SP_Data GmbH & Co. KG
Herford

Bericht über die Prüfung des Softwareproduktes
HRM-Archiv

PDF-Version

Rödl & Partner GmbH

Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Äußere Sulzbacher Straße 100
90491 Nürnberg
Telefon +49 (911) 91 93-0
Telefax +49 (911) 91 93-19 00
Internet www.roedl.de

Inhaltsverzeichnis

1. PRÜFUNGSAUFTRAG UND FACHLICHE GRUNDLAGEN

Mit der am 28. Februar 2019 erfolgten Annahme unseres Angebots vom 21. Februar 2019 wurden wir von den gesetzlichen Vertretern der

SP_Data GmbH & Co. KG
Herford

mit der Prüfung des Softwareprodukts „HRM-Archiv" in der Version 1.2019.19.04.01 gemäß IDW PS 880 beauftragt.

Ziel der Prüfung war es festzustellen, ob die im Rahmen der Speicherlösung angewandten Methoden bezüglich Datentransport, Datenabruf und Datenspeicherung ihre vorgegebenen Funktionen sowie die Prüfungsstandards erfüllen.

Die Software wurde unabhängig von deren Implementierung und Produktivsetzung beim Softwareanwender direkt beim Hersteller an einem Testsystem geprüft.

Der Auftragsgeber bzw. Softwarehersteller war für die Ordnungsmäßigkeit der zu prüfenden Software und Unterlagen verantwortlich.

Die durchgeführte Prüfung orientierte sich an folgenden Grundlagen:

- IDW Prüfungsstandard: Die Prüfung von Softwareprodukten (IDW PS 880)
- IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)
- IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)
- IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)
- die vom Bundesminister für Finanzen herausgegebenen „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD)

Die Prüfung wurde im April 2019 in den Geschäftsräumen der Gesellschaft vorgenommen. Die anschließende Berichtsfertigstellung wurde in unseren Geschäftsräumen durchgeführt.

Unsere Vorgehensweise, Umsetzung und Empfehlungen sind im folgenden Bericht erläutert.

Die Vollständigkeit und Richtigkeit sämtlicher uns übergebener Unterlagen sowie der Angaben, Erläuterungen und Auskünfte, die für die Prüfung und Bescheinigung der Software von Bedeutung waren, bestätigte die SP_Data GmbH & Co. KG in einer schriftlichen Erklärung.

Dem Auftrag liegen die als Anlage 5.1 beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften in der Fassung vom 1. Januar 2017 zu Grunde. Soweit in den für den Auftrag geltenden gesetzlichen Vorschriften eine Haftungshöchstsumme nicht festgelegt ist, bestimmt sich diese nach Nr. 9 der Allgemeinen Auftragsbedingungen und gegebenenfalls nach ergänzenden schriftlichen Vereinbarungen. Im Verhältnis zu Dritten sind Nr. 1 Abs. 2 und Nr. 9 der Allgemeinen Auftragsbedingungen maßgebend.

Die SP_Data GmbH & Co. KG darf den Prüfungsbericht nur in vollem Wortlaut einschließlich der mit diesem fest verbundenen schriftlichen Erklärung über Zweck des Auftrags und Haftungsbedingungen weitergeben. Rödl & Partner ist zur Weitergabe des Berichtes an Dritte nur mit ausdrücklicher Zustimmung der SP_Data GmbH & Co. KG befugt.

2. GEGENSTAND, ART UND UMFANG DER PRÜFUNG

2.1 Ausgangssituation

SP_Data unterstützt ihre Kunden mit innovativen Softwarelösungen in den Bereichen Personalabrechnung, Personalzeitwirtschaft, Personalmanagement, Bewerberverwaltung, Talentmanagement oder Bildungsmanagement. Hierbei fallen Belege an, die in elektronischen Akten gespeichert werden sollen. Hierfür hat SP_Data ein elektronisches Archiv entwickelt, welches nur in Zusammenhang mit den eigenen Produkten („Hauptanwendungen") für die Archivierung von Personalbelegen angeboten wird.

Da es sich hierbei auch um aufbewahrungspflichtige Unterlagen handelt, muss das Archivsystem eine revisionssichere Archivierung ermöglichen. Rödl & Partner wurde damit beauftragt, die Software nach dem IDW PS 880 Standard zu prüfen.

2.2 Prüfungsgegenstand und Kriterien

Gegenstand der Prüfung ist das Produkt „HRM-Archiv". Hierbei handelt es sich um ein elektronisches Archiv, welches zur sicheren elektronischen Archivierung von Dokumenten im Zusammenhang mit der Personalverwaltung und -abrechnung genutzt wird. Zwar kann das Archiv auch für die Ablage von Personaldokumenten von Drittsystemen genutzt werden, dies ist aber nicht der Fokus. Grundsätzlich muss eine der Hauptanwendungen der SP_Data GmbH & Co. KG eingeführt werden, damit auch das elektronische Archiv genutzt werden kann. Es handelt sich somit um keine Stand-Alone Lösung.

Die folgenden Sicherheitsziele stellen die zentralen Anforderungen in der IT dar:

- Vertraulichkeit: Vertraulichkeit verlangt, dass von Dritten erlangte Daten nicht unberechtigt weitergegeben oder veröffentlicht werden. Organisatorische und technische Maßnahmen – wie bspw. Verschlüsselungstechniken – umfassen u.a. Anweisungen zur Beschränkung der Übermittlung personenbezogener Daten an Dritte, die verschlüsselte Übermittlung von Daten an berechtigte Dritte, die eindeutige Identifizierung und Verifizierung des Empfängers von Daten oder die Einhaltung von Löschfristen gespeicherter personenbezogener Daten.

- Verfügbarkeit: Verfügbarkeit verlangt zum einen, dass das Unternehmen zur Aufrechterhaltung des Geschäftsbetriebs die ständige Verfügbarkeit der IT-Infrastruktur, der IT-Anwendungen sowie der Daten gewährleistet. Zum anderen müssen die IT-Infrastruktur, die IT-Anwendungen und Daten sowie die erforderliche IT-Organisation in angemessener Zeit funktionsfähig bereitstehen. Daher sind z.B. geeignete Back-up-Verfahren zur Notfallvorsorge einzurichten. Maßnahmen zur Sicherung der Verfügbarkeit sind erforderlich, um den Anforderungen nach Lesbarmachung der Buchführung gerecht zu werden.

- Integrität: Integrität von IT-Systemen ist gegeben, wenn die Daten und die IT-Infrastruktur sowie die IT-Anwendungen vollständig und richtig zur Verfügung stehen und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind. Organisatorische Maßnahmen sind geeignete Test- und Freigabeverfahren. Technische Maßnahmen sind z.B. Firewalls und Virenscanner. Die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung setzt voraus, dass neben den Daten und IT-Anwendungen auch die IT-Infrastruktur nur in einem festgelegten Zustand eingesetzt wird und nur autorisierte Änderungen zugelassen werden.

Insbesondere die Vertraulichkeit ist beim Umgang mit Mitarbeiterdaten aufgrund der DSGVO von großer Bedeutung.

Die hier aufgeführten Sicherheitsziele sind Grundlage unserer Prüfung.

Die Prüfung umfasst die Beurteilung darüber, ob die Kriterien durch die Verarbeitungsfunktionen und durch das programminterne Kontrollsystem angemessen umgesetzt sind und ob eine aussagefähige Verfahrensdokumentation vorliegt. Die Wirksamkeit der Programmfunktionen wird anhand von Testfällen beurteilt.

Zu den Programmfunktionen zählen:

- Dokumentenablage
- Revisionssicherheit
- Verschlüsselung & Komprimierung
- Protokollierung
- Versionierung[1]

Hierfür werden einerseits die Testfälle des Auftraggebers berücksichtigt und andererseits eigene Testfälle durchgeführt.

Die Prüfung erfolgte nach berufsüblicher Vorgehensweise und war auf die Beurteilung der Ordnungsmäßigkeit und Sicherheit des Verfahrens ausgerichtet.

2.3 Art und Umfang der Prüfung

Die Prüfung erfolgte gemäß IDW PS 880 „Erteilung und Verwendung von Softwarebescheinigungen" für folgende Bereiche:

- Notwendige Verarbeitungsfunktionen,
- Softwaresicherheit und
- Dokumentation.

Die Softwareprüfung wurde so geplant und durchgeführt, dass mit hinreichender Sicherheit beurteilt werden kann, ob das Softwareprodukt bei sachgerechter Anwendung eine ordnungsgemäße Archivierung ermöglicht und den auftragsgemäß zugrunde gelegten Kriterien entspricht. Dabei werden sowohl die Softwareentwicklung als auch die Softwarefunktionen und Prüfkriterien einer Beurteilung unterzogen.

Die Prüfung der notwendigen Verarbeitungsregeln bezog sich auf ausgewählte Stichproben, die Rückschlüsse auf den ordnungsmäßigen und sicheren Ablauf der DV-Anwendung zulassen. Zur Prüfung der Software wurde eine Testumgebung aufgebaut.

Unsere Arbeiten führten wir anhand der uns vorgelegten Dokumentation, durch Gespräche mit Mitarbeitern der SP_Data GmbH & Co. KG sowie durch systemgestützte Prüfungshandlungen durch.

Wir haben die Prüfung (mit Unterbrechungen) im April 2019 in den Räumen der SP_Data GmbH & Co. KG in Herford und in unseren Geschäftsräumen durchgeführt. Art und Umfang unserer Prüfungshandlungen haben wir in unseren Arbeitspapieren festgehalten.

Alle zur Prüfung erforderlichen Unterlagen wurden uns zur Verfügung gestellt. Die gewünschten Auskünfte und Erläuterungen wurden uns von den Mitarbeitern der Gesellschaft erteilt. Unsere Umsetzung und Beurteilungen beruhen auf dem zum Prüfungszeitpunkt vorgefundenen Stand des Testsystems.

---

[1] Unter dem Begriff Versionierung oder auch Versionsverwaltung versteht man ein System, das zur Erfassung von Änderungen an Dokumenten oder Dateien verwendet wird. Bei jeder Änderung an einem Dokument wird in einem entsprechenden Archiv eine neue Version dieses Dokuments (mit Zeitstempel und Benutzerkennung) abgelegt.

2.4 Abgrenzung des Auftrags

Gegenstand unseres Auftrags war weder die Beurteilung der Zweckmäßigkeit der eingesetzten Betriebssysteme und der Betriebssicherheit, noch die Beurteilung des IT-Betriebes und der laufenden Systemadministration. Auch waren Systeme und Programmteile, welche nicht in der uns zur Verfügung gestellten Dokumentation aufgeführt oder nicht für die Datenspeicherung relevant sind, nicht Bestandteil unserer Prüfung.

Ebenfalls geben wir keine Empfehlungen, die auf die Effizienz und Effektivität gewählter Verfahren vor dem Hintergrund unterschiedlicher Systemkonfigurationen bzw. systemischer Ausprägungen hinweisen.

Der Einsatz der Anwendung „HRM-Archiv" beim Anwender, d. h. in einer konkreten Ablauforganisation, war nicht Prüfungsgegenstand. Aussagen zu organisatorischen Regelungen werden daher im Rahmen dieser Prüfung nur dann getroffen, wenn für bestimmte, nicht vorhandene DV-gestützte Funktionen organisatorische Maßnahmen vom Anwender erforderlich sind.

Bei der Durchführung der Softwareprüfung in Stichproben in Verbindung mit den immanenten Grenzen einer Softwareprüfung besteht ein unvermeidliches Risiko, dass selbst wesentliche Fehler und Fehlfunktionen unentdeckt bleiben können.

2.5 Testsystem

Unsere Prüfungshandlungen führten wir in einem Testsystem mit den folgenden Komponenten und Versionen durch:

Komponente	**Version**
HRM-Archiv	1.2019.19.04.01
Datenbank-Sever - Betriebssystem - DB-Version	 Windows 10 Microsoft SQL Server 2016
Fileserver: - Betriebssystem	 Windows 10

3. PRÜFUNGSERGEBNISSE

3.1 Verarbeitungsfunktionen

Die folgenden Verarbeitungsfunktionen sind entweder als eigenständige Funktionen im HRM-Archiv oder in Kombination mit einer der Hauptanwendungen von SP_Data umgesetzt. Das Archivsystem ist nicht als eigenständiges Produkt ohne mindestens eine der Hauptanwendungen nutzbar.

3.1.1 Dokumentenablage

Anforderung

Daten müssen sicher gespeichert sein, um sie gegen Datenverlust zu schützen.

Umsetzung

Die Ablage erfolgt durch die Hauptanwendung über eine fest definierte Programmschnittstelle (API) des Archivsystems. Der Ablageort wird dabei in einer Konfigurationsdatei hinterlegt. Für die Speicherung wird ein Fileserver des Kunden verwendet. Die archivierten Belege werden in einer komprimierten Datei im Format 7-zip gespeichert. Bei der Archivierung wird ein Hash-Wert des zu archivierenden Dokuments erzeugt und in einer Datenbank gespeichert, um eventuelle Änderungen daran feststellen zu können.

Hash-Funktionen werden angewandt, um eine Prüfsumme zu einem Objekt zu berechnen. Dadurch wird das Objekt eindeutig identifiziert, ohne etwas über den Inhalt zu verraten. Änderungen an Daten, beispielsweise durch technische Störeinflüsse oder absichtliche Manipulation, können erkannt werden, da sich hierdurch auch die Prüfsummen der Dateien ändern.

3.1.2 Revisionssicherheit

Belege werden revisionssicher archiviert, wenn sie während der gesetzlichen Aufbewahrungsfrist weder gelöscht noch geändert werden können.

3.1.2.1 Vorhaltezeit / Löschfristen

Anforderung

Es müssen die gesetzlichen Vorschriften zu den Aufbewahrungsfristen (Vorhaltezeiten) eingehalten werden, um sicherzustellen, dass Dokumente nicht während ihrer gesetzlichen Aufbewahrungspflicht gelöscht werden können. In diesem Zusammenhang ist auf die Integrität der Datenbestände zu achten.

Umsetzung

Die Vorhaltezeit bzw. Löschfristen werden über den Dokumententyp (z.B. 120 Monate bei Abrechnungsdokumenten) von der archivierenden Hauptanwendung festgelegt und dem HRM-Archiv mitgegeben. Demnach findet keine direkte Verwaltung der Vorhaltezeit im HRM-Archiv statt.

Die Löschung von archivierten Daten erfolgt dann über die Hauptanwendung. Dort werden jedoch nur Dokumente aufgelistet, welche bereits gelöscht werden können. Dokumente bei denen die Vorhaltezeit noch nicht abgelaufen ist, können nicht gelöscht werden.

3.1.2.2 Unveränderbarkeit

Anforderung

Eine Eintragung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist.

Umsetzung

Im Archiv werden unterschiedliche Belegarten aus dem Personalbereich gespeichert. Hierbei handelt es sich zum Großteil um personenbezogene Daten, welche im Sinne der DSGVO besonders schützenswert sind. Die Unveränderbarkeit soll daher nicht durch ein striktes Unterbinden einer Löschung umgesetzt werden, was ggf. dem Löschrecht eines Betroffenen im Sinne der DSGVO widersprechen könnte. Stattdessen sollen Änderungen oder Manipulationen an den Daten jederzeit festgestellt werden können, um den Originalzustand aus den bestehenden Datensicherungen wiederherstellen zu können.

Eine Integritätsprüfung ist standardmäßig als Funktionalität innerhalb des Archivsystems verfügbar und muss bei Ausführung manuell vom Client aus angestoßen bzw. durchgeführt werden. Eine automatisierte Prüfung in regelmäßigen Zyklen existiert zu diesem Zeitpunkt noch nicht.

Für die Integritätsprüfung wird sowohl vom zu archivierenden Dokument als auch von der finalen ZIP-Datei ein Hash-Wert gebildet.

Die Integritätsprüfung erfolgt somit in vier Stufen:

1. Datei ist vorhanden
2. Hash-Wert der komprimierten Datei stimmt überein
3. Datei kann mit dem hinterlegten Passwort entpackt werden
4. Hash-Wert des Dokuments stimmt überein

Dennoch sollten die Zugriffsrechte auf den Speicherort auf ein Minimum reduziert werden. Auch der Zugriff auf die Archivdatenbank muss eingeschränkt sein, damit die Integrität der Hash-Werte nicht gefährdet ist.

3.1.2.3 Verfügbarkeit

Anforderung

Die archivierten Belege müssen während der Dauer der Aufbewahrungsfrist verfügbar sein und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.

Umsetzung

Die genaue Umsetzung der Sicherstellung der Verfügbarkeit kann der jeweilige Kunde der Software selbst beeinflussen. Die Hauptanwendung lässt eine Löschung nicht vor Ablauf der gesetzlichen Aufbewahrungspflicht zu. Die Verfügbarkeit könnte somit gefährdet werden, wenn die Dateien durch Zugriff auf das Dateisystem oder durch einen Systemausfall verloren gehen.

Eine Löschung auf dem Fileserver kann durch ein strenges Berechtigungskonzept verhindert werden. Auf den Archivpfad sollte niemand Änderungs- und Löschrechte haben – die Berechtigungen von Domain-Administratoren lassen sich allerdings nicht einschränken.

Ein Datenverlust bei einem Systemausfall kann durch ein Redundanz-Konzept, z.B. Speicherung auf einem Cluster oder geeignete Datensicherungsverfahren, verhindert werden. Das Archivsystem muss mit Blick auf die technische Funktionsfähigkeit selbständig durch den Kunden überwacht werden, um technische Probleme zeitnah festzustellen. Die Sicherung der HRM-Archiv Datenbank, der Dateien und File-Struktur auf dem Server und der Konfigurations- und *key-Dateien aus dem Web-Verzeichnis muss kundenseitig erfolgen.

Der Aufruf der Belege erfolgt über die Hauptanwendung. Eine direkte Recherche und Aufruf der Belege im Archivsystem ist nicht vorgesehen, da das Archivsystem nicht ohne eine der Hauptanwendungen vertrieben wird. Der Aufruf erfolgt über eine einheitlich vorgegebene API.

3.1.3 Verschlüsselung & Komprimierung

Anforderung

Um den Schutz von sensiblen Daten, insbesondere im Personalbereich zu gewährleisten, muss die Lesbarkeit von Daten durch nicht autorisierte Personen verhindert werden. Dies geschieht durch eine Verschlüsselung der Daten, bevor sie ins Archiv übertragen werden. Damit die Verschlüsselung dies gewährleisten kann, darf sie nur sehr schwer zu entschlüsseln sein und muss hohen Sicherheitsstandards genügen. Um eine möglichst effektive und effiziente Speichernutzung zu gewährleisten, ist es sinnvoll diese in komprimierter Form abzuspeichern.

Umsetzung

Der Transport der Belege in das Archivsystem kann auf sicherem Wege erfolgen. Hierfür muss die TLS-Verschlüsselung eingerichtet werden. Dies ist nicht standardmäßig eingerichtet, sondern muss von jedem Kunden individuell vorgenommen werden.

Die Dateien werden im, vom Endanwender (Administrator) konfigurierten, Pfad in einem zufällig ausgewählten Verzeichnis (0000-9999) abgelegt. Der Dateiname wird hierbei ebenfalls zufällig mittels einer GUID, der die Bindestriche entfernt werden, erzeugt und enthält keine Dateiendung (z. B. „cbc0177f798c4d308b2805e30d623d86“).

Die Datei selbst ist eine mittels AES-256 geschützte ZIP-komprimierte Datei. Für das Passwort für die Verschlüsselung wird das Passwort verwendet, das der Administrator beim Anlegen des Archivs definiert hat. Zusätzlich wird dies mit der SyncID des Dokuments sowie der Versionsnummer gesalzen. Dies entspricht dem aktuellen Stand der Technik.

Das Passwort in der Konfigurationsdatei wird mit AES-256 verschlüsselt abgespeichert. Hierfür wird bei der Installation des Archivs eine 1.024 Byte große Schlüsseldatei erzeugt, mit der das Passwort verschlüsselt wird. Zusätzlich wird ein Salt[2] erzeugt, welches in der Konfiguration mit abgelegt wird. In der Implementation der Verschlüsselung wird zusätzlich noch ein geheimer Pepper[3] verwendet.

Das daraus errechnete Passwort ist somit für jede Datei und Version unterschiedlich und wird nach oben beschriebenem Verschlüsselungsverfahren in der Datenbank gespeichert.

3.1.4 Protokollierung

Anforderung

Veränderungen und Löschungen von und an elektronischen Buchungen oder Aufzeichnungen müssen so protokolliert werden, dass die Voraussetzungen des § 146 Absatz 4 AO bzw. § 239 Absatz 3 HGB erfüllt sind. Für elektronische Dokumente und andere elektronische Unterlagen, die gem. § 147 AO aufbewahrungspflichtig und nicht Buchungen oder Aufzeichnungen sind, gilt dies sinngemäß.

Umsetzung

Änderungen im Archiv werden direkt in der Datenbank protokolliert. Dabei ist nachvollziehbar, welcher Anwender zu welchem Zeitpunkt Dokumente in das Archiv hochgeladen, bearbeitet oder gelöscht hat. Zusätzlich dazu werden auch Änderungen an Attributen gespeichert. Zukünftig soll neben dem neuen Wert auch noch der alte Wert verfügbar sein. Das Öffnen von Dokumenten im Archiv wird nicht protokolliert.

3.1.5 Versionierung

Anforderung

Die Unveränderbarkeit der elektronischen Dokumente und elektronischen Unterlagen kann sowohl hardwaremäßig (z. B. unveränderbare und fälschungssichere Datenträger) als auch softwaremäßig (z. B. Versionierungen) gewährleistet werden.

Umsetzung

Bei jeder Änderung am Dokument wird automatisch eine neue Dokumentenversion erzeugt. Demnach können Änderungen in der selben Version nicht gespeichert werden, sondern müssen in einer neuen Version gesichert werden. Zukünftig soll das Öffnen von Dokumenten im Schreibschutz-Modus möglich sein.

---

[2] Salt bezeichnet in der Kryptographie eine zufällig gewählte Zeichenfolge, die an einen gegebenen Klartext vor der Verwendung als Eingabe einer Hashfunktion angehängt wird. Es wird häufig für die Speicherung und Übermittlung von Passwörtern benutzt. Bei der Überprüfung eines Passworts wird jedoch nicht jedes Mal ein neuer Salt erzeugt, da sich sonst der entstandene Hashwert von dem gespeicherten unterscheiden und somit das Passwort abgelehnt würde. Deshalb wird bei der Generierung eines Passworts der dort verwendete Salt zusammen mit dem entstandenen Hashwert in einer Datenbank gespeichert.

[3] Um Angriffe zu erschweren, kann das Passwort mit einer vom Server gewählten und geheimgehaltenen Zeichenfolge kombiniert werden, bevor der Hash-Wert berechnet wird. Diese Zeichenfolge wird Pepper (Pfeffer) genannt und ist normalerweise für alle Passwörter auf einem Server gleich. Wenn der Pepper zusätzlich noch jeweils für jedes Passwort geändert wird, kann die Sicherheit weiter erhöht werden. Der Pepper wird nicht in derselben Datenbank gespeichert wie der Hash, sondern an einem anderen und möglichst sicheren Ort hinterlegt. Erlangt ein Angreifer nur Zugriff auf die Datenbank (z. B. per SQL-Injection), so erfährt er zwar immer noch die Hash-Werte, diese Hash-Werte stammen aber nicht mehr von schwachen Passwörtern, sondern von Kombinationen von Passwort und einem starken Pepper.

3.2 Softwaresicherheit

3.2.1 Passwörter

Anforderung

Der Passwortschutz eines IT-Systems soll gewährleisten, dass nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung nachweisen.

Umsetzung

In der Hauptanwendung können Komplexitätsvorgaben für Passwörter hinterlegt werden. Im HRM-Archiv selbst können keine Passwortanforderungen gesetzt werden. Allerdings muss sich auch der individuelle Anwender nicht mit seiner Kennung am HRM-Archiv anmelden.

Für die Verwendung des HRM-Archivs sind mehrere Benutzer notwendig.

1. Das Archivsystem benötigt eine eigene SQL-Datenbank. Hierfür muss ein Datenbankbenutzer angelegt werden. Beim automatischen Erstellen der Datenbank während der Installation des Archivs wird dieser abgefragt. Das Passwort des Datenbankbenutzers sollte nach den Sicherheitslinien des eigenen Unternehmens gewählt werden.

2. Bei der Installation des Archivs über den Installationsassistenten kann ein komplexes Passwort für den Zugriff auf das Archivsystem vergeben werden. Dieses wird anschließend verschlüsselt und in der Parameterdatei gespeichert. Eine Überprüfung in Hinsicht der Passwortkomplexität findet dabei jedoch nicht statt. Dieser wird für den Zugriff auf die APIs des Archivsystems genutzt und darf die Schnittstelle aufrufen – alle anderen dürfen sie nicht aufrufen.

3. Der Zugriff auf das Filesystem erfolgt über den Benutzer, unter dem das Archivsystem als Dienst auf dem Fileserver IIS läuft. Dieser muss dann entsprechende Berechtigungen auf das Filesystem haben.

3.2.2 Differenzierung von Zugriffsberechtigungen

Anforderungen

Mitarbeiter sollten generell nur Zugriff auf Daten haben, die sie für ihre tägliche Arbeit benötigen, d.h. die Berechtigungsvergabe sollte nach dem Minimalprinzip vergeben werden. Eine Anmeldung ohne Benutzername und Passwort darf nicht möglich sein, da sonst den Benutzern keine entsprechenden Benutzerberechtigungen zugewiesen werden können.

Umsetzung

Um sich am HRM-Archiv anmelden zu können, wird ein Standardbenutzer bzw. Systembenutzer mit Name und Passwort benötigt. Dieser Benutzer wird in der Konfiguration der Anwendung hinterlegt. Da für alle Zugriffe derselbe Benutzer im Archivsystem benutzt wird, verfügt das Archiv selbst über kein eigenes Berechtigungskonzept. Die Berechtigungssteuerung erfolgt über die Hauptanwendung.

Über den persönlichen Benutzernamen in der Anwendung werden dann die Berechtigungen ermittelt und gesteuert. Dies liegt daran, dass die Dateien nur über die Hauptanwendung aufgerufen werden können, nachdem sie ins Langzeitarchiv gespeichert wurden.

Dateisystem: Es muss sichergestellt werden, dass der Benutzer, unter dem die Web-Anwendung läuft, lesenden und schreibenden Zugriff auf die File-Struktur bekommt. Anderen Benutzern ist nach Möglichkeit der Zugriff zu entziehen.

Datenbank: Für die HRM-Archiv Tabellen sollte ein eigener Datenbankbenutzer verwendet werden. Das gilt auch, wenn dieselbe Datenbank wie für die Personalabrechnung oder Zeitwirtschaft verwendet wird.

HRM-Archiv: Für den Zugriff auf die APIs des HRM-Archivs ist ein gesonderter Benutzer anzulegen. Hierrüber können die Funktionen des HRM-Archivs genutzt werden. Nur mit diesem Benutzer können auch Drittprogramme auf das HRM-Archiv zugreifen.

3.2.3 Löschung von Archivdaten

Anforderungen

Es muss sichergestellt sein, dass nach Ablauf der festgelegten Speicherfristen, die Daten gelöscht werden. Löschung bedeutet in diesem Zusammenhang eine physikalische Löschung. Eine Markierung als „gelöscht", mit der Folge, dass die Daten nicht mehr angezeigt werden, ist nicht ausreichend.

Umsetzung

Sobald für ein Dokument die Speicherfrist abgelaufen ist, kann in der Hauptanwendung ausgewählt werden, ob einzelne Versionen oder das gesamte Dokument (mit allen Versionen) gelöscht werden soll. Bei der Löschung werden dann die entsprechenden Versionen und alle zugehörigen Datenbank-Informationen eines Dokuments mit der übergebenen SyncID aus dem Archiv gelöscht. Die physikalischen Dateien auf dem File-Server werden dabei auch gelöscht. Anschließend wird ein Status zurückgegeben, ob das Löschen erfolgreich war. Handelt es sich bei der Version um die einzige Version des Dokuments, wird auch der Haupteintrag und die Attribute aus der Datenbank gelöscht.

Zusätzlich gibt es die Funktion Löschfristenprüfung, bei der alle Dokumente, bei denen die Aufbewahrungsfrist bereits abgelaufen ist, angezeigt und auf einmal gelöscht werden können. Die Prüfung erfolgt dabei auf Basis der Felder Bezugsjahr und Bezugsmonat.

Außerdem hat der Anwender die Möglichkeit, bei Dokumenten eine manuelle Löschsperre zu setzen. Auch wenn die Vorhaltezeit bereits abgelaufen ist, können diese dann nicht gelöscht werden.

Gelöschte Versionen können nicht mehr aus dem Archiv zurückgeholt bzw. wiederhergestellt werden. Damit sind die Metadaten auch nicht mehr verfügbar. Die einzige Möglichkeit, versehentlich gelöschte Dokumente wiederherzustellen, ist über ein Restore des manuell durchgeführten BackUps vom Archiv und dem File-Server.

Zukünftig sollen bei der Löschung einer Version in der Hauptanwendung die Metadaten (z.B. Personalnummer) im Protokoll weiterhin vorhanden sein. Aktuell ist nur beschrieben welche Dokumenten-IDs gelöscht wurden.

3.2.4 Softwareentwicklung, -wartung und –freigabe

Es bestehen in dieser Phase typischerweise folgende Risiken:

- Risiken aufgrund fehlender Nachvollziehbarkeit in der Entwicklung
- Risiken aufgrund mangelnder Qualitätssicherung und unzureichenden Testverfahren

3.2.4.1 Softwareentwicklung

Die Entwicklung wird vom SP_Data Entwicklungsteam durchgeführt. Die Module werden dabei nach einem etablierten Entwicklungsprozess entwickelt und getestet. Nach der Entwicklung wird die Software an die Mitarbeiter der Qualitätssicherung weitergegeben.

Es existiert ein Code Styleguide, der als Leitfaden zum einheitlichen Schreiben von Quellcode (GUI/Maskentypen, Datenbankdesign, Quellcode/Formatierung/Konventionen) für alle Entwickler dient. Sofern vorhandener Quellcode nicht diesen Richtlinien entspricht, sollen Erweiterungen trotzdem gemäß dieses Styleguides implementiert werden.

Für die Versionsverwaltung werden VisualSVN Server und TortoiseSVN verwendet. Dabei existiert ein zentrales Repository für sämtliche Produkte und Module von SP_Data. Auf dem Quellcodeverwaltungssystem ist eine Benutzerverwaltung mit Rechtevergabe eingerichtet. Die Qualitätssicherung hat zum Teil lesenden Zugriff auf den Quellcode. Die Entwickler hingegen sind alle mit der Rolle „Entwicklung" gleich berechtigt.

Generell ist zu jeder Zeit nachvollziehbar, welcher Entwickler zu welchem Zeitpunkt was entwickelt oder geändert hat.

3.2.4.2 Qualitätssicherung (QS)

Anforderungen

Die Qualitätssicherung hat generell die Aufgabe, Risiken und Fehler im Softwareentwicklungsprozess aufzudecken und zu beheben. Zu den möglichen Risiken in diesem Prozess gehören u.a.:

- fehlende Freigabeverfahren
- unzureichende Fehlerbearbeitung
- mangelhaftes Laufzeitverhalten und mangelnde Verwendbarkeit

Nach dem IDW PS 880 besteht im Rahmen von Tests das Risiko unzureichender Testkonzepte, ungeeigneter Testverfahren und –tools sowie fehlender Dokumentation der Testergebnisse.

Umsetzung

Die Qualitätssicherung übernimmt in diesem Zusammenhang alle Tests der verschiedenen Versionen der Softwareprodukte und leitet aufkommende Fehler an die Entwicklung zurück.

Die Qualitätssicherung wird von den Mitarbeitern des Teams QS der SP_Data durchgeführt. Hierfür wurde ein durchgängiger Support- bzw. Qualitätsmanagementprozess etabliert. Durch die Qualitätssicherung kann somit das 4-Augen-Prinzip umgesetzt werden, da die Entwickler nicht ihre selbst erstellten Entwicklungen testen und beurteilen können.

<u>Tests</u>

Ein wichtiger Aspekt der Qualitätssicherung ist die Durchführung von Tests. Durch Tests der Software soll eine fehlerhafte Funktionsweise der Software ausgeschlossen werden. Die Tests müssen systematisch erfolgen, alle Bereiche der Entwicklung des Softwareprodukts abdecken und ausreichend dokumentiert sein.

Es stehen verschiedene Konzepte und Systeme zur Testdurchführung zur Verfügung:

- Manuelle Tests werden von den Mitarbeitern der Qualitätssicherung, Entwicklung und Support / Beratung durchgeführt. Dabei werden Testversionen und frühzeitige Versionsstände der Software (Nightly Build) intern verteilt.

- Die automatisierten Testverfahren werden seitens der Qualitätssicherung durchgeführt und kontinuierlich weiterentwickelt. Hierbei werden Unit-Tests (Prüfung der korrekten Funktionalität von Einzelteilen der Software), GUI-Tests (Automatisierte Aufrufe von Masken und Dialogen zur Simulation von Anwender-Szenarien), Integrationstests (Durchführung verschiedener komplexer Prozesse in den verschiedenen Anwendungen) und Anwendungsfallspezifische Tests eingesetzt.

Freigabe

Die technische Freigabe bzw. Bereitstellung der Software erfolgt seitens der Qualitätssicherung. Anschließend wird der Kunde per E-Mail informiert und kann die neuste Version bzw. Updates und Patches über die Homepage herunterladen. Die dazugehörige Installation erfolgt dann über einen Installationsassistenten.

3.3 Dokumentation

Anforderungen

Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) setzten eine aussagefähige und aktuelle Verfahrensdokumentation voraus, die alle System- bzw. Verfahrensänderungen inhaltlich und zeitlich lückenlos dokumentiert. Dazu gehören eine Anwenderdokumentation, eine Technische Dokumentation und eine Betriebsdokumentation.

Umsetzung

Sämtliche Dokumentationen sind aktuell gehalten und in deutscher Sprache verfügbar.

Eine ausführliche Anwenderdokumentation ist zu diesem Zeitpunkt (16.05.2019) in der Vorbereitung, jedoch noch nicht verfügbar. Für die Installation des HRM-Archivs ist eine Benutzeranweisung vorhanden.

Es existiert eine technische Dokumentation, welche das Benutzermanagement, die Installation, Datensicherung, Datenwiederherstellung und Dateiablage beinhaltet. Des Weiteren gibt es eine ausführliche Schnittstellendokumentation, welche die einzelnen Funktionen des HRM-Archivs beschreibt.

Durch die Weiterentwicklung auf Basis des Scrum-Prinzips wird sichergestellt, dass bei Veränderung der Systemkonfiguration entsprechende Anpassungen in der Dokumentation vorgenommen werden.

4. SOFTWAREBESCHEINIGUNG

An die gesetzlichen Vertreter SP_Data GmbH & Co. KG**.**

Die gesetzlichen Vertreter der SP_Data GmbH & Co. KG, Herford, haben uns am 28. Februar 2019 beauftragt, eine Prüfung des Softwareprodukts

HRM-Archiv

in der Version 1.2019.19.04.01

vorzunehmen.

Die gesetzlichen Vertreter der Gesellschaft sind für das Softwareprodukt und die Planung, Durchführung und Überwachung der Softwareentwicklung verantwortlich. Diese Verantwortung wird durch unsere Prüfung nicht berührt. Unsere Aufgabe ist es, auf Grundlage der von uns durchgeführten Prüfung eine Beurteilung über das Softwareprodukt abzugeben.

Wir haben unsere Prüfung unter Beachtung des IDW Prüfungsstandards: Die Prüfung von Softwareprodukten (IDW PS 880) durchgeführt. Danach ist die Softwareprüfung so zu planen und durchzuführen, dass mit hinreichender Sicherheit beurteilt werden kann, ob das Softwareprodukt bei sachgerechter Anwendung eine sichere und vollständige Archivierung der Daten ermöglicht und den auftragsgemäß zugrunde gelegten Kriterien entspricht.

Dies umfasst unsere Beurteilung, ob die Kriterien durch die Verarbeitungsfunktionen und durch das programminterne Kontrollsystem angemessen umgesetzt sind sowie ob eine aussagefähige Verfahrensdokumentation vorliegt. Die Wirksamkeit der Programmfunktionen wurde anhand von Testfällen beurteilt.

Unserer Prüfung haben wir auftragsgemäß folgende Kriterien zugrunde gelegt:

- Handels- und steuerrechtliche Vorschriften zur Ordnungsmäßigkeit der Buchführung (§§ 238 – 239 und 257 HGB sowie §§ 145 bis 147 AO),
- die vom Bundesminister für Finanzen herausgegebenen „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD)
- IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)
- IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)

Da Softwareprodukte an die Anforderungen des Einsatzgebiets angepasst werden, kann sich unser Urteil ausschließlich darauf beziehen, dass das Softwareprodukt bei sachgerechter Anwendung ermöglicht, den Kriterien zu entsprechen.

Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse ermöglicht das von uns geprüfte Softwareprodukt HRM-Archiv bei sachgerechter Anwendung eine sichere und vollständige Archivierung der Daten und erfüllt die Anforderungen aus den vorstehend aufgeführten Standards.

Für eine sachgerechte Anwendung und somit einen ordnungsgemäßen Betrieb sollten bei Kundeninstallationen die folgenden Maßnahmen durchgeführt werden:

- Datenhaltung / Sicherstellung der Verfügbarkeit:
  - Die Vorhaltezeit der Belege, d.h. die Zeit die sie mindestens aufbewahrt werden müssen, ist vom Kunden in der Hauptanwendung selbst festzulegen und einzurichten.
  - Für die sichere Übertragung in das Archivsystem sollte eine TLS-Verschlüsselung eingerichtet werden.
  - Für die sichere Dateiablage auf dem Fileserver sollte ein Redundanz-Konzept, z.B. in Form eines Speicherclusters, eingesetzt werden. Gleichzeitig muss der Ablageort in das Datensicherungskonzept eingebunden werden und es sollten regelmäßig Wiederherstellungstests durchgeführt werden, um die Funktionsfähigkeit der Backups zu garantieren. Die SQL-Datenbank ist ebenfalls in die Datensicherung einzubeziehen.
  - Das Archivsystem muss mit dem Blick auf die technische Funktionsfähigkeit selbstständig durch den Kunden überwacht werden, um technische Probleme zeitnah festzustellen.
  - Um die Verfügbarkeit der Originalbelege sicherzustellen, sollte in regelmäßigen Zyklen eine Integritätsprüfung durchgeführt werden, so dass die ursprünglichen Belege notfalls wiederhergestellt werden können.

- Berechtigungen / Zugriffsrechte:
  - Es muss sichergestellt werden, dass der Benutzer, unter dem der Service auf dem Fileserver IIS läuft, über einen lesenden und schreibenden Zugriff auf die File-Struktur verfügt. Anderen Benutzern sollte der Zugriff nicht gestattet werden. Kein anderer Benutzer sollte Änderungs- und Löschrechte besitzen.
  - Da im HRM-Archiv selbst keine Passwortanforderungen gesetzt werden können, sollten in der Hauptanwendung hohe Komplexitätsvorgaben für Passwörter hinterlegt werden.
  - Um die Risiken eines unberechtigten Zugriffs zu minimieren, sollte das Passwort des Archiv-Benutzers für den Zugriff auf das Archivsystem, welches bei der Installation des Archivs über den Installationsassistenten vergeben wird, komplex sein.
  - Für die HRM-Archiv Tabellen sollte ein eigener Datenbankbenutzer verwendet werden. Das gilt auch, wenn die selbe Datenbank wie für die Personalabrechnung oder Zeitwirtschaft verwendet wird. Für den Benutzer sollte ein komplexes Passwort verwendet werden.

Wir erteilen diese Bescheinigung auf Grundlage des mit der SP_Data GmbH & Co. KG geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Bescheinigung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.

Diese Softwarebescheinigung berechtigt nicht automatisch zur Vernichtung von Originalbelegen. Hierfür ist eine Bestätigung der Revisionssicherheit in der jeweiligen Kundenumgebung notwendig. Die Revisionssicherheit umfasst eine Beschreibung der Abläufe (Verfahrensdokumentation), Prozesskontrollen zur Sicherstellung der Vollständigkeit und Richtigkeit der archivierten Belege sowie eine technische Sicherstellung der Verfügbarkeit während der gesamten gesetzlichen Aufbewahrungsfrist.

Nürnberg, den 7. Juni 2019

Rödl & Partner GmbH
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

gez. Schwabe
Wirtschaftsprüfer

gez. Schwestka
CISA
IT-Auditor[IDW]

5. ANLAGEN ZUM BERICHT

5.1 Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2017

DokID:

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im Nachstehenden zusammenfassend „Wirtschaftsprüfer“ genannt) und ihren Auftraggebern über Prüfungen, Steuerberatung, Beratungen in wirtschaftlichen Angelegenheiten und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Dritte können nur dann Ansprüche aus dem Vertrag zwischen Wirtschaftsprüfer und Auftraggeber herleiten, wenn dies ausdrücklich vereinbart ist oder sich aus zwingenden gesetzlichen Regelungen ergibt. Im Hinblick auf solche Ansprüche gelten diese Auftragsbedingungen auch diesen Dritten gegenüber.

2. Umfang und Ausführung des Auftrags

(1) Gegenstand des Auftrags ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer übernimmt im Zusammenhang mit seinen Leistungen keine Aufgaben der Geschäftsführung. Der Wirtschaftsprüfer ist für die Nutzung oder Umsetzung der Ergebnisse seiner Leistungen nicht verantwortlich. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen schriftlichen Vereinbarung.

(3) Ändert sich die Sach- oder Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Wirtschaftsprüfer alle für die Ausführung des Auftrags notwendigen Unterlagen und weiteren Informationen rechtzeitig übermittelt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrags von Bedeutung sein können. Dies gilt auch für die Unterlagen und weiteren Informationen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden. Der Auftraggeber wird dem Wirtschaftsprüfer geeignete Auskunftspersonen benennen.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der weiteren Informationen sowie der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

(1) Der Auftraggeber hat alles zu unterlassen, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährdet. Dies gilt für die Dauer des Auftragsverhältnisses insbesondere für Angebote auf Anstellung oder Übernahme von Organfunktionen und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Sollte die Durchführung des Auftrags die Unabhängigkeit des Wirtschaftsprüfers, die der mit ihm verbundenen Unternehmen, seiner Netzwerkunternehmen oder solcher mit ihm assoziierten Unternehmen, auf die die Unabhängigkeitsvorschriften in gleicher Weise Anwendung finden wie auf den Wirtschaftsprüfer, in anderen Auftragsverhältnissen beeinträchtigen, ist der Wirtschaftsprüfer zur außerordentlichen Kündigung des Auftrags berechtigt.

5. Berichterstattung und mündliche Auskünfte

Soweit der Wirtschaftsprüfer Ergebnisse im Rahmen der Bearbeitung des Auftrags schriftlich darzustellen hat, ist alleine diese schriftliche Darstellung maßgebend. Entwürfe schriftlicher Darstellungen sind unverbindlich. Sofern nicht anders vereinbart, sind mündliche Erklärungen und Auskünfte des Wirtschaftsprüfers nur dann verbindlich, wenn sie schriftlich bestätigt werden. Erklärungen und Auskünfte des Wirtschaftsprüfers außerhalb des erteilten Auftrags sind stets unverbindlich.

6. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Arbeitsergebnisse oder Auszüge von Arbeitsergebnissen – sei es im Entwurf oder in der Endfassung) oder die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, es sei denn, der Auftraggeber ist zur Weitergabe oder Information aufgrund eines Gesetzes oder einer behördlichen Anordnung verpflichtet.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers und die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber zu Werbezwecken durch den Auftraggeber sind unzulässig.

7. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen, Unterlassen bzw. unberechtigter Verweigerung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung kann er die Vergütung mindern oder vom Vertrag zurücktreten; ist der Auftrag nicht von einem Verbraucher erteilt worden, so kann der Auftraggeber wegen eines Mangels nur dann vom Vertrag zurücktreten, wenn die erbrachte Leistung wegen Fehlschlagens, Unterlassung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muss vom Auftraggeber unverzüglich in Textform geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z.B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse infrage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

8. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze (§ 323 Abs. 1 HGB, § 43 WPO, § 203 StGB) verpflichtet, über Tatsachen und Umstände, die ihm bei seiner Berufstätigkeit anvertraut oder bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer wird bei der Verarbeitung von personenbezogenen Daten die nationalen und europarechtlichen Regelungen zum Datenschutz beachten.

9. Haftung

(1) Für gesetzlich vorgeschriebene Leistungen des Wirtschaftsprüfers, insbesondere Prüfungen, gelten die jeweils anzuwendenden gesetzlichen Haftungsbeschränkungen, insbesondere die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Sofern weder eine gesetzliche Haftungsbeschränkung Anwendung findet noch eine einzelvertragliche Haftungsbeschränkung besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, sowie von Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen, bei einem fahrlässig verursachten einzelnen Schadensfall gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt.

(3) Einreden und Einwendungen aus dem Vertragsverhältnis mit dem Auftraggeber stehen dem Wirtschaftsprüfer auch gegenüber Dritten zu.

(4) Leiten mehrere Anspruchsteller aus dem mit dem Wirtschaftsprüfer bestehenden Vertragsverhältnis Ansprüche aus einer fahrlässigen Pflichtverletzung des Wirtschaftsprüfers her, gilt der in Abs. 2 genannte Höchstbetrag für die betreffenden Ansprüche aller Anspruchsteller insgesamt.

50261
09/2016

(5) Ein einzelner Schadensfall im Sinne von Abs. 2 ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(6) Ein Schadensersatzanspruch erlischt, wenn nicht innerhalb von sechs Monaten nach der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde. Dies gilt nicht für Schadensersatzansprüche, die auf vorsätzliches Verhalten zurückzuführen sind, sowie bei einer schuldhaften Verletzung von Leben, Körper oder Gesundheit sowie bei Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen. Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt.

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Ändert der Auftraggeber nachträglich den durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschluss oder Lagebericht, darf er diesen Bestätigungsvermerk nicht weiterverwenden.

Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfasst nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, dass der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Fall hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, dass dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfasst die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 Buchst. d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Sofern der Wirtschaftsprüfer auch Steuerberater ist und die Steuerberatervergütungsverordnung für die Bemessung der Vergütung anzuwenden ist, kann eine höhere oder niedrigere als die gesetzliche Vergütung in Textform vereinbart werden.

(6) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrags. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z.B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen,

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlungen, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen und

d) die Unterstützung bei der Erfüllung von Anzeige- und Dokumentationspflichten.

(7) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzugs wird nicht übernommen.

12. Elektronische Kommunikation

Die Kommunikation zwischen dem Wirtschaftsprüfer und dem Auftraggeber kann auch per E-Mail erfolgen. Soweit der Auftraggeber eine Kommunikation per E-Mail nicht wünscht oder besondere Sicherheitsanforderungen stellt, wie etwa die Verschlüsselung von E-Mails, wird der Auftraggeber den Wirtschaftsprüfer entsprechend in Textform informieren.

13. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Ist der Auftraggeber kein Verbraucher, so ist eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

14. Streitschlichtungen

Der Wirtschaftsprüfer ist nicht bereit, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle im Sinne des § 2 des Verbraucherstreitbeilegungsgesetzes teilzunehmen.

15. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.