REVIDATA GmbH
Kompetenz schafft Vertrauen

Funktionsprüfung betriebswirtschaftlicher Anwendungssoftware auf der Grundlage des IDW-Prüfungsstandards 880 „Erteilung und Verwendung von Softwarebescheinigungen“

1 Einführung

Moderne EDV-Anwendungssysteme unterstützen die Abwicklung aller wesentlichen Geschäftsprozesse eines Unternehmens. Die hierin integrierte Finanzbuchhaltung empfängt und verarbeitet Unternehmensdaten zu rechnungsrelevanten Informationen. Unzureichend innerhalb der EDV abgebildete Prozesse und unvermeidliche Programmfehler beeinträchtigen dabei sowohl betriebliche Funktionen als auch die Qualität der hieraus resultierenden Finanzbuchhaltung, Bilanz- und G&V- Daten.

Angesichts der beschriebenen Situation, zunehmender gesetzlicher Anforderungen an die Ordnungsmäßigkeit der buchhalterischen Verarbeitung steuerlich relevanter Vorgänge (GoBD) und Sicherheit der Verarbeitung vertraulicher Daten (DSGVO) sowie verschärfter Prüfungsstandards legen sowohl Abschlussprüfer als auch die Anwender betriebswirtschaftlicher Anwendungssysteme verstärkt Wert auf die Qualitätsmerkmale einer Software. Hierzu gehört vorrangig die Softwarebescheinigung, welche bestätigt, dass bei sachgerechter Programmanwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung gewährleistet wird. Grundlage einer solchen Softwarebescheinigung bildet die Funktionsprüfung der Software, mit deren Hilfe die Ordnungsmäßigkeit und Sicherheit analysiert und festgestellt werden.

Die nachfolgenden Ausführungen beschäftigen sich mit Verfahren und Techniken einer Funktionsprüfung und vermitteln einen Überblick über den Differenzierungsgrad und die Nachhaltigkeit der unterschiedlichen Prüfungshandlungen sowie die Form der Ergebnisdokumentation.

2 Inhalte einer Funktionsprüfung

Funktionsprüfungen werden von Softwareherstellern beauftragt und von Prüfungs- bzw. Revisionsgesellschaften durchgeführt. Erfolgreiche Funktionsprüfungen sind Voraussetzung für die Erteilung entsprechender Prüfungsbescheinigungen durch sachverständige Dritte wie IT-Gutachter, Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften. Die Funktionsprüfung kann sich hierbei sowohl auf ein integriertes ERP-Softwarepaket, wie z. B. Finanz- und Anlagenbuchhaltung, Bilanz, G&V, sowie Materialwirtschaft, Kostenrechnung und HR-Systeme, beziehen oder einzelne Programme oder einzelner Programmfunktionalitäten (z. B. die allgemeine Programmsicherheit) betreffen.

Den Einmalprüfungen und Bescheinigungen stehen regelmäßige Prüfungen (Follow-ups) gegenüber, die auf der Basis einer vorhandenen Prüfungsbescheinigung für zukünftige Software-Releasestände vorgenommen werden und den Prüfungsschwerpunkt auf die programmierten Softwareerweiterungen und Softwareänderungen legen.

Im Unterschied zur DV-Verfahrensprüfung werden Funktionsprüfungen grundsätzlich in einer separaten Testumgebung durchgeführt und berücksichtigen nicht die individuelle Implementierung und Programmeinstellungen beim Anwender. Der Prüfer greift als entsprechender Benutzer auf das Testsystem zu und prüft sachlogisch, funktionell und ergebnisorientiert die Ordnungsmäßigkeit und Funktionssicherheit der Software mit Hilfe definierter Testfallszenarien und erzielter Auswertungen.

3 Gesetzliche und sonstige Grundlagen

Im Rahmen einer Funktionsprüfung werden folgende Prüfungsmaßstäbe herangezogen:

- die handels- und steuerrechtlichen Vorschriften zur Ordnungsmäßigkeit der Buchführung (§§ 238 ff. HGB, §§ 140 ff. AO)
- die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“, veröffentlicht am 14. November 2014, GZ IV A 4 – S 0316/13/10003, DOK 2014/0353090
- der IDW-Prüfungsstandard „Erteilung und Verwendung von Softwarebescheinigungen“ (IDW PS 880), Stand 10. März 2010
- die Stellungnahme des Fachausschusses für moderne Abrechnungssysteme (FAMA) des Instituts der Wirtschaftsprüfer in Deutschland e. V. über die „Grundsätze ordnungsmäßiger Buchführung bei computergestützten Verfahren und deren Prüfung“
- der IDW-Prüfungshinweis PH 9.100.1
- der IDW-Prüfungsstandard „Abschlussprüfung bei Einsatz von Informationstechnologie“ (IDW PS 330/EPS 450 n. F.)
- die IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1)
- der IDW-Prüfungsstandard „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“ (IDW PS 261 n. F.)
- der IDW-Prüfungsstandard „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen“ (IDW PS 331)
- der IDW-Prüfungsstandard „Arbeitspapiere des Abschlussprüfers“ (IDW EPS 460 n. F.)
- der IDW-Prüfungsstandard „Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen“ (IDW EPS 951 n. F.
- die Bestimmungen des Bundesdatenschutzgesetzes BDSG sowie der EU-Datenschutz-Grundverordnung EU-DSGVO

Dabei beschreibt der IDW-Prüfungsstandard PS 880 die Inhalte der Verfahrensprüfung, die Art der Berichterstattung sowie die Erstellung der Softwarebescheinigung und die Verwendung derartiger Bescheinigungen im Rahmen der Jahresabschlussprüfung.

Über die aufgeführten Grundlagen hinaus sind – je nach Notwendigkeit – weitere Vorschriften und branchenspezifische Gesetze heranzuziehen.

4 Rahmenbedingungen einer Funktionsprüfung

Die Komplexität einer Funktionsprüfung und die damit verbundene Verantwortung verlangen eine detaillierte Abstimmung nachfolgender Rahmenbedingungen:

- ***Prüfungsobjekte***

In einem ersten Schritt gilt es, das Prüfungsobjekt und hiermit das Ziel und den Umfang der Funktionsprüfung möglichst exakt abzugrenzen.

Insbesondere ist im Falle der Erstellung einer Bescheinigung oder der Erstellung eines Gutachtens für die Software der Geltungsbereich festzulegen, d. h. zu definieren, welche Bestandteile der Software zu prüfen sind. Hierzu gehört eine Bestandsaufnahme der Anwendungssysteme, Module, Zusatzfunktionalitäten, Schnittstellen, etc., die in Ergänzung zur IT-geführten Rechnungslegung zu prüfen sind. Es gilt dabei zu beachten, dass nur die Elemente geprüft werden können, die der Prüfungsgesellschaft bekannt gemacht worden sind. Grundlage für den Umfang einer Funktionsprüfung sollten demzufolge stets die Dokumentationsbestandteile sein (Anwenderhandbuch, System- und Verfahrensdokumentation, Release Dokumentationen und Ablaufbeschreibungen, etc.), die für den aktuell zu prüfenden Release-Stand der Software gültig sind.

Darüber hinaus besteht die Möglichkeit einer Konformitätsprüfung der Software im Hinblick auf die datenschutzrechtlichen Anforderungen der EU-DSGVO. In diesem Zusammenhang wird geprüft, ob die Software hinsichtlich technischer Gestaltung, der Bedienung und der sicheren Datenhaltung und Datenlöschung den Anforderungen der EU-DSGVO genügt.

Darüber hinaus wird beurteilt, inwieweit die vorhandenen Dokumentationen (u. a. Anwenderdokumentation, Verfahrensbeschreibungen, Systemdokumentation) auch den Anforderungen der EU-DSGVO genügen, besonders auch im Hinblick auf die neuen Auskunftspflichten gemäß der EU-DSGVO gegenüber den Kunden, Lieferanten und dem Personal.

- ***Prüfungsvorgehen und -budget***

In einem zweiten Schritt sind das Prüfungsvorgehen, die Dauer der Prüfung einschließlich ggf. notwendiger Nachprüfungen, die Dokumentation der Prüfungsergebnisse (Erstellung eines Prüfberichtes, ggfs. zusätzlich einer Softwarebescheinigung) sowie das Budget zu bestimmen. Hierbei ist auch der Einarbeitungsaufwand des Prüfers angemessen zu berücksichtigen.

- ***Prüfungsort***

Die Abstimmung der Rahmenbedingungen muss auch den Prüfungsort einbeziehen. Für die Prüfungen selbst muss eine Testumgebung im erforderlichen Umfang (Testsystem mit dem zu prüfendem aktuellen Releasestand der Software) eingerichtet werden, die vorzugsweise beim Softwarehersteller betrieben wird. Der Zugriff auf das System kann entweder vor Ort oder via Remotezugriff durch den Prüfer (z. B. via TeamViewer oder sonstiger RDP-Verbindung erfolgen). Auch besteht die Möglichkeit, ein entsprechendes Testsystem in einem REVIDATA Büro zu installieren.

Zu Beginn der Softwareprüfungstätigkeit hat zweckmäßigerweise eine Einweisung des Prüfers in die Handhabung der Software durch den Auftraggeber zu erfolgen.

- ***Prüfungszeitpunkt***

Aus Effizienzgründen ist es empfehlenswert, die Terminierung der Prüfung an der Releaseplanung des Softwareherstellers auszurichten. Findet die Prüfung im Anschluss an die interne Qualitätssicherung eines neuen Releases statt, können noch vor dessen Auslieferung Änderungen, die sich aufgrund der Prüfungsfeststellungen ergeben, integriert werden.

- ***Vollständigkeitserklärung***

Vor Beginn der Prüfung hat der Softwarehersteller eine Vollständigkeitserklärung auszufüllen und der Prüfungsgesellschaft zur Verfügung zu stellen. Hierbei hat der Softwarehersteller auf alle ihm bekannten Software- bzw. Dokumentationsmängel hinzuweisen.

5 Ablauf einer Funktionsprüfung

In Anlehnung an den IDW-Prüfungsstandard PS 880 bietet sich folgender Ablauf für eine Funktionsprüfung an:

5.1 Prüfung der Verarbeitungsfunktionen (buchungstechnische Sicht)

5.1.1 Prüfungsziel und -inhalt

Ziel der Prüfung der Verarbeitungsfunktionen ist die Feststellung, dass die *Beleg-, Journal- und Kontenfunktion* im Hinblick auf die Ordnungsmäßigkeit der Buchführung unter Einbeziehung der zu prüfenden Module des Anwendungssystems erfüllt werden (Integrationsprüfung).

Bezüglich der *Erfüllung der Beleg-, Journal- und Kontenfunktion* sind vorrangig folgende Angaben bei der systemseitigen Verarbeitung zu erbringen[1, 2]:

- hinreichende Erläuterung des Vorgangs (Buchungstext oder -schlüssel),
- Buchungsbetrag (Mengen- oder Wertangaben, aus denen sich der zu buchende Betrag ergibt) und Buchungswährung,
- Zeitpunkt des Vorgangs (Belegdatum, Bestimmung der Buchungsperiode),
- Bestätigung des Vorgangs (Autorisation) durch den Buchführungspflichtigen.
- Kontierung (Konto und Gegenkonto),
- Ordnungskriterium (Belegnummer),
- Buchungsdatum (Kennzeichnung des Zeitpunkts der Buchung),

Es ist grundsätzlich festzustellen, ob die progressive und retrograde Nachvollziehbarkeit der Buchungen gewährleistet ist, und zwar über den Beleg, das Journal und die Konten bis zur Bilanz und G&V und umgekehrt. Ergänzend sind *weitere Verarbeitungsfunktionen*, die zur Verarbeitung abrechnungsrelevanter Daten systemseitig angeboten werden, im Hinblick auf die Erfüllung der Anforderungen der Ordnungsmäßig der Rechnungslegung zu testen.

Auf Basis der Verfahrensdokumentation (Anwenderhandbuch, Systemdokumentation, herstellerseitige Feinkonzeption, Leistungsbeschreibung, etc.) ist festzustellen, ob die beschriebenen Funktionalitäten systemseitig identisch realisiert und verständlich dargestellt worden sind.

---

1 vgl. IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1, Stand 24. September 2002)“, Textziffer 35, 36

2 vgl. Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“, veröffentlicht im Bundessteuerblatt 1995, Teil I, Nr. 18; S. 6-8 (GoBS)

5.1.2 Prüfungsablauf

5.1.2.1 Anlagen von Testmandanten und Konzeption der Testfälle

Das Prüfungsvorgehen sollte sich an den vorhandenen Testvorfällen des Softwareherstellers orientieren. Unabhängig davon sind seitens des Prüfers Testvorfälle zu definieren, die auch Fehlerkonstellationen beinhalten, um insgesamt ein fundiertes umfassendes Prüfungsergebnis zu erhalten.

Aus der Erfahrung heraus hat es sich als zweckmäßig herausgestellt, im Vorfeld der Prüfung unterschiedliche Testmandanten (Firmen) zu definieren, um eine hohe Bandbreite an verschieden Testvorfällen abbilden und untersuchen zu können. Es können beispielsweise Testmandanten für die Überprüfung der nachstehenden Ausprägungen gebildet werden:

- *Prüfung von Stammdaten* (in diesem Zusammenhang auch: Referenzieren auf andere Mandanten (bezüglich der Stammpflege),

- *Prüfung von Standardgeschäftsvorfällen – Massentests* - (ca. 200 bis 500 Testvorfälle),

- Prüfung der Definition eines *Rumpfgeschäftsjahres* bzw. von abweichenden Wirtschaftsjahren,

- Prüfung der *Konsolidierungsfunktionalitäten*, falls diese realisiert sind (dazu ist es notwendig, mindestens zwei „Tochter-Mandanten festzulegen, die auf den „Mutter-“ Mandanten konsolidieren),

- Prüfung von *Sonderfunktionalitäten* (z. B. Parallelwährungsfähigkeit, *Hauswährungsumstellung auf den Euro* mit sämtlichen angebotenen Umstellungsvarianten),

- Ergänzend: Prüfung der *programmierten Verarbeitungsregeln* (auch Fehlerprüfungen) und Plausibilitätskontrollen.

Es ist hilfreich, die Konzeption der Testvorfälle auf Basis eines im Vorhinein bestimmten Kontenrahmens durchzuführen und hierbei die Anzahl und unterschiedliche Ausprägung von Personenkonten sowie weiterer Stammdaten und Parameter festzulegen.

5.1.2.2 Prüfungen der Verarbeitung von Stammdaten

Im ersten Schritt erfolgt die Überprüfung der korrekten Verarbeitung von Stammdaten. Hierzu gehören insbesondere die Bearbeitungsfunktionen „Anzeigen“, „Anlegen“, „Ändern“, „Sperren/Freigeben“, „Löschen/Inaktivieren“. Als Voraussetzung für die Prüfung der Verarbeitungsfunktionen ist die korrekte Anlage folgender Stammdaten zu prüfen:
- Mandanten (Firmen),
- Wirtschaftsjahre und die (parallel) bebuchbaren Abrechnungsperioden,
- Währungen (Firmen- und Fremdwährungen),
- Sachkonten (auch Offene-Posten-geführte Sachkonten),
- Auswahl/Definition eines Kontenrahmens,
- Personenkonten (auch CPD-Konten, Verbandskonten),
- Kostenstellen und Kostenträger,
- Buchungstypen,
- Belegarten und
- weitere softwarespezifische Stammdaten bzw. Parameter (wie z. B. Steuerschlüssel).

5.1.2.3 Prüfungen von Beleg-, Journal- und Kontenfunktion

Im zweiten Schritt sind zur Prüfung der Beleg-, Konten- und Journalfunktion sowie der weiteren Funktionalitäten Geschäftsvorfälle zu Buchungstypen zu den aufgeführten Testvorfällen zu bilden und im Rahmen von Massen- und Einzeltests in den unterschiedlichen Testfirmen mit unterschiedlichem Buchungsumfang zu prüfen. Hierzu gehören z. B. folgende Testvorfälle:

- Erfassung und Buchung von *„Standard-Geschäftsvorfällen*“ (Rechnungseingang, Rechnungsausgang, Anzahlungen, Sachkontenbuchungen, Gutschriften, Stornierungen, Dauerbuchungen, Fremdwährungsbuchungen, Sammelkontenumbuchung, statistische Buchungen, Verrechnungsbuchungen, Buchungen aus Datenübernahmen)

- Verarbeitung von Geschäftsvorfällen bezüglich der *Umsatzsteuer und der Zahlungsbedingungen nebst Rückrechnungen* (Steuerbuchungen allgemein, USt im EG-Binnen-markt, innergemeinschaftlicher Warenverkehr),

- Erstellung der *Umsatzsteuervoranmeldung* (ergänzend: systemseitiges Vorhandensein von Abstimmkontrollen) und der zusammenfassenden Meldung,

- Prüfung der Zuordnung von Zahlungen zu *offenen Posten* und der verschiedenen *Ausgleichsmöglichkeiten*,

- Durchführung von *Mahnläufen*, Prüfung der Mahnvorschlagsliste, der Mahnliste und der Mahnungen nebst Mahnstufen,

- Prüfung des *Zahlungsmanagements* bezüglich der unterschiedlichen Zahlungsarten (Überweisung, Einzugsverfahren, Scheck, Wechsel, Datenträgeraustausch) und der korrekten vollständigen Erstellung von Zahlungsvorschlags- und Regulierungslisten sowie der automatischen oder manuellen Generierung von *Zahlungsbuchungen*,

- die Realisierung der *Jahreswechselfunktionalitäten* (Jahresabschlussbuchungen, Umbuchung der GuV-Salden auf ein Bilanzvortragskonto, Verhinderung des Saldovortrags für GuV-Kontensalden ins neue Geschäftsjahr, Buchung von Saldovorträgen in die Eröffnungsbilanz, systemseitige Prüfung der Soll-/Haben-Identität beim endgültigen Jahresabschluss, Feststellung der Bilanzidentität, Verhinderung der Buchung in das alte Geschäftsjahr nach dem endgültigen Jahresabschluss),

- die *Vollständigkeit und Richtigkeit der systemseitig zur Verfügung gestellten Auswertungen* (Stammdatenlisten für Sachkonten, Debitoren und Kreditoren, Bilanz und GuV, Summen- und Saldenlisten, Kontoauszug, Offene-Posten-Listen, Einzelpostenlisten, Fälligkeitsvorschau, Mahnungen, Saldenbestätigungen, Umsatzsteuervoranmeldung, zusammenfassende Meldung, etc.). Dabei ist insbesondere die Konsistenz der Auswertungen untereinander zu prüfen.

5.2 Prüfung der programmierten Verarbeitungsregeln (DV-technische Sicht)

5.2.1 Datenerfassung und Datenfluss

Im Anschluss an die Dokumentationsprüfung oder parallel wird die programmtechnische Lösung bezüglich der Datenerfassung, des Datenflusses und der Datenübernahme anhand von Testfällen verifiziert.

In dieser Prüfungsphase ist es notwendig, dass der Softwarehersteller dem Prüfer die notwendigen Informationen zu den unterschiedlichen Datenbeständen (Dateien, Tabellen, Datenbankmodell), zum Datensatzaufbau sowie zu den programmierten Verarbeitungsfunktionen und Kontrollen verschafft.

Das Prüfungsvorgehen ist effizient und vollständig, wenn ein Testvorfallskonzept erarbeitet wird, das auf die *programmierten Verfahren und Regeln* zur Stammdatenpflege und Verarbeitung von Bewegungsdaten, zur Datenübertragung an Schnittstellen und zur Datensicherheit ausgerichtet ist.

Gemäß GoBS hat „die Beschreibung der programmtechnischen Lösung ... zu zeigen, wo und wie die sachlogischen Forderungen in Programmen umgesetzt sind. Tabellen, über die die Funktionen der Programme beeinflusst werden können, sind wie Programme zu behandeln.“ [3]

Wesentlich sind:[4]

a) *Richtigkeit* der programmierten Verarbeitungsregeln und Fehlerprüfungen:

- *Kontierung und Buchung* nebst Berücksichtigung von Steuervorgängen und Zahlungsbedingungen,
- korrekte *Periodenzuordnung*,
- richtige *Fortschreibung von Hauptbuch- und Personenkonten* und dabei Sicherstellung, dass Forderungs- und Verbindlichkeitsbuchungen ausschließlich über das Debitoren- bzw. Kreditorenbuch (Nebenbuch) und nicht direkt gebucht werden können,
- systemseitige *Summierungen und Saldierungen* (ggf. Stapelsummenkontrolle),
- Währungsbuchungen,
- Funktionen zur Durchführung des *Jahreswechsels*, Saldovortrag,
- Kontrolle, dass *gesperrte Daten* nicht geändert werden können,
- Prüfung, dass systemseitig sichergestellt ist, dass *Konten nicht gelöscht* werden können, deren Saldo ungleich Null ist, der Jahresvortrag per Saldo ungleich Null ist und die unterjährig einen Umsatz haben,
- Prüfung der Gewährleistung, dass *Stammdaten nicht gelöscht* werden können, wenn sie in noch nicht verarbeiteten Buchungsstapeln verwendet werden,
- Prüfung der systemseitigen Kontrollen gegen *doppelte Stammdatenanlage*,

---

[3] Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (kurz GoBS), veröffentlicht im Bundessteuerblatt 1995, Teil I, Nr. 18; S. 13 (GoBS)

[4] vgl. IDW-Prüfungsstandard PS 880: „Erteilung und Verwendung von Softwarebescheinigungen“ (Stand Juni 1999), S. 5-6

- Prüfung, welche programmierten Verfahren zur *Protokollierung von Stammdaten* vorhanden sind. Insbesondere sind bei der Änderung und Löschung von Stammdaten Protokollierungen systemseitig zur Verfügung zu stellen, die sicherstellen, dass der ursprüngliche Zustand der Stammdaten festgestellt werden kann,

- Verifizierung, dass *gesperrte Daten* nicht geändert werden können,

- Feststellung, dass systemseitig sichergestellt ist, dass weder *Sachkontenbuchungen*, noch offene Posten oder gespeicherte Buchungsperioden gelöscht werden können,

b) die Wirksamkeit der enthaltenen Plausibilitätskontrollen (Eingabe und maschinelle Kontrollen sowie systemseitige Abstimmverfahren):

- Definition von *Parametern* (z. B. Steuerschlüssel),

- *Felddefinitionen* (gültige Formate -auch Datum-, Werte, Grenzwerte, Prüfziffernkontrollen, Muss- oder Kannfeld-Definition, Datenfeldkombinationen),

- *Existenzkontrolle* definierter Konten,

- Prüfung der *Soll-Haben-Identität* bei der Buchung

- Prüfung der *Konto- und Belegnummernkreise*,

- Lückenlosigkeit der *Belegnummernvergabe*,

- Kontrollen gegen doppelte *Belegnummernvergabe*,

- Plausibilität von *Steuerbuchungen* (Umsatzsteuerermittlung),

- Umsatzverprobung, Verkehrszahlenabstimmung.

Zur Absicherung der Ergebnisse können die Prüfungen durch den *stichprobenartigen Nachvollzug des Quellcodes* zur systemseitigen Fehlererkennung und zu den Plausibilitätskontrollen abgesichert werden.

5.2.2 Datenübernahmeverfahren an Schnittstellen

Ist die Prüfung der Schnittstellen bzw. die Anbindung von vorgelagerten oder nachgelagerten Systemen Bestandteil der Funktionsprüfung, bildet die Schnittstellendokumentation die Prüfungsgrundlage. Hieraus ist die eindeutige Schnittstellenbezeichnung, die Übertragungsdatei und der Datensatzaufbau der Schnittstelle zu entnehmen.

Grundsätzlich ist im Rahmen der Datenübertragung sicherzustellen, dass sämtliche zu exportierende Daten des Quellsystems vollständig und richtig in das Zielsystem gelangen. Die Prüfung der programmierten Verarbeitungsregeln gilt an dieser Stelle entsprechend. Im Rahmen der Prüfungshandlungen ist besonderer Wert auf die systemseitig verfügbaren Protokollierungen zur Datenübertragung zu legen.

Sie sind vollständig und nachvollziehbar, wenn neben dem Einzelnachweis der übertragenen Sätze die Angabe von Satzzählern und Kontrollsummen sowie des Übertragungszeitpunktes vorhanden ist. Daneben müssen Fehlerprotokolle den Nachweis von fehlerhaften Sätzen oder Sätzen mit Warnhinweisen enthalten.

5.2.3 Datensicherheit

Das Sicherheitskonzept einer Software beinhaltet die Differenzierung von Zugriffsberechtigungen, Datensicherungs- und Wiederanlaufverfahren (Recovery), Programmentwicklung, -freigabe und -wartung.

Zur Gewährleistung der Sicherheit und Integrität der Datenbestände sowie zum Zwecke einer adäquaten Funktionstrennung müssen Benutzungsbeschränkungen in Form von Zugriffsberechtigungen für zu definierende Programme, Bearbeitungsfunktionen, Geschäftsvorfallstypen, Dateien und Datenfelder vorhanden sein. Für die einzelnen Benutzer müssen systemseitig Benutzerkennungen hinterlegt werden können. Hierzu gehört die Definition von Profilen, die eine rollen-/stellenspezifische Zuordnung der Berechtigungen und die Zuordnung geheimer Passwörter ermöglichen.

Im Rahmen der Prüfung der programmierten Kontrollen ist festzustellen, ob[5]

- *autorisierte* und gegebenenfalls *nichtautorisierte Zugriffe* vom Anwendungssystem mit der Benutzerkennung *protokolliert* werden (z. B. auch Abweisung wiederholt fehlerhafter Login-Versuche, etc.),

- die turnusgemäße *Änderung von Passwörtern* systemseitig erzwungen wird,

- Passwörter einer definierten *Mindestlänge* unterliegen und triviale Wörter grundsätzlich von der Vergabe ausgeschlossen sind.

Für den Fall einer Störung oder Unterbrechung bei der Eingabe oder der systemseitigen Verarbeitung von Daten ist deren teilweise oder vollständige Rekonstruktion sicherzustellen. Die Ordnungsmäßigkeit des Datensicherungsverfahrens im Zusammenspiel mit dem möglichen Einsatz einer Datensicherungssoftware oder auf Betriebssystemebene ist ebenfalls zu prüfen.

5.2.4 Programmentwicklung und -freigabe

Die Einführung einer Verfahrensregelung für die Programmentwicklung und -freigabe beim Softwarehersteller ist notwendig, um zu verhindern, dass unautorisierte, ungewollte oder fehlerhafte Änderungen im IT-Umfeld wirksam werden.

Im Zuge der Programmentwicklung und -änderung muss seitens des Softwareherstellers sichergestellt werden, dass ein ordnungsgemäßer Zustand über ein nachvollziehbares und abgesichertes Programmentwicklungs- und Freigabeverfahren in einen neuen, ordnungs-gemäßen Zustand überführt wird (interne Qualitätssicherung).

Hieraus ergeben sich Anforderungen an die Planung, Dokumentation und die Durchführung der Verfahren, die folgenden Phasen berücksichtigen sollte:

- Anforderung zur Programmentwicklung/-änderung,
- Genehmigung der Anforderung,
- Planung, Umsetzung (Programmierung) und Dokumentation der Entwicklung,
- Testverfahren,

---

5 vgl. IDW-Prüfungsstandard PS 880: „Erteilung und Verwendung von Softwarebescheinigungen“ (Stand März 2010), S. 7

- Entwicklertests,
- Tests aus Anwendersicht (Qualitätssicherung),
- Abnahme,
- Dokumentation der Programmentwicklungen,
- Freigabe der Entwicklung,
- Produktivsetzung (Auslieferung).

5.3 Prüfung der Verfahrensdokumentation

Die *Funktionsprüfung beginnt man aus Effizienzgründen erfahrungsgemäß mit der Dokumentationsprüfung*. Dies ermöglicht es, in kurzer Zeit die Funktionen zur Datenerfassung und -übernahmen und den Datenfluss kennenzulernen und festzustellen, ob die Programmidentität gewährleistet ist. Die Verfahrensdokumentation besteht aus der Systemdokumentation und dem Anwenderhandbuch.

Die Dokumentationsprüfung beinhaltet[6, 7]:

- eine Beschreibung der sachlogischen Lösung,
- eine Beschreibung der programmtechnischen Lösung,
- eine Beschreibung, wie die Programmidentität gewahrt wird,
- eine Beschreibung, wie die Integrität der Daten gewahrt wird, und
- Arbeitsanweisungen für den Anwender.

Der Vorteil einer begleitenden Dokumentationsprüfung liegt für den Softwarehersteller darin, dass von neutraler Seite die Übereinstimmung zwischen den Softwarefunktionalitäten und der Verfahrensdokumentation überprüft wird, um so die Vollständigkeit, Richtigkeit, Übersichtlichkeit, Verständlichkeit und Zugänglichkeit der Beschreibungen zu sichern. Die Verfahrensdokumentation muss hiernach geeignet sein, einem sachverständigen Dritten, in angemessener Zeit das notwendige Verständnis über die dargestellten Abläufe zu verschaffen.

5.4 Prüfung der DSGVO-Konformität der Software

Im Hinblick auf die DSGVO-Grundsätze ergeben sich für eine datenschutzrechtliche Konformität der Software folgende Tatbestände, die im Rahmen dieser Prüfung beurteilt werden:

- Gewährleistung ausschließlich zweckbezogene (bzw. aufgabenbezogene) Verarbeitung und Auswertung [betrifft Grundsätze 1 bis 5]
- Gewährleistung Grundsatz Datenminimierung und datenschutzfreundliche Voreinstellungen im Programm [betrifft Grundsätze 2, 4, 5 und 7]
- Logische Sicherheit durch sichere Authentifizierung (Log-In) und differenziertes Berechtigungskonzept sowohl für die Anwendung als auch die mit der Anwendung in Verbindung stehende Datenbank [betrifft Grundsätze 1, 3, 4, 6, 8]
- Funktionsfähige und funktionssichere Software [betrifft Grundsätze 3, 6 und 8]
- Physikalische Sicherheit der mit der Anwendung in Verbindung stehende IT-Infrastruktur und Hardware [betrifft Grundsatz 8]

---

6 vgl. Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (kurz GoBS), veröffentlicht im Bundessteuerblatt 1995, Teil I, Nr. 18; S. 13 (GoBS)

7 vgl. IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1, Stand 24. September 2002)“, Textziffer 51- 56

- DS-konforme Archivierung und Löschung von personenbezogenen Daten [betrifft Grundsätze 3, 8 und 9]

Ausgehend von diesen Bewertungskriterien erfolgt eine Bewertung der Software.

5.5 Erstellung einer Softwarebescheinigung und eines Prüfungsberichtes

Wurden im Rahmen der vorstehend aufgeführten Prüfungen Mängel festgestellt, sind diese in einem entsprechenden Katalog zu erfassen und um eine Risikoeinschätzung zu ergänzen. Die Mängel müssen vor Erstellung der Softwarebescheinigung bzw. des Prüfungsberichtes behoben werden. Hiernach erfolgt eine Nachprüfung. Die Mängel werden nebst dem Ergebnis der Nachprüfung im Prüfungsbericht dargestellt und gewürdigt[8].

Der zu erstellende Prüfungsbericht sollte die „Grundsätze ordnungsmäßiger Berichterstattung bei Abschlussprüfungen“ (IDW-Prüfungsstandard PS 450) beachten. Hiernach erfolgt eine Beurteilung hinsichtlich der Einhaltung der Grundsätze ordnungsmäßiger Buchführung.

Für den Bericht ist folgender Aufbau zu empfehlen:

1. *Auftrag und Auftragsdurchführung* (Auftraggeber, eindeutige Abgrenzung des Prüfungsgegenstandes unter Nennung der geprüften Version und der Konfiguration der Testumgebung, gesetzliche Grundlagen, Art und Umfang der Prüfungshandlungen)
2. *Darstellung der Prüfungsergebnisse* (Verarbeitungsfunktionen, Verarbeitungsregeln, Softwaresicherheit und Dokumentation)
3. Zusammenfassung der Prüfungsergebnisse und Bescheinigung

Die Zusammenfassung beinhaltet das abschließende Ergebnis der Funktionsprüfung aus der die mögliche Erteilung einer Softwarebescheinigung abzuleiten ist, die bestätigt, dass die Software bei sachgerechter Anwendung eine Rechnungslegung ermöglicht, die den Grundsätzen ordnungsmäßiger Buchführung entspricht[9].

5.6 Durchführung von Folgeprüfungen

Aufgrund der fortlaufenden Weiterentwicklung von Software und der damit verbundenen Releaseplanungen der Softwarehersteller werden Folgeprüfungen notwendig, die den aktuellen Entwicklungsstand der Software beurteilen. Da gemäß IDW Prüfungsstandard PS 880 dieselben Maßstäbe und Kriterien wie bei der Erstprüfung heranzuziehen sind, ist es sinnvoll, die Erstprüfung so zu konzipieren, dass eine Folgeprüfung in effizienter und kostengünstiger Form durchgeführt werden kann. Dies kann dadurch geschehen, dass die definierten *Geschäftsvorfälle im Batch erfasst und gesichert* werden und erst anschließend zur Buchung bereitstehen.

Auf die gesicherten Stände kann im Rahmen einer Folgeprüfung zurückgegriffen werden, um Massentests vorzunehmen. Ergänzend sind gezielte Prüfungen bezüglich der geänderten weiterentwickelten Funktionalitäten vorzunehmen, die herstellerseitig in nachvollziehbarer und verständlicher Form (z. B. im Rahmen der Releaseinformation) dokumentiert sein müssen. Der Umfang der ergänzenden Prüfungen ist im Einzelfall festzulegen.

---

8 vgl. IDW-Prüfungsstandard PS 880: „Erteilung und Verwendung von Softwarebescheinigungen“ (Stand März 2010), S. 11

9 vgl. Philipp, Mathias, „Software-Zertifizierung nach IDW PS 880“, S. 3

6 Softwaretestate

Auf Wunsch besteht zusätzlich die Möglichkeit, dass einer unserer Wirtschaftsprüferpartner unsere Prüfungshandlungen und Testergebnisse der Funktionsprüfung nachvollzieht und mit unserer Unterstützung abschließend eine Softwarebescheinigung erstellt. In diesem Fall erstellt der Wirtschaftsprüfer auf Basis unserer Prüfungsfeststellungen eine Softwarebescheinigung. Für den Fall, dass Sie eine Softwarebescheinigung wünschen, erhalten Sie ein mit unserem Angebot abgestimmtes, eigenes verbindliches Angebot des Wirtschaftsprüfungspartners zur Testatserstellung.

Dennoch möchten wir an dieser Stelle auf die in den GoBD (= Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)) formulierte Bedeutung eines Testats hinweisen:

Nach Abschnitt 12 „Zertifizierung und Software-Testate“ der GoBD gilt entsprechend RZ 181:

„… „Zertifikate“ oder „Testate“ Dritter können bei der Auswahl eines Softwareproduktes dem Unternehmen als Entscheidungskriterium dienen, entfalten jedoch aus den in RZ. 179 genannten Gründen gegenüber der Finanzbehörde keine Bindungswirkung.“

In diesem Zusammenhang ist auch noch hinzuweisen, dass beim Einsatz einer testierten betriebswirtschaftlichen Anwendungssoftware zwar grundsätzlich ordnungsgemäße Ergebnisse erzielt werden können, diese jedoch nicht zwangsläufig richtig sind, da mögliche Anwendungsfehler oder die materielle Richtigkeit der Buchführung nicht systemseitig festgestellt werden können. Softwaretestate bestätigen daher nicht die anwenderseitig realisierte Buchführung und nicht die Bilanz. Vielmehr dient eine Softwarebescheinigung als Teilurteil dem Wirtschaftsprüfer zur Absicherung der Jahresabschlussprüfung bzw. der DV-Prüfung.

Die Softwarebescheinigung besitzt nur Gültigkeit, wenn der Releasestand der beim Anwender befindlichen Software und der testierte Releasestand übereinstimmen. Seitens des Wirtschaftsprüfers ist darüber hinaus festzustellen, ob anwenderseitig Eigenentwicklungen genutzt werden und die testierte Software eventuell verändert wurde. Auch in diesem Fall ist die Gültigkeit des Softwaretestates nicht gegeben oder sehr eingeschränkt. Darüber hinaus sind grundsätzlich die anwenderseitigen Organisationsstrukturen und die intern angewendeten Verfahren im Einzelfall zu berücksichtigen. Eine Softwarebescheinigung ersetzt demzufolge keine EDV-Systemprüfung beim Anwender.

Düsseldorf im Mai 2020

REVIDATA GmbH - Düsseldorf
Tel.: +49 211 655 843 95
Fax: +49 211 655 843 96
E-Mail: zentrale@revidata.de
Home: https://revidata.de

Literaturhinweise:

- Bundesministerium für Finanzen, „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“, veröffentlicht am 14. November 2014, GZ IV A 4 – S 0316/13/10003, DOK 2014/0353090,

- Fachausschuss für moderne Abrechnungssysteme (FAMA) 1/1987: „Grundsätze ordnungsmäßiger Buchführung bei computergestützten Verfahren und deren Prüfung, i.d.F. 11/1993,

- Institut der Wirtschaftsprüfer, IDW-Prüfungsstandard: „Erteilung und Verwendung von Softwarebescheinigungen“ (IDW-PS 880, Stand 10.03.2010),

- Institut der Wirtschaftsprüfer, IDW-Stellungnahme zur Rechnungslegung: „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“
- (IDW RS FAIT 1, Stand 24. September 2002),

- Institut der Wirtschaftsprüfer, Entwurf IDW-Stellungnahme zur Rechnungslegung: „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce (IDW ERS FAIT 2, Stand 1. Juli 2002),

- Institut der Wirtschaftsprüfer, IDW-Prüfungsstandard: „Abschlussprüfung bei Einsatz von Informationstechnologie“ (IDW PS 330, Stand 24. September 2002),

- Institut der Wirtschaftsprüfer, IDW-Prüfungsstandard: „Grundsätze ordnungsmäßiger Berichterstattung bei Abschlussprüfungen“ (IDW PS 450 1/1988 bzw. IDW EPS 450 n.F. vom 4. November 2002),

- Philipp, Mathias, „Software-Zertifizierung nach IDW PS 880“: in: „Durchsetzung von Ordnungsmäßigkeit durch aktive Interne Kontrollsysteme“ (http://www.mphilipp.de/papers/conquest 99.html).