorschrift mit Verbindlichkeitscharakter zu verstehen. Sie sind am 1.1.2015 in Kraft getreten und gelten damit für alle Veranlagungszeiträume nach dem 31.12.2014. Durch sie werden die bisher bestehenden Regelungen, die GoBS[2] und die GDPdU,[3] abgelöst. Durch die GoBD wird einerseits die bereits bestehende Rechtslage und Rechtsprechung aufgegriffen und teilweise anhand von anschaulichen Beispielen wiedergegeben. Andererseits stellen die neu formulierten Anforderungen an die ordnungsmäßige IT-gestützte Buchführung auch eine logische Fortentwicklung bereits bestehender Regelungen dar. Die Finanzverwaltung folgt damit auch der Forderung der Wirtschaftsverbände und steuerberatenden Berufe nach der dringend benötigten Modernisierung und Klarstellung bzw. Konkretisierung der Rechtslage u. a. in Bezug auf zwischenzeitlich stattgefundene rechtliche, prozessuale oder technische Entwicklungen.

Dennoch enthalten die GoBD auch weitergehende Anforderungen, die sich bislang nicht oder nur unzureichend in der unternehmerischen Wahrnehmung und betrieblichen Praxis widerspiegelten. Damit wird deutlich, dass die lange gewährte „Schonfrist" durch Betriebsprüfer zur revisions- und manipulationssicheren Rechnungslegung und digitalen Buchprüfung voraussichtlich enden wird. Handlungsbedarf in vielen Unternehmen zur Einhaltung der neuen Vorgaben und Regelungen zeichnet sich damit ab, um Konflikten mit Betriebsprüfern vorzubeugen und Sanktionen zu vermeiden.

II. Wer ist betroffen und verantwortlich?

Die GoBD sind für alle Veranlagungszeiträume anzuwenden, die nach dem 31.12.2014 beginnen und betreffen grundsätzlich alle Steuerpflichtigen, die Bücher oder Aufzeichnungen ganz oder teilweise elektronisch führen oder erfassen. Die Steuerpflicht kann sich dabei sowohl aus dem Bereich der Ertragssteuern als auch aus den Objekt- oder Verkehrssteuern ergeben. Damit sind zwingend auch sog. Einnahmen-Überschuss-Rechner sowie Freiberufler im Geltungsbereich der GoBD mit eingeschlossen.[4]

Die GoBD gelten aber auch dann, wenn der Steuerpflichtige seine Betriebsabläufe freiwillig elektronisch abbildet, ohne dazu verpflichtet zu sein.[5] Effektiv kann somit davon ausgegangen werden, dass nahezu die gesamte deutsche Unternehmenslandschaft betroffen ist, was nicht zuletzt auch zu den Zielen des BMF gehört, die mit der GoBD verfolgt werden.

Wichtig zu beachten bleibt in jedem Falle, dass der Steuerpflichte auch dann die Verantwortung für die Einhaltung der GoBD trägt, wenn die Aktivitäten zur Aufzeichnung oder Buchführung ganz oder teilweise an externe Dienstleister ausgelagert sind.

Die GoBD konkretisieren neben rechtlichen und prozessualen Anforderungen auch wie eingangs erwähnt Anforderungen und Regelungen in Bezug auf die zur Buchhaltung eingesetzten IT-Systeme. Von den GoBD betroffen sind allerdings nicht nur die primären Buchführungssysteme (z. B. SAP, Microsoft usw.), sondern auch alle sonstigen rechnungslegungsrelevanten Vor- oder Nebensysteme im Unternehmen wie z. B. Warenwirtschaftssysteme, elektronische Kassen oder Waagen, Taxameter, Lohnbuchführungs- und Zeiterfassungssysteme o. ä.,[6] da diese Systeme im direkten prozessualen wie technischen Zusammenhang mit dem primären Buchführungssystem agieren.

Außerdem gelten die GoBD nicht nur für sämtliche steuerliche Aufzeichnungspflichten, sondern auch für alle außersteuerlichen, die sich aus sonstigen handelsrechtlichen oder branchenspezifischen Aufzeichnungspflichten ergeben können.[7]

1 BMF-Schreiben v. 14.11.2014, abrufbar unter www.bundesfinanzministerium.de.
2 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS).
3 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).
4 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 25.
5 Vgl. § 140 AO.
6 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 20.
7 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 3.

III. Allgemeine Anforderungen an die IT-gestützte Buchführung

Die GoBD folgt in Aufbau und Struktur weitgehend einem idealisierten Buchungsprozess und greift dabei die einschlägigen Ordnungsvorschriften wie den Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit[8], die Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung[9] und den Grundsatz der Unveränderbarkeit[10] auf, um die Anforderungen an die IT-gestützten Prozesse zu formulieren.
Die Anforderungen an die Datensicherheit, die Verfahrensdokumentation und das interne Kontrollsystem (IKS) bilden die Grundlage für die Durchführung der eigentlichen Buchhaltungs- und Aufzeichnungsprozesse. Diese werden im Folgenden weiter erläutert und spezifiziert.
Aufgrund der rasch voranschreitenden Entwicklungen im IT-Bereich ist die GoBD selbst frei von technischen Spezifikationen und konkreten Bezügen zu marktüblichen Softwareprodukten (z. B. SAP, Microsoft usw.) gehalten. Offene Fragen zur Umsetzung der Anforderungen sollen stattdessen durch einen sog. Analogieschluss beantwortet werden. Dabei soll durch einen Vergleich mit einer handschriftlich geführten Buchführung festgestellt werden, ob die Ordnungsvorschriften eingehalten werden.

IV. Verfahrensdokumentation

Die GoBD legen nicht zuletzt durch 20 explizite textuelle Erwähnungen einen besonderen Fokus auf die sog. Verfahrensdokumentationen. Durch Verfahrensdokumentationen sind die organisatorisch und technisch gewollten Prozesse, wie z. B. Belege erfassen, empfangen, verarbeiten, ausgeben und aufbewahren, nachvollziehbar zu beschreiben. Die Betriebs- und Geschäftsabläufe sollen sich durch die Verfahrensdokumentationen einem sachverständigen Dritten, wie dem Betriebs- oder Wirtschaftsprüfer, in angemessener Zeit erschließen lassen. Ist dies aufgrund unvollständiger oder unverständlicher Dokumentation nicht möglich, so kann das zur Verwerfung der Buchführung führen. Dabei ist außerdem darauf zu achten, dass die Dokumente stets auf dem aktuellen Stand zu halten sind und anlassbezogen, z. B. bei technischen, prozessualen oder organisatorischen Änderungen, zu überprüfen und wenn notwendig, anzupassen sind. Im Rahmen der Anpassung ist auch eine Historisierung in der Art vorzunehmen, dass sich der aktuelle Stand der Dokumentation für ein beliebiges Datum rekonstruieren lässt.
Zum Umfang der Verfahrensdokumentationen gehören außerdem die Beschreibung der Vorgehensweisen zur Einhaltung der Datensicherheit (siehe Kapitel V.) sowie die Wirkungsweise des internen Kontrollsystems (siehe Kapitel VI.). Für die im Rahmen der Buchführung eingesetzten IT-Systeme und deren betrieblichen Prozesse sind konkretisierend Verfahrensbeschreibungen und Dokumentationen vorzuhalten, u. a. zur Beschreibung der eingestellten Programmlogik, der betrieblichen Abläufe (u. a. Umgang mit Benutzern und Berechtigungen, Änderungs- und Entwicklungsmanagement, Datensicherheit, Datensicherung und Wiederherstellung, Archivierung usw.) und der fachlichen Endanwenderdokumentation zur Nutzung.

V. Datensicherheit

Typischerweise ist das Ziel der IT- und Datensicherheit (umfassender auch Informationssicherheit genannt) die Einhaltung der Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität, welche neben Normen wie der ISO 27001:2013[11] auch von den GoBD direkt oder indirekt genannt werden. Direkte Vorgaben stellen die GoBD an die Verfügbarkeit. Vorgaben an die Integrität und Vertraulichkeit ergeben sich indirekt aus den fachlichen Anforderungen zur Handhabung der aufzeichnungspflichtigen Unterlagen. Die daraus, sowie aus weiteren Regelwerken und Gesetzen resultierenden vielschichtigen Anforderungen an die IT- und Datensicherheit, sind für die meisten Unternehmen heute ohnehin unternehmerischer Alltag. Diese gilt es verpflichtend umzusetzen und einzuhalten.
Um IT- und Datensicherheit (zusammengefasst als Informationssicherheit) ganzheitlich im Unternehmen abbilden zu können, ist auch, abhängig vom Komplexitätsniveau der Geschäftstätigkeit, der Aufbau eines sog. Informationssicherheitsmanagementsystems (ISMS), z. B. nach dem Vorbild der ISO 27001, empfehlenswert bis unabdingbar.[12]

1. Verfügbarkeit

Eine der Grundvoraussetzungen für eine funktionsfähige IT-gestützte Buchführung ist die Verfügbarkeit der Daten, die für die Dauer der gesamten Aufbewahrungsfrist eingehalten werden muss. Es empfiehlt sich daher, organisatorische und technische Maßnahmen zum Schutz der Daten zu treffen. Denn wenn Unterlagen aufgrund unzureichender oder unangemessener Schutzmaßnahmen dem Betriebsprüfer nicht mehr vorgelegt werden können, droht schlimmstenfalls die Verwerfung der gesamten Buchführung.[13]

2. Integrität

Dem Grundsatz der Unveränderbarkeit nach dürfen die aufzeichnungspflichtigen Informationen nicht in der Weise verändert werden, dass ihr ursprünglicher Inhalt und zugefügte Änderungen nicht mehr nachvollziehbar sind. Dieser Grundsatz wird auch als sog. „Radierverbot“ bezeichnet. Für dessen Gewährleistung bedeutet das, dass Informationen einerseits durch technisch-organisatorische Maßnahmen wie Zugriffs- und Berechtigungsbeschränkungen (z. B. in SAP keine Vergabe von Debugging-Berechtigungen in Produktionssystemen) gegen unautorisierte Eingaben und Veränderungen (sog. „elektronisches Radieren“) zu schützen sind. Weiterhin sind technische Maßnahmen zu treffen, um die Nachvollziehbarkeit von Änderungen z. B. durch eine angemessene Protokollierung unterstützen zu können. Eine Möglichkeit der elektronischen Umsetzung der Unveränderbarkeit bietet der Einsatz von sog. WORM-Speicher-Systemen.[14]

Exkurs: WORM-Speicher
Durch die GoBD wird nicht mehr ausschließlich eine Hardware-Technologie (z. B. optische Medien wie CDs oder DVDs) gefordert. Stattdessen steht es dem Steuerpflichtigen nun frei, die WORM-Eigenschaft systemisch oder softwareseitig (z. B. CAS-Speichersysteme[15]) zu organisieren. Allerdings kann dabei die Unveränderbarkeit nicht vollständig bewiesen werden, und durch das Ausnutzen

8 Vgl. § 145 Abs. 1 AO bzw. § 238 Abs. 1 HGB.
9 Vgl. § 146 Abs. 1 AO bzw. § 239 Abs. 2 HGB.
10 Vgl. § 146 Abs. 4 AO bzw. § 239 Abs. 3 HGB.
11 ISO/IEC 27001:2013 spezifiziert die Anforderungen für Erstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines Informationssicherheits-Managementsystems (ISMS).
12 Zum Aufbau eines ISMS: *Giebichenstein/Schirp*, CB 2015, 108.
13 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 103, 104.
14 WORM („write once read many“ oder „write once read multiple“).
15 CAS (Content-Addressed Storage).

von Sicherheitslücken ist ggf. eine Verletzung der Unveränderbarkeit möglich. Die meisten optischen Speichermedien, wie z. B. CDs oder DVDs, haben hingegen den Nachteil, dass ihre physische Haltbarkeit für die gesamte Aufbewahrungsfrist, u. a. aufgrund fehlender Erfahrungswerte, nicht garantiert werden kann.
Eine Aufbewahrungstechnologie sollte insbesondere vor dem Hintergrund, dass bei der aktuellen Entwicklungsgeschwindigkeit mehrere Technologiesprünge bei Speichermedien innerhalb weniger Jahre vollzogen wurden, sehr sorgfältig ausgewählt werden.

3. Vertraulichkeit

Es obliegt dem Steuerpflichtigen die eigenen Daten gegen unberechtigte Einsichtnahme zu schützen. Damit sind u. a. schützenswerte Betriebs- und Geschäftsgeheimnisse, Daten, die unter das Berufsgeheimnis fallen sowie personenbezogene Daten gemeint. Der Schutzbedarf besteht auch für den Datenzugriff durch den Betriebsprüfer (Kapitel VIII.). Dabei können die Informationen durch geeignete Zugriffsbeschränkungen (ERP-Systeme bieten i. d. R. die Möglichkeit, dafür sog. „Prüferrollen" anzulegen) oder die Technik des „digitalen Schwärzens" geschützt werden. Diese Maßnahme des restriktiven Datenzugriffs nach dem sog. „need-to-know Prinzip" obliegt dem Buchführungspflichtigen. Es sei angemerkt, dass durch zu weitreichende Zugriffe oder Einsichtnahmen erlangte Erkenntnisse der Betriebsprüfer zum Nachteil des Buchführungspflichtigen gereichen können.

VI. Internes Kontrollsystem (IKS)

Das IKS umfasst alle technischen und organisatorischen Maßnahmen, die im Unternehmen zum Zwecke der Sicherstellung des ordnungsgemäßen Geschäftsablaufs und deren Steuerung implementiert sind. Um die Einhaltung der Ordnungsvorschriften gewährleisten und nachweisen zu können, sind entsprechende Kontrollmaßnahmen einzurichten, regelmäßig durchzuführen und zu protokollieren. Das IKS selbst und alle es umfassende Kontrollen sind als Teil der Verfahrensdokumentation nachvollziehbar zu beschreiben und im unternehmerischen Alltag wirksam umzusetzen. Ein gesonderter Teil des IKS, das sog. IT-IKS, umfasst die Kontrollen zur Einhaltung der Ordnungsmäßigkeit der steuer- und rechnungslegungsrelevanten eingesetzten IT-Systeme (inkl. Vor- und Nebensysteme sowie erforderlicher IT-Infrastrukturen wie Netzwerkkomponenten, Rechenzentren usw.) sowie die Informationssicherheit. Ein solches IT-IKS betrachtet die IT-Systeme aus drei Perspektiven, wobei diese aufeinander aufbauen.[16]

1. In nahezu jedem Unternehmen werden die Geschäftsprozesse, insbesondere die steuer- und abrechnungsrelevanten, vollständig durch IT-Anwendungen abgebildet oder essentiell unterstützt. Dabei sollten Kontrollmaßnahmen wie z. B. Vollständigkeitschecks oder Berechtigungsbeschränkungen implementiert werden, um das Risiko für Fehler oder Missbrauch zu begrenzen.
2. Die IT-Anwendungen, die für die Prozesse genutzt werden, sollten danach kontrolliert werden, ob alle Funktionen der Datenverarbeitung wie vorgesehen ablaufen, dass keine Sicherheitslücken oder Software- und Infrastrukturfehler offenstehen und alle Schnittstellen ordnungsgemäß funktionieren. Dazu gehört auch die Kontrolle von Unternehmensprozessen zur sicheren Entwicklung von Software, sowie dem Änderungs-, Entwicklungs- und Releasemanagement.
3. Die IT-Anwendungen selbst werden von der ihnen zugrundeliegenden IT-Infrastruktur ausgeführt oder unterstützt. Diese gilt es ebenfalls mit entsprechenden Kontrollen auszustatten. Dazu gehören z. B. Zutrittskontrollen oder Hochwasserschutz von vorhandenen Rechenzentren.

Eine umfangreiche Auflistung von Risiken und entsprechenden Gegenmaßnahmen und Kontrollen für IT-Systeme bietet u. a. die bereits erwähnte Norm ISO 27001:2013. Zum Umfang eines IKS gehört außerdem ein kontinuierlicher Verbesserungsprozess (kurz KVP), durch den die Wirksamkeit und Effizienz der umgesetzten Maßnahmen und Kontrollen regelmäßig evaluiert und auf Basis der Ergebnisse entsprechend weiterentwickelt werden kann. Den GoBD nach besteht keine Anerkennungspflicht von Zertifizierungen oder Softwaretestaten durch Prüfer.[17]

VII. Anforderungen an den Umgang mit aufzeichnungs- und aufbewahrungspflichtigen Unterlagen

1. Erfassung der Geschäftsvorfälle

Es müssen alle von den Buchführungs- und Aufzeichnungspflichten betroffenen Unterlagen vollständig, zeitgerecht und geordnet erfasst werden. Dabei muss gewährleistet sein, dass zwischen dem Empfang von Unterlagen und deren Erfassung keine Informationen verloren gehen oder verändert werden können.
Originär elektronisch erstellte oder empfangene Daten sind auch elektronisch, im Ursprungsformat, aufzubewahren. Eine Ausnahme dieser Regel bilden elektronisch, aber nicht in Vor-, Haupt-, oder Nebensystemen erstellte Dokumente, die ausschließlich in Papierform versendet wurden (z. B. eine in einem Textverarbeitungsprogramm erstellte Rechnung).
Eine Erfassung der Geschäftsvorfälle sollte möglichst unmittelbar nach deren Entstehung erfolgen. Dabei kann jede nicht durch den regulären Geschäftsbetrieb bedingte und dokumentierte Zeitspanne als bedenklich angesehen werden. Die Erfassung der Geschäftsvorfälle endet mit der sog. Festschreibung, ab dieser unterliegen die erfassten Daten dem Grundsatz der Unveränderbarkeit. Die Festschreibung selbst unterliegt durch die GoBD erstmals konkreten Fristen, die sich am Termin der Umsatzsteuer-Voranmeldung orientieren. Unbare Geschäftsvorfälle müssen grundsätzlich innerhalb von zehn Tagen und Eingangsrechnungen innerhalb von 8 Tagen erfasst werden. Die Führung von Kassen bzw. die Buchung von baren Geschäften muss dagegen täglich erfolgen. Wird allerdings nicht laufend, sondern nur periodenweise gebucht, müssen alle unbaren Vorfälle spätestens bis zum Ablauf des Folgemonats erfasst werden.
Mit der GoBD wird den Steuerpflichtigen ein Wahlrecht eingeräumt, ob in Papierform empfangene Dokumente elektronisch, als Scan oder weiterhin physisch aufbewahrt bzw. archiviert werden sollen. Damit ist es deutlich vereinfacht worden, nahezu alle Unterlagen ausschließlich elektronisch aufzubewahren (Stichwort „papierloses Büro").

Exkurs Scanvorgang
Wenn Dokumente in Papierform zum Zwecke elektronischer Aufbewahrung und Archivierung eingescannt werden sollen („papierloses Büro"), ist dafür ein Prozess zu etablieren, der in einer Verfahrensanweisung, als Teil der GoBD-relevanten Verfahrensdokumentationen, nachvollziehbar zu beschreiben ist. Dabei ist

16 Vgl. IDW PS 330 – Abschlussprüfungen bei Einsatz von Informationstechnologie.
17 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 181.

u. a. auch zu bestimmen, ob eine inhaltliche Übereinstimmung (z. B. Schwarz-Weiß oder OCR-Scans) ausreichend ist oder weitergehend eine bildliche oder sogar farbliche Übereinstimmung (Farbscan) notwendig ist.
Die einmal eingescannten Dokumente sind der weiteren Bearbeitung im Unternehmen zu entziehen und können anschließend vernichtet werden, sofern keine sonstigen Vorschriften dem entgegenstehen. Die weitere Bearbeitung der Dokumente sollte anschließend digital nach dem Grundsatz der Nachvollziehbarkeit erfolgen. Sollte die weitere Bearbeitung nicht ausschließlich digital möglich sein, müssen organisatorische Vorkehrungen getroffen werden, um die Nachvollziehbarkeit trotzdem gewährleisten zu können, bspw. indem das bearbeitete Papierdokument nochmals eingescannt und mit dem ersten verknüpft wird. [18]

Exkurs E-Mail
Es ist regelmäßig strittig, ob E-Mails zu den aufbewahrungspflichtigen Unterlagen gezählt werden. Die Frage kann nicht pauschal beantwortet werden und ist einzelfallabhängig. Handelt es sich bei der betroffenen E-Mail ausschließlich um ein Transportmedium für Anhänge, wie z. B. eine Rechnung im PDF-Format, dann kann die E-Mail selbst wie ein „Briefumschlag" angesehen und entsprechend gelöscht werden. Enthält die E-Mail im Text oder Header aber selbst bereits aufzeichnungspflichtige Inhalte, dann muss diese ebenfalls im Originalformat aufbewahrt werden.[19] Weiterhin sei darauf hingewiesen, dass im Falle von signierten aufbewahrungspflichtigen E-Mails weitere Vorgaben im Einzelfall zu beachten sind (z. B. Aufbewahrung der Signaturprüfschlüssel).

2. Buchführung

Die Buchung folgt der Erfassung des Geschäftsvorfalls, kann aber zeitlich auseinanderfallen. Für die Buchung und die Erfüllung der Belegfunktion ist jedem Geschäftsvorfall ein Beleg (Eigen- oder Fremdbeleg) zugrunde zu legen.[20] Bei IT-gestützten Prozessen erfolgt die Belegfunktion teilweise nicht mehr durch konventionelle Belege, sondern ist durch den ordnungsmäßigen Einsatz der jeweiligen Verfahren und IT-Anwendungen nachzuweisen.
Die Geschäftsvorfälle müssen anschließend so verarbeitet werden, dass in angemessener Zeit ein Überblick über die Vermögens- und Ertragslage des Steuerpflichtigen abgeleitet und nachvollzogen werden kann.
Alle (elektronischen) Unterlagen zu den jeweiligen Geschäftsvorfällen müssen für die Dauer der jeweils geltenden Aufbewahrungsfrist in angemessener Zeit auffindbar sein. In der praktischen (prozessualen und technischen) Ausgestaltung der Verknüpfung von zusammengehörenden elektronischen Dokumenten ist der Steuerpflichtige frei, allerdings empfiehlt das BMF die Dokumente und Geschäftsvorfälle mit einer festen Indexierung zu versehen.
Alle Änderungen, die Auswirkungen auf die spätere Nachvollziehbarkeit der Geschäftsvorfälle haben können, sind entsprechend zu protokollieren und zu historisieren. Das gilt insbesondere für programmtechnische Änderungen, die Anpassungen von Automatismen oder die Stammdatenpflege. Die dabei anfallenden Änderungsbelege oder -protokolle sind ebenfalls als Teil der Verfahrensdokumentation aufzubewahren und zu schützen.

3. Aufbewahrung

Im Unternehmen entstandene oder dort in digitaler Form eingegangene aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze und elektronische Dokumente sind unverändert aufzubewahren und dürfen nicht vor Ablauf der Aufbewahrungsfrist gelöscht werden.[21]
Sollten durch die operative Tätigkeit Konvertierungen in andere Dateiformate vorgenommen werden (z. B. in ein sog. „Inhouse-Format"), bei dem das Ergebnis der Umwandlung inhaltlich identisch (verlustfrei) und für die maschinelle Auswertbarkeit verfügbar ist, ist die ursprünglich (daher im Original) in das Unternehmen eingegangene Datei vor ihrer Konvertierung trotzdem sicher aufzubewahren und darf folglich nicht gelöscht werden.
Werden beim Transport, der Verarbeitung oder Aufbewahrung von elektronischen Unterlagen kryptografische Techniken eingesetzt, so ist darauf zu achten, dass das unverschlüsselte Dokument in angemessener Zeit wieder, z. B. bei einer Prüfung, zur Verfügung gestellt werden kann. Wenn Dokumente außerdem elektronisch signiert werden, sind die Schlüssel ebenfalls so lange mit aufzubewahren wie die Dokumente selbst.[22]
Die Unveränderbarkeit der Informationen und die Möglichkeit des langfristigen Speicherns spielt eine wichtige Rolle bei der Erfüllung verschiedener Compliance-Anforderungen (neben den GoBD z. B. auch UStG oder Sarbanes-Oxley-Act). Eine einfache Ablage im Dateisystem oder die Nutzung von Programmen, die unprotokollierte Änderungen an Daten oder Dokumenten erlauben, sind nun durch die GoBD für unzureichend erklärt worden und genügen folglich den Grundsätzen der Unveränderbarkeit und Nachvollziehbarkeit nicht mehr.[23] Hieraus lässt sich für die unternehmerische Praxis ableiten, dass das BMF darauf abzielt, statt einer Dateisystemablage den Einsatz eines sog. Dokumentenmanagementsystems (DMS) zu bevorzugen.
Es müssen außerdem grundsätzlich die technischen und prozessualen Voraussetzungen geschaffen sein, dass alle Unterlagen während ihrer Aufbewahrungsfristen in angemessener Zeit lesbar gemacht werden können.

Exkurs: DMS
Eine DMS-Anwendung dient der Organisation und Koordination der Erstellung, Überarbeitung, Überwachung und Verteilung sowie der geordneten Aufbewahrung von Dokumenten und Informationen unterschiedlichster Art über ihren gesamten Lebenszyklus bzw. ihre vorgegebene Aufbewahrungsfrist im Unternehmen.[24]
Durch den Einsatz einer geeigneten DMS-Lösung kann außerdem der Einhaltung des Grundsatzes der Unveränderbarkeit von elektronischen Unterlagen (technisch sowie prozessual) nachgekommen werden. Mit einem DMS kann zudem die Verknüpfung von Dokumenten/Unterlagen mit ihren entsprechenden Geschäftsvorfällen und Buchungen inklusive Historisierung unterstützt sowie eine Löschung nach Beendigung der Aufbewahrungspflichten erleichtert werden.

18 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 136 ff.
19 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 121.
20 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 77 ff.
21 Vgl. Aufbewahrungsfristen § 147 AO bzw. § 257 HGB.
22 Vgl. Aufbewahrung bei Einsatz von Kryptografietechniken GoBD Tz. 134.
23 Vgl. BMF-Schreiben v. 14.11.2014, Tz. 110.
24 Vgl. GoBD-Checkliste für Dokumentenmanagement-Systeme des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V.

4. Löschen

Aufbewahrungspflichtige und archivierte Dokumente dürfen erst nach Ablauf der Aufbewahrungsfrist vernichtet bzw. gelöscht werden. Bei der Einführung einer elektronischen Archivierung sollten die für das Löschen notwendigen technischen und organisatorischen Prozesse, entsprechend den gesetzlichen Vorgaben, von Anfang an bedacht und dokumentiert werden. Hierdurch lässt sich eine unabsichtliche Löschung vor Ablauf der Fristen sowie eine längere Aufbewahrung als notwendig vermeiden.

VIII. Datenzugriff und maschinelle Auswertbarkeit

Alle originär digital erzeugten und aufbewahrungspflichtigen Unterlagen müssen in maschinell auswertbarer Form (damit zwingend auch auf maschinell auswertbaren Datenträgern) aufbewahrt werden. Das Finanzamt hat dabei Anrecht auf:

- unmittelbaren, nur-lesenden Datenzugriff (Z1) auf die Systeme des Steuerpflichtigen.
- mittelbaren Datenzugriff (Z2). Es kann verlangen, dass Daten auf eine bestimmte Weise aufbereitet und mit nur-lesendem Datenzugriff zur Verfügung gestellt werden.
- Datenträgerüberlassung (Z3), d. h. es kann verlangen, dass Daten auf einem Datenträger oder gar als Ausdruck ausgeliefert werden.

Das gilt nicht nur für Daten der Buchführung, sondern auch für alle Einzelaufzeichnungen und Stammdaten mit steuerlicher Relevanz aus den Vor- und Nebensystemen der Buchführung. Das BMF fordert für die nachvollziehbare Auswertung der Datenbanken des Steuerpflichtigen, dass neben der Datei auch eine Datensatzbeschreibung im XML-Format vorzuhalten ist.

Exkurs: Erfordernis einer „Maschinellen Auswertbarkeit“[25]

Eine maschinelle Auswertbarkeit bei aufzeichnungs- und aufbewahrungspflichtigen Daten, Datensätzen, und elektronischen Unterlagen ist gegeben, wenn mathematisch-technische Auswertungen (z. B. mittels „IDEA“[26]), eine Volltextsuche oder Prüfungen im weitesten Sinne möglich sind.

IX. Hinweise, Handlungsempfehlungen und Fazit

Fehlende Konformität bzw. nicht erfüllte Anforderungen im Rahmen der Buchführung können zu erheblichen Diskussionen während der Betriebsprüfung führen. Schlimmstenfalls können Verfehlungen mit einer Versagung der kompletten Buchführung und damit einhergehenden Strafen, Sicherheitszuschlägen oder Steuerschätzungen sanktioniert werden[27] und sogar strafbar sein.[28] Bereits im Falle von Fahrlässigkeit drohen Geld- oder Freiheitsstrafen. Durch eine gute Vorbereitung kann sich jeder Steuerpflichtige in einem für sein Unternehmen angemessenem Umfang vor derartigen Schäden schützen. Es empfiehlt sich daher, sofern noch keine ausreichende Klarheit zum derzeitigen Status der Konformität zu den neuen GoBD besteht, hier zeitnah eine Erhebung und qualifizierte Bewertung des Status Quo (sog. Health Check) durchzuführen, Handlungsfelder zu identifizieren und entsprechende Maßnahmen zu planen. Dies sichert in der Prüfungssituation zumindest, dass nicht der Prüfer eventuelle Missstände erkennt und zur Diskussion bringt, sondern erlaubt einen proaktiven Umgang durch die Verantwortlichen auf Basis einer bereits vorliegenden Maßnahmenplanung, auch wenn noch nicht alle Maßnahmen in Gänze umgesetzt sein sollten.

Generell gilt, dass strukturierte Prozesse, wirksame interne Kontrollstrukturen an den risikobehafteten Prozessschritten, klare Rollen und Verantwortlichkeiten bei Mitarbeitern sowie eine nachvollziehbare und aktuelle Dokumentation der internen Betriebs- und Geschäftsprozesse eine fundierte Ausgangsbasis schaffen. Das schafft neben Transparenz auch ablauforganisatorische Sicherheit sowie die notwendigen Steuerungsmöglichkeiten. Zudem sollte sichergestellt sein, dass alle Mitarbeiter, die mit steuer- und rechnungslegungsrelevanter Datenverarbeitung zu tun haben, die Verfahrensdokumentationen verpflichtend beachten müssen. Der gezielte Einsatz moderner IT-Systeme zur optimalen Unterstützung der Prozesse und Kontrollen im Unternehmen kann zusätzlich helfen, neben wirtschaftlichen Aspekten auch zielgerichtet die Compliance-Anforderungen zu unterstützen. Zu beachten bleibt, dass auch für den Einsatz der IT die Compliance-Vorgaben Gültigkeit besitzen.

Auch im Interesse des Unternehmens sollte durch ein umfassendes Informationssicherheits-Management dafür gesorgt werden, dass alle IT-Systeme, die direkt oder indirekt zur Verarbeitung steuer- und rechnungslegungsrelevanter Vorgänge und Dokumente herangezogen werden, vor allen internen und externen Risiken bzw. Bedrohungen angemessen geschützt sind und dies auch bleiben.

Es empfiehlt sich zudem, ein DMS sowohl in die bestehende Systemlandschaft als auch die entsprechenden Geschäftsprozesse zu integrieren, um eine GoBD-konforme Aufbewahrung aufzeichnungspflichtiger Unterlagen gewährleisten zu können.

AUTOREN

Rüdiger Giebichenstein, *Dipl.-Wirtschaftsinformatiker, mit den Beratungsschwerpunkten Cyber Security, (IT-) Compliance und (IT-)Governance, (IT-)Risikomanagement, Datenschutz und Business Continuity Management.*

Carsten Alexander Schirp, *Dipl.-Ing., ist als Experte in den Schwerpunkten Cyber Security, (IT-) Risikomanagement, (IT-) Governance, (IT-) Compliance, Datenschutz, Informationssicherheitsmanagement nach ISO/IEC 27001 sowie GRC-Tools und Jahresabschlussprüfung tätig.*

25 Vgl. § 147 Abs. 2 Nr. 2 AO.
26 IDEA – Software zur Analyse von Massendaten, die von Finanzbehörden zur digitalen Unterstützung ihrer Prüfungshandlungen eingesetzt wird.
27 Vgl. § 158 AO und § 162 AO.
28 Vgl. § 283b StGB.