Bericht

über die Prüfung der

Ordnungsmäßigkeit und Sicherheit

der Anwendung „SecuTix 360°“

SecuTix Deutschland GmbH

15. Dezember 2021

FALK IT Audit & Consulting GmbH
Wirtschaftsprüfungsgesellschaft
Im Breitspiel 21
69126 Heidelberg

PRAXITY™
Empowering Business Globally

www.falk-co.de

Inhaltsverzeichnis

1. Auftrag, Auftragsdurchführung und Gegenstand der Prüfung

1.1 Auftrag

Im Auftrag der

SecuTix Deutschland GmbH

München

(kurz: SecuTix oder Gesellschaft)

haben wir die Anwendungssoftware gemäß dem IDW-Prüfungsstandard „Prüfung von Softwareprodukten (IDW PS 880)“

SecuTix

in der Version Bishorn V3.18

geprüft.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung berichten wir im Folgenden. Diesen Bericht haben wir unter Berücksichtigung der „Grundsätze ordnungsmäßiger Berichterstattung bei Abschlussprüfungen“, niedergelegt im IDW-Prüfungsstandard 450 (IDW PS 450), erstellt.

1.2 Gegenstand der Prüfung

„SecuTix 360°“ ist eine eigenentwickelte, Cloud-basierte SaaS-Plattform speziell für Veranstaltungsanbieter, die organisatorische und operative Prozesse eines typischen Veranstaltungsanbieters digital abbildet und die Angebote des Veranstaltungsanbieters den Endkunden online zum Kauf verfügbar macht (Webshop/Online-Kanal), sofern dies vom Betreiber der Veranstaltung erwünscht ist. Ebenso sind „Vor-Ort-Buchungen“ (sog. Box Office/Offline-Kanal) über die SecuTix durch das Personal selbst möglich. SecuTix kann mit anderen Vertriebsplattformen, Ticketing-Lösungen und digitalen Anwendungen (Buchhaltungssysteme, Zutrittskontrollsysteme) integriert werden. Die Module Finanzbuchhaltung und Kassenbuchführung sind Bestandteile dieser Plattform und sind Prüfungsgegenstand unseres Auftrags.

Gegenstand unserer Prüfung war die Beurteilung des Softwareprodukts mit den für die Finanzbuchhaltung und Kassenbuchführung implementierten Funktionen im Hinblick auf die Einhaltung der Anforderungen der Grundsätze ordnungsmäßiger Buchführung (GoB) einschließlich der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) sowie der Kassensicherungsverordnung (KassenSichV) wie sie sich aus den handels- und steuerrechtlichen Vorschriften ableiten. Bei der Prüfung standen die Erfordernisse hinsichtlich Vollständigkeit, Richtigkeit, Zeitgerechtheit, Ordnung, Nachvollziehbarkeit und Unveränderbarkeit im Vordergrund.

Die Softwareprüfung haben wir in einer Testumgebung durchgeführt, die uns seitens SecuTix zur Verfügung gestellt wurde. Der Einsatz der Anwendung SecuTix beim Anwender bzw. in einer konkreten Ablauforganisation, war nicht unser Prüfungsgegenstand.

Nicht zum Gegenstand der Prüfung gehören die folgenden Elemente:

- die Prüfung der Datenextraktion und maschineller Auswertbarkeit („Z1-Zugriff“ und „Z3-Zugriff“),
- IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)“,
- die Funktionsfähigkeit der hardware- und softwaretechnischen Grundlagen der Softwareapplikation (hierunter werden bspw. Computer bzw. Notebooks, das Betriebssystem oder andere von Dritten gelieferte systemnahe Bestandteile der Software subsumiert),
- die Benutzerfreundlichkeit und Wirtschaftlichkeit des Produkts, die Sicherheit des Einsatzes von Entwicklungswerkzeugen, anwendungsunabhängige Anforderungen, die Ordnungsmäßigkeit des laufenden Betriebs der Software beim Anwender sowie
- die Beurteilung der technischen Funktionsfähigkeit in einer zur Testumgebung abweichender Systemumgebung.

1.3 Verantwortlichkeiten

Verantwortung der SecuTix Deutschland GmbH

Die gesetzlichen Vertreter der Gesellschaft sind für die Ordnungsmäßigkeit und Sicherheit der Anwendung SecuTix sowie für die Planung, Durchführung und Überwachung der Softwareentwicklung verantwortlich. Diese Verantwortung wird durch unsere Prüfung nicht berührt.

Verantwortung der FALK IT Audit & Consulting GmbH

Unsere Prüfung erstreckt sich nicht auf Folgeversionen. Jede Übertragung unseres Prüfungsergebnisses auf eine zukünftige Version birgt die Gefahr in sich, dass aufgrund durchgeführter Softwareänderungen oder Änderungen gesetzlicher bzw. regulatorischer Vorgaben funktionale Anforderungen an die Software nicht mehr erfüllt werden.

Verantwortung der Anwender

Die sachgerechte Anwendung und der ordnungsmäßige Betrieb von SecuTix beinhalten insbesondere die Umsetzung der folgenden Maßnahmen bei den Anwendern:

- In Ergänzung zur Verfahrensdokumentation von SecuTix sind die Anwender verpflichtet, den Einsatz von SecuTix in ihrem Verantwortungsbereich sachgerecht zu dokumentieren. Dies beinhaltet eine Beschreibung des tatsächlichen Einsatzes von SecuTix beim Anwender sowie der kundenindividuellen Umsetzung des Berechtigungsverfahrens.
- Die Anwender sind für eine sachgerechte Datensicherung der in SecuTix erfassten und verarbeiteten Daten verantwortlich. Darüber hinaus müssen die Anwender eine vertragliche Vereinbarung über die Speicherung und im Falle von Datenverlusten über eventuelle Wiederherstellungsverfahren treffen.

- Durch technische und organisatorische Maßnahmen ist seitens der Anwender sicherzustellen, dass die zu verarbeitenden Daten vollständig nach SecuTix übertragen werden.
- Der Anwender muss sachgerechte Maßnahmen im Bereich Zugriffsschutz ergreifen, dass seine für das System genutzte Anmeldekennung und das Anmeldepasswort ausschließlich der dafür befugten Mitarbeiter bekannt sind.
- Durch organisatorische Maßnahmen ist sicherzustellen, dass jeder Benutzer zur Durchführung von Transaktionen ausschließlich seine eigene Benutzerkennung verwendet.
- Der Anwender hat dafür Sorge zu tragen, dass Geschäftsvorfälle zeitnah erfasst und verbucht werden.
- Die Sichtung der Protokolle auf Erfassung umsatzrelevanter Vorgänge liegt in der Verantwortung des Anwenders.

1.4 Prüfungskriterien

Ziel der Softwareprüfung ist es, mit hinreichender Sicherheit zu beurteilen, ob die Anwendung SecuTix bei sachgerechter Anwendung ermöglicht, den Kriterien zu entsprechen, die als Maßstab für die Beurteilung der funktionalen Anforderungen heranzuziehen sind.

Zur Beurteilung der Ordnungsmäßigkeit und Sicherheit rechnungslegungsrelevanter Programmfunktionen wurden folgende Kriterien (Standards) herangezogen:

- IDW-Prüfungsstandard „Die Prüfung von Softwareprodukten“ (IDW PS 880, Stand 11. März 2010),
- IDW-Prüfungsstandard „Abschlussprüfung bei Einsatz der Informationstechnologie“ (IDW PS 330, Stand 24. September 2002),
- IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1, Stand 24. September 2002),
- IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce“ (IDW RS FAIT 2, Stand 29. September 2003),
- Gesetzliche Vorschriften des Handels- und Steuerrechts (§§ 238 ff. HGB, §§ 140 ff. AO),
- das Schreiben des Bundesministeriums der Finanzen über die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) vom 28. November 2019,
- Kassensicherungsverordnung (KassenSichV) vom 26. September 2017 sowie
- die Verordnung zur Änderung der Kassensicherungsverordnung (KassenSichV) vom 30. Juli 2021.

Spezielle regulatorische, aufsichtsrechtliche oder aufgabenbezogene Anforderungen an die Gestaltung rechnungslegungsrelevanter Verarbeitungsfunktionen wurden nicht berücksichtigt.

Die Anforderungen der Grundsätze ordnungsmäßiger Buchführung haben hierbei einen direkten Einfluss auf die Gestaltung von Softwareprodukten, indem die nachfolgenden gesetzlichen bzw. regulatorischen Vorgaben von dem Softwarehersteller umzusetzen sind:

- die allgemeinen Grundsätze gemäß §§ 238 und 239 HGB,
- die funktionalen Grundlagen eines Buchführungsverfahrens (Beleg-, Journal-, Kontenfunktion) sowie
- die Anforderungen zur Dokumentation und Archivierung.

2. Beschreibung des Prüfungsgegenstands

2.1 Version und Testumgebung

Bei der zu prüfenden Anwendung handelt es sich um **SecuTix** in der Version **Bishorn V3.18** vom 8.12.2021.

Die Anwendung SecuTix ist mit der Programmiersprache JAVA entwickelt worden und kann grundsätzlich auf allen gängigen Betriebssystemen installiert, betrieben und weiterentwickelt werden, die eine JAVA-Laufzeitumgebung unterstützen.

Im Verlauf unserer Prüfung der Anwendung SecuTix wurde uns eine Testumgebung mit Zugriff auf die SecuTix unter Echtbedingungen in der nachfolgend beschriebenen Konfiguration zur Verfügung gestellt:

Server

- Hardware: AWS DELL/HP (ELCA Cloud)
- Virtualisierungssoftware: AWS VMWare für ELCA Cloud
- Betriebssystem für Web-Application-Server: Tomcat8 (8.5.54)
- Datenbanksoftware: Oracle 19.10.

Client

Der Client ist grundsätzlich plattformunabhängig und benötigt lediglich eine Netzwerkverbindung und einen Firefox-Browser-Kit. SecuTix ist eine Cloud-basierte SaaS-Plattform, daher ist eine Verbindung zwischen SecuTix und dem physischen Computer erforderlich. Dies ist in erster Linie erforderlich, um die Kommunikation mit den an den Computer angeschlossenen Geräten sicherzustellen.

2.2 Entwicklungsumgebung

Eingesetzte Software

- Code-Review: Git-Flow-Prozess anhand der Pull-Requests
- Source-Code-Verwaltungssystem: GIT / Bitbucket v7.6
- Continuous-Integration-Software: Automatische Tests durch Fitness, Junit und Selenium
- JAVA-Laufzeitumgebung: JDK11
- Bereitstellung: JENKINS / Rundeck wird für alle Module verwendet; für E-Payment-Prozess wird Quantum Factory verwendet (= AWS CodeBuild / CodePipeline / CodeDeploy)
- Datenbanksoftware: Oracle 19.10

- Software-Entwicklungswerkzeug: Jira v8.20.1
- Software-Entwicklungsumgebung: IntelliJ v2021.3.

3. Prüfungshandlungen und Prüfungsdurchführung

3.1 Prüfungshandlungen

Die Prüfung der Anwendung SecuTix erfolgte gemäß dem IDW-Prüfungsstandard "Die Prüfung von Softwareprodukten (IDW PS 880)". Der Aufgabenstellung haben wir in unsere Prüfung der Ordnungsmäßigkeit und Sicherheit folgende Bereiche entsprechend einbezogen:

- Softwareentwicklungsverfahren,
- Angemessenheit der Programmfunktionen,
- Funktionsfähigkeit der Programmfunktionen sowie
- Dokumentation.

Die Prüfung beinhaltete folgende rechnungslegungsrelevanten Programmfunktionen, die anhand von Testfällen geprüft wurden:

- Anlegen einer Institution und Organisation
- Einrichtung eines Arbeitsplatzes
- Parametrisierung in der Anwendung
- Benutzeranlegen und Verwaltung (Operatoren)
- Rechtevergabe
- Stammdatenanlegen und Verwaltung (Endkunden)
- Konfiguration der Kataloge (Saisonen, Aktivitäten, Veranstaltungen, Produkte, Tarife, Preistabellen)
- Konfiguration der Zahlungs- und Versandarten
- Buchung von Verkäufen (Online- und Offline-Verkaufskanäle)
- Stornobuchungen von Geschäftsvorfällen
- Zahlungsabwicklung
- Belegerstellung (Rechnungen, Lieferscheine und Kassenbon-Duplikaten)
- Kassenbuchführung
- Kassenabschluss
- Buchhaltungsabschluss
- Export der Buchhaltungsdaten
- Protokollierung von Änderungen
- Berichtswesen/Auswertungen.

In Gesprächen mit den zuständigen Mitarbeitern sowie durch die Einsichtnahme in die Dokumentation wurden die DV-technischen Werkzeuge und organisatorischen Maßnahmen aufgenommen und beurteilt.

Die formellen Voraussetzungen für die Ordnungsmäßigkeit und Sicherheit der Anwendung wurden anhand der vorgelegten Dokumentationen beurteilt.

Im Rahmen unserer Prüfung untersuchten wir, inwieweit SecuTix einen fehlerfreien Ablauf der Funktionalitäten ermöglicht.

Die Untersuchung der notwendigen Verarbeitungs- bzw. Programmfunktionen bezog sich auf ausgewählte Stichproben und Testfälle, die Rückschlüsse auf den ordnungsmäßigen und sicheren Ablauf der Anwendung zulassen.

Im Rahmen der von uns durchgeführten Prüfungshandlungen wurden die Dokumentation, der Softwareentwicklungsprozess und wesentliche Programmfunktionen, die für die Einhaltung der GoB erforderlich sind, geprüft.

3.2 Prüfungsdurchführung

Unsere Prüfungshandlungen und -aussagen basieren auf eigenen Prüfungstätigkeiten und Auswertungen in der Testumgebung, und den uns seitens der Gesellschaft zur Verfügung gestellten Dokumentationen sowie den Auskünften von deren Mitarbeitern. Die Prüfung haben wir im Zeitraum vom November bis Dezember 2021 durchgeführt. Die Berichterstellung erfolgte in unseren Büroräumen in Heidelberg.

Folgende Mitarbeiter der Gesellschaft standen zum Prüfungszeitpunkt als Ansprechpartner zur Verfügung:

- Herr Norbert Stockmann (Managing Director, SecuTix DACH Region)
- Herr Lennart Bosche (Senior Manager Professional Service, SecuTix Deutschland)
- Herr Charles-Paul Friden (Product Owner, SecuTix Schweiz)
- Herr Fiorenzo Morini (Head of Development, SecuTix)
- Herr Lionel Matthey (Head of QA, SecuTix Schweiz).

Die erforderlichen Unterlagen standen uns im Verlauf der Prüfung uneingeschränkt zur Verfügung. Auskünfte und Nachweise wurden seitens der Gesellschaft in gewünschtem Umfang erteilt. Über Prüfungsfeststellungen im Einzelnen berichten wir im Kapitel 4 des Berichts.

4. Prüfungsergebnisse

4.1 Softwareentwicklungsverfahren

<u>Anforderungen</u>

Die Qualität der Softwareentwicklung ist wesentlich für die Beherrschung von Risiken und für eine sachgerechte Umsetzung der Programmfunktionen. Standardisierte und normierte Entwicklungsprozesse, die Toolunterstützung von Routineaufgaben in der Entwicklung und vollständige und aktuelle Verfahrens- und Testdokumentationen wirken fehlermindernd. Demgegenüber können unzureichende Softwareentwicklungsverfahren und der Umgang mit

veralteten oder nicht ausgereiften Technologien eine fehlererhöhende Auswirkung haben. Programmneuerungen sollten in sogenannten Release-Notes dem Kunden mitgeteilt werden.

Feststellungen

Im Rahmen unserer Prüfung nahmen wir die Einsicht in die Softwareentwicklungs- und Qualitätssicherungsverfahren der Anwendung SecuTix. Die Softwareentwicklungs- und Qualitätssicherungsverfahren sind angemessen aufgebaut, so dass sie eine ordnungsgemäße Entwicklung, Wartung, Test und Freigabe der Anwendung ermöglichen.

Bei der Entwicklung der Anwendung SecuTix wird eine „agile“ Methodik verwendet, die auf einem zyklischen Ansatz basiert ist.

Die Programmänderungen unterscheiden sich grundsätzlich wie folgt:

- **Funktionsänderungen (feature patches)** bringen neue Funktionen in das System ein
- Bei der **Fehlerbehebung (bug fixing patches)** handelt es sich ausschließlich um die Behebung der systemseitigen Fehler.

Jede Programmänderungsanfrage läuft einen geregelten Prozess durch. Dieser Prozess wird mit Hilfe eines Kanban-Boards unterstützt. Hierfür wurden Bitbucket und JIRA zusammen integriert, so dass die jeweiligen Statusänderungen von der Erstellung bis zum Abschluss automatisch in JIRA aktualisiert werden.

Jede Programmänderung bzw. „Change“ läuft in der Regel die folgenden Phasen durch:

Jeder „Change“ beginnt seinen Lebenszyklus in der Phase „Opened“. Die sog. „New Changes“ werden zur Planung und zur Aggregation von Informationen benutzt. Während dieser Phase werden u.a. Ziele und Meilensteine definiert, Anfragen gesammelt, betroffene Konfigurationselemente identifiziert, Risiken analysiert, der zeitliche und personelle Aufwand geschätzt, Dokumente hinzugefügt und ein Fälligkeitsdatum gesetzt.

In der Phase „Planned“ findet die Projektplanung statt. Sobald alle relevanten Informationen zusammengetragen wurden, wird ein Zuständige festgelegt, der „Change“ überwacht, sobald diese aktiviert ist. Schließlich werden die zur Durchführung der „Change“ erforderlichen Teammitglieder bestimmt.

In der Phase „Specified“ werden die jeweiligen Anforderungen definiert. Sobald ein „Change“ die obengenannten Phasen durchgelaufen ist, kann es mit der Entwicklung begonnen werden. Dies erfolgt in der Phase „Ready“.

In der Phase “In Arbeit” beginnt der Entwicklungsprozess. Während dieser Phase ist eine Kommunikation zwischen Teamleiter und den Kunden von SecuTix erforderlich. Nach dem Start wird die Entwicklung in Form von täglichen Notizen (Screenshots, Testanweisungen, Testdaten) dokumentiert.

Bei der Phase „To Validate“ wird der „Change“ geprüft, ob die vorab definierten Anforderungen erfüllt sind.

Phase „Fertig“ ist erreicht, sobald der „Change“ erfolgreich getestet worden ist, kann er in die Produktivumgebung übermittelt und dort integriert werden.

Phase „Delivered“ wird gesetzt, sobald die Ziele eines „Change“ erreicht, die Änderungen an dem jeweiligen „IT-Service“ in den Live- Betrieb überführt und alle ggf. erforderlichen Kommunikationsschritte durchgeführt wurden, so gilt der „Change“ als abgeschlossen bzw. ausgeliefert.

Zur Unterstützung des Entwicklungsprozesses wird die Gesamtheit des Codes täglich durch das Tool „Sonar“ analysiert. Das Tool „Sonar“ bietet die Möglichkeit, die Sicherheitslücken sowie die Leistungsprobleme automatisch zu erkennen. Die Ergebnisse bzw. Hauptkennzahlen von „Sonar“ werden vom Entwicklungsteam wöchentlich überprüft, um die Qualität und Sicherheit zu gewährleisten.

Im Rahmen von unserer Prüfung des Softwareentwicklungsprozesses haben wir stichprobenartig den Quellcode überprüft. Der Quellcode enthält an vielen Stellen die entsprechenden Anmerkungen, die die Nachvollziehbarkeit der Programmierung sicherstellen. Darüber hinaus wird jede Quellcodeänderung unter einem Vier-Augen-Prinzip in Bitbucket geprüft.

Die Anwendung SecuTix wird auf Quartalsbasis über die jeweiligen Release-Zyklen aktualisiert. Darüber hinaus wird jede Woche ein neuer Release veröffentlicht. Die entsprechenden Releases werden von SecuTix in Form von einem Online-Installationskalender festgelegt und dort dokumentiert.

Im Laufe der Prüfung des Softwareentwicklungsprozesses haben wir keine wesentlichen Beanstandungen festgestellt, die eine Auswirkung auf die Ordnungsmäßigkeit und Sicherheit der Anwendung haben.

Prüfungsergebnis

Die Anforderungen an das Softwareentwicklungsverfahren sind erfüllt.

4.2 Angemessenheit und Funktionsfähigkeit

4.2.1 Belegfunktion

Anforderungen

Die Belegfunktion ist der nachvollziehbare Nachweis über den Zusammenhang zwischen den Geschäftsvorfällen in der Wirklichkeit und deren Abbildung im Buchungssystem. Die Erfüllung der Belegfunktion hängt darüber hinaus im wesentlichen Maße von der Organisation des Belegwesens beim Benutzer ab und ist nur in Teilen durch die Applikation selbst sicherzustellen. Die nach § 238 Abs. 1 HGB geforderte Nachvollziehbarkeit der Buchführung vom Urbeleg bis zum Abschluss muss erfüllt sein. Jede Buchung ist vollständig durch einen Beleg nachzuweisen.
Im Zusammenhang mit der Ausführung von Buchungen muss die Software für den Beleg die Angabe eines Buchungsbetrags (oder Mengen- und Wertangaben, aus denen sich der zu buchende Betrag ergibt), der Kontierung, des Buchungstextes, der Belegnummer bzw. des Ordnungskriteriums für die Ablage, des Beleg- und des Buchungsdatums sicherstellen.

Feststellungen

Im Rahmen von unserer Prüfung haben wir ein Verständnis über die Generierung und Verarbeitung der Geschäftsvorfälle in der Anwendung SecuTix gewonnen. Die Erfassung der Daten wird bei Online-Verkäufen durch den Endkunden selbst und nur im Fall von Offline-Verkäufen durch die Anwender (Kunden von SecuTix) vorgenommen. Beim Verkauf eines Tickets wird ein Vorgang generiert. Der Vorgang ist das zentrale Element eines Ticketverkaufs und die Basis für die Generierung eines Auftrags in der Anwendung SecuTix. Ein Vorgang kann die Basis für mehrere Aufträge sein (z.B. der Verkauf oder die Stornierung). Im Laufe unserer Prüfung haben wir festgestellt, dass die Rechnungen nur dann erstellt werden können, wenn die Generierung der Rechnungen in der Anwendung SecuTix durch die Anwender eingeschaltet ist. Beim Einschalten dieser Funktion können die Rechnungen sowohl automatisch als auch manuell erstellt werden. Den Anwendern von SecuTix wird empfohlen, die entsprechenden technischen und organisatorischen Maßnahmen umzusetzen, um die Erfüllung der Belegfunktion sicherzustellen.

Wir haben festgestellt, dass die geforderte Nachvollziehbarkeit von der Anwendung SecuTix erfüllt wird, indem:

- die programmierten Vorschriften zur Generierung der Geschäftsvorfälle in der Online-Anwenderdokumentation beschrieben sind,
- der Nachweis der tatsächlichen Durchführung der einzelnen Geschäftsvorfälle erbracht wird und
- die Geschäftsvorfälle über entsprechende Auswertungen nachgewiesen werden können.

Die Nummernvergabe erfolgt automatisch in SecuTix. Für die Rechnungen muss in den Systemeinstellungen vorab ein Rechnungsnummernkreis definiert werden. Laut den Zuständigen von SecuTix gibt es keinen Nummernkreis für die Vorgänge und Aufträge, der in den Einstellungen vorab definiert werden könnte. Hierfür gibt es ein systeminterner „Counter“, der die Nummern ab „1“ bei der Neuanlage einer Institution vergibt und ferner hochzählt. Die Nummern der Geschäftsvorfälle sind fortlaufend und können nicht geändert werden. Genauso sind das Datum und die Uhrzeit an die Anwendung gebunden.

Darüber hinaus enthält jede Buchung folgende Elemente:

- Belegnummer
- Belegdatum und die Uhrzeit
- Name und Kunden-ID der Endkunden (im Fall von bekannten Verkäufen)
- Menge
- Einzelpreis
- Gebühren
- Betrag
- Gesamtbetrag
- Währung

- Produkt/Veranstaltung
- Datum der Veranstaltung
- Tarif
- Benutzer
- Status
- Bemerkungen.

Die Belege sind durch den Anwender weder änderbar noch löschbar und sie werden in der Art gespeichert, dass auch bei nachträglicher Änderung von z.B. Stammdaten (Kontaktdaten von Endkunden) die gespeicherten Daten unberührt bleiben.

SecuTix bietet die Möglichkeit, Daten bzw. Buchungen anhand verschiedener Methoden nach anderen Finanzbuchhaltungssystemen zu übertragen. Der Buchhaltungsexport kann manuell oder automatisch gestartet werden. Mit ihm können Datensätze aller Verkäufe in einem standardisierten Format (.csv) exportiert werden. Zum Prüfungszeitpunkt waren die folgenden Datenübertragungs-methoden in SecuTix vorhanden:

- Über E-Mail: die Buchungsdaten werden aus SecuTix exportiert und in Form einer csv.-Datei per E-Mail an Anwender gesendet; daraufhin werden die Daten manuell in ein Finanzbuchhaltungssystem hochgeladen,
- Automatische Datenübermittlung auf einen FTP oder SFTP-Server und
- Webhooks (sind https-Endpunkte, die von Drittanbieterprogrammen für SecuTix bereitgestellt werden). Die Daten aus SecuTix können dort anhand von POST-Anfragen gesendet werden. Das Datenformat ist hauptsächlich JSON.

Die zeitgerechte Buchung und Aufzeichnung betrifft in erster Linie die Buchhaltungsprogramme. Es ist vorgesehen, dass jeder Geschäftsvorfall zeitnah, d.h. also möglichst unmittelbar nach seiner Entstehung in einer Grundaufzeichnung oder in einem Grundbuch zu erfassen sind. Die Anwender sollten durch die entsprechenden technischen und organisatorischen Maßnahmen sicherstellen, dass eine zeitnahe Übergabe sowie die Vollständigkeit der in die Finanzbuchhaltung zu erfassenden Daten gewährleistet ist.

Prüfungsergebnis

Die Anwendung SecuTix erfüllt die Anforderungen an die Belegfunktion.

4.2.2 Journalfunktion

Anforderungen

Die Journalfunktion verlangt, dass alle buchungspflichtigen Geschäftsvorfälle zeitnah nach ihrer Entstehung vollständig und verständlich in zeitlicher Reihenfolge aufgezeichnet werden und in dieser Reihenfolge ausgegeben werden können (Journal). Während durch die Erfüllung der Belegfunktion die Existenz eines eindeutigen Geschäftsvorfalles nachgewiesen wird, hat die Journalfunktion den Nachweis der tatsächlichen und zeitgerechten Verarbeitung der Geschäftsvorfälle zum Ziel. Die

Software hat sicherzustellen, dass ein Ausdruck in der Reihenfolge der Buchungszeitpunkte, die jeweils erkennbar sein müssen, möglich ist. Hierzu ist auch nachzuweisen, dass die Software den Ausdruck des Buchungsstoffs oder eine Speicherung des Buchungsstoffs in Kombination mit Ausdruckbereitschaft unterstützt.

Feststellungen

Die Buchungsdaten können in chronologischer Reihenfolge ausgedruckt werden. Die gebuchten Geschäftsvorfälle werden klar strukturiert dargestellt. Die Anwendung SecuTix bietet die Möglichkeit, die gebuchten Geschäftsvorfälle anhand verschiedener Funktionalitäten darzustellen:

- Übersicht täglicher Vorgänge
- Übersicht aller Aufträge
- Übersicht aller Rechnungen
- Übersicht aller Zahlungen
- Kassenabschluss.

Prüfungsergebnis

Die Anwendung SecuTix erfüllt die Anforderung an die Journalfunktion.

4.2.3 Kontenfunktion

Anforderungen

Die Kontenfunktion legt fest, dass Geschäftsvorfälle in sachlicher Ordnung (z.B. durch Sach- und Personenkonten) geordnet dargestellt werden können. Die Darstellung der Konten kann durch Bildschirmanzeige, auf Papier sowie auf einem Bild- oder anderen Datenträger erfolgen.

Die Software hat zu gewährleisten, dass Buchungsaufzeichnungen die Kontenbezeichnung, einen Nachweis der lückenlosen Blattfolge, die Kennzeichnung der Buchungen, Summen und Salden nach Soll und Haben, das Buchungsdatum, einen Belegverweis sowie den Buchungstext oder dessen Verschlüsselung enthalten.

Feststellungen

Da es sich um eine Ticketing-Lösung handelt, ist eine reine Kontenfunktion nicht gegeben. Die Geschäftsvorfälle beschränken sich auf Ticketverkauf und die Weiterverarbeitung deren Zahlungen und der damit verbundenen Transaktionen. Die Daten aus SecuTix werden in ein Finanzbuchhaltungssystem übertragen und dort erfolgt die Zuordnung der Geschäftsvorfälle zu entsprechenden Konten.

Im Laufe unserer Prüfung konnten wir feststellen, dass

- die Geschäftsvorfälle mittels einer eindeutigen Belegnummer im Journal nachvollzogen werden können und
- direkt auf ein Konto-ID von Endkunden verbucht werden sowie

- es eine Möglichkeit gibt, ein Konto den Buchungen bzw. Geschäftsvorfallarten zuzuordnen, damit sie beim Datenexport in ein Finanzbuchhaltungssystem entsprechend verbucht werden können.

Prüfungsergebnis

Die Anwendung SecuTix erfüllt die Anforderungen an die Kontenfunktion.

4.2.4 Kassenbuchführung

Anforderungen

Allgemeine Anforderungen der Kassensicherungsverordnung (KassenSichV)

Die Kassensicherungsverordnung (KassenSichV) vom 26. September 2017 (BGBl. I S. 3515) wurde am 30. Juli 2021 geändert. Nach der geltenden KassenSichV sind die Unternehmen verpflichtet, die folgenden Anforderungen einzuhalten:

I. Technische Sicherheitseinrichtung

Das Bundesamt für Sicherheit in der Informationstechnik legt im Benehmen mit dem Bundesministerium der Finanzen in technischen Richtlinien und Schutzprofilen die technischen Anforderungen fest an (§ 5 der KassenSichV):

1. die digitale Schnittstelle, soweit diese den standardisierten Export aus dem Speichermedium und die Anbindung der zertifizierten technischen Sicherheitseinrichtung an das elektronische Aufzeichnungssystem betreffen. Die einheitliche digitale Schnittstelle ist eine Datensatzbeschreibung für den standardisierten Datenexport aus dem Speichermedium, der Anbindung an das elektronische Aufzeichnungssystem und dem elektronischen Aufbewahrungssystem zur Übergabe an den mit der Kassen-Nachschau oder Außenprüfung betrauten Amtsträger der Finanzbehörde. Sie stellt eine einheitliche Strukturierung und Bezeichnung der aufzuzeichnenden Daten in Datenschema und Datenfelderbeschreibung für die Protokollierung und die Speicherung sicher. Dies gilt unabhängig vom Programm des Herstellers. Die einheitliche digitale Schnittstelle für den standardisierten Export aus dem Speichermedium und die einheitliche digitale Schnittstelle für den standardisierten Export aus dem elektronischen Aufzeichnungssystem können getrennt voneinander erstellt und veröffentlicht werden.
2. das Sicherheitsmodul und
3. das Speichermedium. Die Speicherung der laufenden Geschäftsvorfälle oder anderen Vorgänge muss vollständig, unverändert und manipulationssicher auf einem nichtflüchtigen Speichermedium erfolgen. Die gespeicherten Geschäftsvorfälle müssen als Transaktionen so verkettet werden, dass Lücken in den Aufzeichnungen erkennbar sind. Werden die gespeicherten digitalen Grundaufzeichnungen ganz oder teilweise von einem elektronischen Aufzeichnungssystem in ein externes elektronisches Aufbewahrungssystem übertragen, so muss sichergestellt werden,

dass die Verkettung aller Transaktionen nach § 3 Absatz 2 der KassenSichV und die Anforderungen an die einheitliche digitale Schnittstelle nach § 4 der KassenSichV erhalten bleiben. Eine Verdichtung von Grundaufzeichnungen in einem elektronischen Aufbewahrungssystem ist für die Dauer der Aufbewahrung nach § 147 Absatz 3 der Abgabenordnung unzulässig, wenn dadurch deren Lesbarkeit nicht mehr gewährleistet ist.

II. Belegausgabepflicht
III. Anmeldung beim Finanzamt
IV. Protokollierung von digitalen Grundaufzeichnungen (s.u.)
V. Anforderungen an den Beleg (s.u.).

Anforderungen an die Protokollierung von digitalen Grundaufzeichnungen (§ 2 der KassenSichV)
Für jede Aufzeichnung eines Geschäftsvorfalls oder anderen Vorgangs im Sinne des § 146a Absatz 1 Satz 1 der Abgabenordnung muss von einem elektronischen Aufzeichnungssystem unmittelbar eine neue Transaktion gestartet werden. Die Transaktionsnummer muss so zu beschaffen sein, dass Lücken in Transaktionsaufzeichnungen erkennbar sind. Die Transaktion hat zu enthalten:

- den Zeitpunkt des Vorgangbeginns,
- eine eindeutige und fortlaufende Transaktionsnummer,
- die Art des Vorgangs,
- die Daten des Vorgangs,
- die Zahlungsarten,
- den Zeitpunkt der Vorgangsbeendigung oder des Vorgangsabbruchs,
- einen Prüfwert sowie
- die Seriennummer des elektronischen Aufzeichnungssystems und die Seriennummer des Sicherheitsmoduls.

Anforderungen an den Beleg (§ 6 der KassenSichV)
Ein Beleg muss mindestens enthalten:

- den vollständigen Namen und die vollständige Anschrift des leistenden Unternehmers,
- das Datum der Belegausstellung und den Zeitpunkt des Vorgangbeginns im Sinne des § 2 Satz 2 Nummer 1 sowie den Zeitpunkt der Vorgangsbeendigung im Sinne des § 2 Satz 2 Nummer 6,
- die Menge und die Art der gelieferten Gegenstände oder den Umfang und die Art der sonstigen Leistung,
- die Transaktionsnummer im Sinne des § 2 Satz 2 Nummer 2,
- das Entgelt und den darauf entfallenden Steuerbetrag für die Lieferung oder sonstige Leistung in einer Summe sowie den anzuwendenden Steuersatz oder im Fall einer Steuerbefreiung einen Hinweis darauf, dass für die Lieferung oder sonstige Leistung eine Steuerbefreiung gilt,

- die Seriennummer des elektronischen Aufzeichnungssystems sowie die Seriennummer des Sicherheitsmoduls und
- den Prüfwert im Sinne des § 2 Satz 2 Nummer 7 und den fortlaufenden Signaturzähler, der vom Sicherheitsmodul festgelegt wird.

Die Angaben müssen für jedermann ohne maschinelle Unterstützung lesbar oder aus einem QR-Code auslesbar sein. Der QR-Code hat der digitalen Schnittstelle der Finanzverwaltung (DSFinV), die für die jeweils zugehörige Art des Aufzeichnungssystems vorgeschrieben ist, zu entsprechen. Ein Beleg kann in Papierform oder mit Zustimmung des Belegempfängers elektronisch in einem standardisierten Datenformat ausgegeben werden.

Feststellungen

Im Rahmen von unserer Prüfung haben wir ein Verständnis über die Prozesse im Bereich Kassenbuchführung gewonnen, die durch die Anwendung SecuTix unterstützt werden. Die Anwender bzw. Kunden von SecuTix melden ihre Kassen anhand eines Tickets direkt an SecuTix. Hierfür werden ausschließlich die Offline-Verkaufskanäle gemeldet, an denen die Bargeldtransaktionen erfolgen. SecuTix erwirbt nach den Tickets von den Anwendern bei ihrem Geschäftspartner EFSTA ein Kassensystem mit einer TSE-Anbindung und rechnet die jeweiligen Gebühren an die Kunden ab. EFSTA bietet den Kunden bzw. den Anwendern von SecuTix die Fiskallösungen für Kassensysteme und deren weitere Implementierung und Wartung. Größtenteils ist eine Cloud-basierte technische Sicherheitseinrichtung (TSE) vom Hersteller „fiskaly“ bei den Kunden von SecuTix eingerichtet. Die „fiskaly sign Cloud-TSE“ wurde im Mai 2021 nach technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik zertifiziert. Die Konformität der „fiskaly sign Cloud-TSE“, Version 1.2.0-1.0.5 zur „Technischen Richtlinie BSI TR-03153“ wurde von einer gemäß DIN ISO/IEC 17025 anerkannten Prüfstelle überprüft und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt.

Laut den Anforderungen von KassenSichV muss jede Registrierkasse mit ihrer Seriennummer beim Finanzamt angemeldet werden. Hierfür obliegt es dem Anwender, angemessene organisatorische Maßnahmen zu treffen.

Zwecks des Datenaustauschs zwischen EFSTA und SecuTix wird von den Anwendern von SecuTix eine Schnittstelle (Externer Verwalter RKSV) eingestellt. Der Datenaustausch erfolgt wie folgt:

- Die Transaktionsdaten werden von Anwendung SecuTix zu einer EFR (EFSTA Fiscal Register) geschickt (Auftrag, Betrag, MwSt, Zahlungsort usw.)
- Die EFR bearbeitet die Daten und sendet sie an SecuTix zurück, um das weitere Ausdrucken der Daten auf einen Kassenbon zu ermöglichen.

Im Laufe unserer Prüfung haben wir eine Einsicht in die technischen Dokumentationen von EFSTA genommen. Laut den technischen Dokumentationen von EFSTA bietet EFSTA zusätzlich eine Archivierungsfunktion in der EFSTA-Cloud, wobei die Transaktionen für die Dauer der gesetzlichen Aufbewahrungsfrist archiviert werden können. Darüber hinaus bietet die EFSTA nach ihren technischen Dokumentationen eine Exportfunktion gemäß den Anforderungen von DSFinV-K

(Zusammenstellung der Beschlüsse und Bundeskonventionen zu den Standardtabellen im Bereich der Kassenbuchhaltung - Digitale Schnittstelle der Finanzverwaltung für Kassensysteme). Außerdem beschreibt EFSTA in ihren technischen Dokumentationen einen Backup-Prozess, in dem die sog. internen Signaturen ('sysLog') in jedem TSE-Export enthalten sein sollten, um die Lückenlosigkeit der Aufzeichnungen nachzuweisen. Die EFR führt daher regelmäßig einen TSE-Backup durch und zeichnet diese Signaturen im Journal unter dem „Record-Type“ "_":"audit" auf. Die Funktionsfähigkeit und Wirksamkeit der Archivierungs- und Exportfunktionen in EFSTA waren nicht unser Prüfungsgegenstand. Die Dokumentation der entsprechenden Archivierungs- und Exportfunktionen ist bei EFSTA einsehbar.

Im Rahmen von unserer Prüfung haben wir stichprobenweise die Belegausgabefunktion geprüft, ob die Kassenbelege den Anforderungen der KassenSichV entsprechen (§ 6 Anforderungen an den Beleg). Ein Teil der Transaktionsdaten ist beim Kassenbon ohne maschinelle Unterstützung lesbar, für den Rest von Transaktionsdaten ist ein QR-Code auf dem Kassenbon aufgesetzt. Es wurde festgestellt, dass ein Beleg bzw. Kassenbon keine Seriennummer der Kasse und der technischen Sicherheitseinrichtung enthält. Es konnten jedoch die Informationen zu einem Client-ID bzw. einem Kassen-ID aus dem im Beleg enthaltenen QR-Code mit einer maschinellen Unterstützung ausgelesen werden. Die TSE-Seriennummer konnte ferner anhand der Daten aus dem QR-Code mit einem aus den Prüfungshandlungen vorab bekannten Client-ID/Kassen-ID abgestimmt werden. Es wird empfohlen, die Seriennummer des elektronischen Aufzeichnungssystems (Kasse) sowie des Sicherheitsmoduls (TSE) auf den Kassenbons bzw. den Kassenbelegen aufzusetzen, um die Anforderungen der KassenSichV einzuhalten.

Außerdem haben wir im Laufe unserer Prüfung die Kassenbelege geprüft, ob sie den Anforderungen des § 2 der KassenSichV entsprechen. Ein Kassenbeleg enthält eine Referenznummer, die aus einer Kombination von Vorgangs- und Auftragsnummern besteht (Vorgangsnummer/Auftragsnummer). Aus dem im Beleg enthaltenen QR-Code kann die Transaktionsnummer der TSE ausgelesen werden. Die Nummern sind nicht identisch und können nur anhand eines Datenexports abgestimmt werden. Um ferner eine Kassennachschau bzw. eine Prüfung der Kassendaten (Belegverifikation, Prüfung der Integrität und Authentizität der Aufzeichnungen) bei den Anwendern zu unterstützen, wird empfohlen, der Aufbau eines Kassenbelegs und die Logik der Nummernvergabe in der SecuTix-Anwenderdokumentation zu beschreiben sowie einen Verweis auf die technischen Dokumentationen von EFSTA zu geben.

Darüber hinaus wurde festgestellt, dass das Ausdrucken eines Kassenbons nur dann erfolgen kann, wenn das von den Anwendern in den Einstellungen entsprechend eingestellt wurde. Es obliegt grundsätzlich dem Anwender, durch Nutzung der systemseitigen Funktionen und organisatorischer Abläufe, das Ausdrucken der Kassenbons zu gewährleisten, um die Belegausgabepflicht nach KassenSichV einzuhalten.

Prüfungsergebnis

Die Anforderungen an die Kassenbuchführung in der Anwendung SecuTix sind teilweise erfüllt. In Bezug auf die einzelnen Empfehlungen wird auf die oben beschriebenen Feststellungen verwiesen.

4.2.5 Protokollierungsfunktion

Anforderungen

Nach dem Buchungszeitpunkt darf entsprechend dem Grundsatz der Unveränderlichkeit eine Eintragung oder Aufzeichnung nicht so verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Daher sind spätere Eintragungen oder Aufzeichnungen ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, in einer für einen sachverständigen Dritten in angemessener Zeit nachvollziehbaren Form erkennbar bleiben.

Bei programmgenerierten bzw. programmgesteuerten Buchungen (automatisierte Belege bzw. Dauerbelege) sind Änderungen an den der Buchung zu Grunde liegenden Generierungs- und Steuerungsdaten aufzuzeichnen. Dies betrifft insbesondere die Protokollierung von Änderungen in rechnungslegungsrelevanten Einstellungen, die Parametrisierung der Software und die Aufzeichnung von Änderungen an Stammdaten.

Die Sicherung der Journale über die gesetzlich vorgeschriebene Aufbewahrungsfrist kann durch eine Protokollierung auf Papier oder auf maschinell lesbaren Datenträgern erfüllt werden. Sofern das Journal in ausgedruckter Form aufbewahrt wird, muss die Vollständigkeit der Druckliste z.B. über fortlaufende Seitennummern bzw. Summenvorträge nachweisbar sein. Bei der Aufbewahrung auf Datenträgern ist zu beachten, dass das zu Grunde liegende Verfahren die Lesbarkeit über den gesamten Aufbewahrungszeitraum gewährleisten muss.

Feststellungen

Die Anwendung SecuTix besitzt eine umfangreiche Protokollierungsfunktion. Die Protokollierungsfunktion ist in der Anwendung SecuTix hartkodiert und immer aktiv, deshalb gibt es keine Möglichkeit für die Anwender, die Protokolldaten weder zu ändern noch zu löschen.

Die Protokollierungsfunktion der Anwendung SecuTix unterscheidet sich zwischen zwei Protokollierungsarten (Application Logs):

1. Das sog. „Audit log“ protokolliert die in der Anwendung vorgenommenen Datenänderungen. Das betrifft auch die Stammdatenänderungen (Kontaktdaten von Endkunden), Änderungen der rechnungslegungsrelevanten Einstellungen (Zahlungsarten, Organisationseinstellungen, Preistabellen usw.) sowie die Änderungen der Benutzerberechtigungen. Laut den Zuständigen von SecuTix sollen hierfür die folgenden Voraussetzungen getroffen werden:
    - die betreffenden Daten wurden systemseitig bereits validiert und
    - die Daten gehören zu einer nicht versionierten Kategorie. Hierzu haben wir im Rahmen von unserer Prüfungshandlungen stichprobenartig die Protokollierung von Änderungen in rechnungslegungsrelevanten Einstellungen (Mehrwertsteuersätze) geprüft. In Gesprächen mit den Zuständigen wurde festgestellt, dass Mehrwertsteuersätze nicht versioniert werden. Deshalb werden die Änderungen der

Mehrwertsteuersätze nicht in einem „Audit log“ protokolliert, sondern direkt in einer relevanten Tabelle gezeigt.

2. In der Anwendung SecuTix können alle durch die Anwender vorgenommenen Aktivitäten protokolliert werden (list of operator actions). Dies umfasst unter anderem die folgenden Aktivitäten:
    - Anmelden/Abmelden
    - Passwortänderungen
    - Auftragserstellung
    - Kasseneröffnung/Abschluss
    - Ausdrucken der Tickets sowie der Belege.

Das Änderungsprotokoll kann ausgewertet werden. Es zeigt eine chronologische Übersicht der vorgenommenen Änderungen mit den Angaben zum Datum, Organisation, Benutzer, Modul, Funktion, Entität, Änderungstyp, Identifikation sowie den alten Werten.

Die Protokolldaten werden in der Anwendung SecuTix für ein Jahr gespeichert. Daraufhin werden sie automatisch überschrieben.

Prüfungsergebnis

Die Anforderungen an die Protokollierungsfunktion sind erfüllt, wenn der Anwender entsprechende Vorkehrungen in Bezug auf die die Aufbewahrung der rechnungslegungsrelevanten Protokolldaten für die Dauer der gesetzlichen Aufbewahrungsfrist trifft. Diese sind den Anwendern zu kommunizieren.

4.2.6 Zugriffsschutz

Anforderungen

Über die Software ist die Einhaltung der Funktionstrennung sowie der Schutz der Daten und Programme vor unberechtigten Zugriffen angemessen zu sichern. Die Anwendungssoftware - ggf. im Zusammenspiel mit dem Betriebssystem bzw. einem übergeordneten Sicherheitssystem - hat durch Benutzerkennungen (User-IDs) und Passworte sowie die Zuordnung von Berechtigungen individuelle Benutzerprofile zu verwalten. Die Einrichtung muss so möglich sein, dass es nur befugten Personen ermöglicht wird, auf bestimmte Funktionen und/oder Datenfelder zuzugreifen.

Feststellungen

Wir haben geprüft, ob die Anwendung SecuTix durch die Vergabe von Benutzerkennungen, Passwörtern und Zuordnungen von Berechtigungen die Einhaltung der Funktionstrennung gewährleistet.

Dabei wurden von uns die folgenden systemseitigen Funktionen überprüft:

- Protokollierung von Zugriffen und Benutzerkennungen
- Ausschluss trivialer Passwörter
- Rollenspezifische Zuordnung von Berechtigungen.

Den Benutzern in der Anwendung SecuTix können nach einem Kontext-Prinzip die folgenden Berechtigungen erteilt werden:

- Kontext Institution
- Kontext Organisation.

Darüber hinaus können den Benutzern unterschiedliche Rechte über Benutzergruppen zugewiesen werden (z.B. Kasse, Marketing und Kommunikation, Gruppenreservation, Callcenter usw.). Die Rechte lassen sich hierbei auf die Berechtigungen Lesen, Erstellen, Bearbeiten, Löschen und Ausführen begrenzen. Die Zuordnung von Berechtigungen zu den Benutzern können jederzeit durch die Administratoren von SecuTix-Kunden nachvollzogen werden.

Im Laufe der Prüfung haben wir festgestellt, dass die Passwortrichtlinien (Passwortlänge, Komplexität) in der Anwendung hartkodiert sind und nur von den Entwicklern geändert werden können.

Dabei unterscheidet SecuTix zwischen zwei Benutzerarten:

1. Back-Office-Operatoren - die Authentifizierung erfolgt über Active Directory. Die Passwortrichtlinien werden dabei direkt in der Active Directory festgelegt.
2. Webshop-Endkunden.

In der Anwendung SecuTix sind die Richtlinien an ein komplexes Passwort für die beiden Benutzerarten festgelegt.

Somit ermöglicht die Anwendung SecuTix die Einhaltung der Funktionstrennung und eine sachgerechte Vergabe von Berechtigungen. Es obliegt grundsätzlich dem Anwender, durch Nutzung der systemseitigen Funktionen und organisatorischer Abläufe, ein angemessenes internes Kontrollsystem umzusetzen.

Prüfungsergebnis

Die Anforderungen an Zugriffschutz sind erfüllt.

4.2.7 Datensicherungs- und Wiederanlaufverfahren

Anforderungen

Die Anwendung muss über geeignete Datensicherungs- und Wiederanlaufverfahren die Möglichkeit bieten, Daten und Programme periodisch zu sichern. Neben den von der Software vorgesehenen Maßnahmen (z. B. Datenspiegelung, Wiederanlaufpunkte) können ggf. auch die im technischen und organisatorischen Umfeld verfügbaren Datensicherungs- und Wiederanlaufverfahren verwendet werden.

Feststellungen

Im Laufe unserer Prüfung wurden uns die benötigten Dokumentationen zur Verfügung gestellt. Durch die Einsichtnahme in die Dokumentationen sowie die geführten Gespräche mit zuständigen Mitarbeitern haben wir ein Verständnis zur Durchführung von Datensicherungs- und Wiederanlaufverfahren in der Anwendung SecuTix gewonnen.

SecuTix hostet seine SaaS-Lösung auf öffentlichen Cloud-Diensten wie Amazon Web Services (AWS) und der Cloud-Kapazität von ELCA-Gruppe.

Alle auf AWS eingesetzten Anwendungsserver werden in mindestens zwei Verfügbarkeitszonen eingesetzt, wodurch das Risiko der Nichtverfügbarkeit von Diensten erheblich verringert wird.

Für die Komponenten, die in der ELCA-Group-Cloud gehostet werden, sind alle dedizierten physischen Komponenten von SecuTix (Server, Datenbanken, Netzwerke) redundant. Eine Fehlfunktion einer Komponente hat keinen Einfluss auf die Verfügbarkeit des Dienstes. Darüber hinaus wird die Datenwiederherstellung beim Kopieren von Daten aus der Produktionsumgebung in die Vorproduktionsumgebung getestet.

Neben der Duplizierung von Komponenten im Haupt-Hosting-Standort verfügt SecuTix auch über einen Notfall-Backup-Standort, der im Falle eines vollständigen Ausfalls des Hauptstandorts auf kritische Funktionen reagieren kann. Die Daten werden regelmäßig auf die Backup-Site übertragen, was ihre Wiederherstellung ohne Datenverlust ermöglicht.

Die Backups werden täglich an einem Remote-Standort repliziert. Die Daten werden beim Transport verschlüsselt (HTTPS und VPN). Im Fall eines Backup-Fehlers wird eine Warnung an einen zuständigen Techniker gesendet.

Laut den Zuständigen von SecuTix werden die ECLA-Cloud-Backups im Avamar-Tool durchgeführt und auf Kundenanfrage verschlüsselt. Der Zugriff auf die Backup-Ausrüstung ist sicher. Die AWS-Backups werden auf Basis eines Amazon RDS (Amazon Relational Database Services) durchgeführt und systematisch verschlüsselt. Zur Überwachung von Backups von SecuTix wird die Nagios-Anwendung in Kombination mit AWS-Cloud-Watch verwendet.

In Gesprächen mit den zuständigen Mitarbeitern von SecuTix haben wir festgestellt, dass die Tests zur Datenwiederherstellung bei ELCA-Cloud auf jährlicher Basis durchgeführt werden. Bei den AWS-Tests zur Datenwiederherstellung stützt sich SecuTix auf die AWS-eigenen Wiederanlaufverfahren.

Prüfungsergebnis

Die Anforderungen an die Datensicherungs- und Wiederanlaufverfahren sind erfüllt.

4.3 Funktionsfähigkeit der Programmfunktionen

4.3.1 Eingabekontrollen

Anforderungen

Damit nur einwandfreie Daten in die weitere Verarbeitung eingehen, sind angemessene Fehlerprüfungen bei der Dateneingabe vorzusehen.

Feststellungen

Anhand der vorgelegten Anwenderdokumentation sowie der während der Prüfung gewonnenen Erkenntnisse über wesentliche Verarbeitungsschritte wurden die untersuchungsrelevanten Eingabefelder ermittelt. Die Eingabetests wurden in Stichproben durchgeführt (Testumgebung).

Die Tests zur Prüfung der Angemessenheit der programmierten Eingabekontrollen wurden nach folgenden Kriterien erstellt:

- Vollständigkeitsprüfungen:
  Kontrolle auf zwingende Eingabe der erforderlichen Datenfelder („Pflichtfelder“).
- Formatprüfungen:
  Kontrolle, ob nur Daten mit zulässigem Format (alphabetisch, numerisch oder alphanumerisch) eingegeben werden können.
- Zulässigkeitsprüfungen:
  Kontrolle, ob eine Prüfung der einzelnen Felder auf zulässige Eingaben erfolgt.
- Kombinationsprüfungen:
  Feststellung, ob die Dateneingaben auf Verträglichkeit untereinander bzw. zu bereits erfassten oder gespeicherten Stamm-, Bewegungs- oder Tabellendaten kontrolliert werden.

Unsere Stichproben zur Prüfung der Eingabekontrollen betrafen u. a. folgende Bereiche:

- Buchungserfassungen
- Stammdaten (Kontaktdaten von Endkunden)
- Anlegen und Bearbeitung von Produkten, Tarifen und Preistabellen
- Parameter (Mehrwertsteuersätze).

Prüfungsergebnis

Die durchgeführten Tests zeigten, dass die implementierten Kontrollen und Maßnahmen innerhalb der Anwendung eine richtige und vollständige Verarbeitung der Datensätze sicherstellen. Die Anforderungen an Eingabekontrollen sind erfüllt.

4.3.2 Verarbeitungskontrollen

Anforderungen

Ziel der Prüfung ist es, eine Aussage über die ordnungsmäßige Verarbeitung der Daten, insbesondere der logischen Verknüpfungen, im Hinblick auf die Richtigkeit der Ergebnisse zu treffen. Es ist deshalb zu prüfen, ob die eingegebenen Daten richtig bearbeitet und zugeordnet ausgegeben werden.

Feststellungen

Die Beurteilung der programminternen Kontrollen erfolgte anhand der Anwenderdokumentation sowie durch die Tests. Die Tests wurden in Stichproben durchgeführt. Bei den Testfällen wurden bewusst und systematisch Fehleingaben vorgenommen, um die Verarbeitungskontrollen zu überprüfen.

Um die Richtigkeit der Programmabläufe sowie die sachlogische Richtigkeit der programmierten Verarbeitungsregeln sicherzustellen, haben wir uns den Verarbeitungsprozess - von Dateneingabe, Buchungen, Buchhaltungsabschluss/Kassenabschluss in der Anwendung und bis hin zum Datenexport - geprüft.

Im Laufe unserer Prüfung haben wir festgestellt, dass bei einem der Kunden bzw. Anwendern von SecuTix zum Prüfungszeitpunkt noch 16% als Mehrwertsteuersatz in den Geschäftsvorfällen im Jahr 2021 verwendet wurde. Den Sachverhalt haben wir an die Zuständigen von SecuTix kommuniziert. Laut den Zuständigen von SecuTix werden die Mehrwertsteuersätze von den Anwendern selbst in der Anwendung eingepflegt. Es obliegt grundsätzlich dem Anwender, durch Nutzung der systemseitigen Funktionen und organisatorischer Abläufe, sicherzustellen, dass die entsprechenden Konfigurationen ordnungsgemäß eingepflegt sind.

Prüfungsergebnis

Die Anforderungen an Verarbeitungskontrollen können durch entsprechende Konfigurationen seitens der Anwender erfüllt werden. Diese sind den Anwendern zu kommunizieren.

4.3.3 Anwenderdokumentation

Anforderungen

Voraussetzung für die Nachvollziehbarkeit des Buchführungs- bzw. Rechnungslegungsverfahrens ist eine ordnungsgemäße Verfahrensdokumentation, die die Beschreibung aller zum Verständnis der Rechnungslegung erforderlichen Verfahrensbestandteile enthalten muss. Die Beurteilung der Ordnungsmäßigkeit – insbesondere komplexer Verfahren – ist für einen sachverständigen Dritten nur dann möglich, wenn ihm neben den Eingabedaten und Verarbeitungsergebnissen auch eine aussagefähige, der Komplexität entsprechend detaillierte Dokumentation zur Verfügung steht. Der Aufbau und die Pflege der zum Verständnis der Rechnungslegung erforderlichen Dokumentation sind Voraussetzung für die Erfüllung der Grundsätze ordnungsmäßiger Buchführung.

Die Verfahrensdokumentation in einer IT-gestützten Rechnungslegung besteht aus der *Anwenderdokumentation*, der technischen *Systemdokumentation* sowie der *Betriebsdokumentation*.

Die *Anwenderdokumentation* muss alle Informationen enthalten, die für eine sachgerechte Bedienung einer IT-Anwendung erforderlich sind. Neben einer allgemeinen Beschreibung der durch die IT-Anwendung abgedeckten Aufgabenbereiche sowie einer Erläuterung der Beziehungen zwischen einzelnen Anwendungsmodulen sind Art und Bedeutung der verwendeten Eingabefelder, die programminterne Verarbeitung (insbesondere maschinelle Verarbeitungsregeln) und die Vorschriften zur Erstellung von Auswertungen anzugeben.

Feststellungen

Für die Anwendung SecuTix steht die Anwenderdokumentation elektronisch als Online-Hilfe zur Verfügung. Der Inhalt der Online-Hilfe sowie ergänzende Dokumentationen sind über das Internet abrufbar. Eine Änderungshistorie ist bei der Anwenderdokumentation gepflegt, um die Nachvollziehbarkeit der Änderungen im Dokument sicherzustellen. Im Verlauf der Prüfung wurden von uns einzelne Verbesserungsvorschläge hinsichtlich der Anwenderdokumentation geäußert. Wesentliche Feststellungen ergaben sich nicht. Es wird allerdings empfohlen, die folgenden Rechnungslegungsverfahren in die Anwenderdokumentation aufzunehmen bzw. aktualisieren:

- Kapitel 10.7 - Um ferner eine Kassennachschau bzw. eine Prüfung der Kassendaten (Belegverifikation, Prüfung der Integrität und Authentizität der Aufzeichnungen) bei den Anwendern zu unterstützen, wird empfohlen, der Aufbau eines Kassenbelegs und die Logik der Nummernvergabe in der SecuTix-Anwenderdokumentation zu beschreiben sowie einen Verweis auf die technischen Dokumentationen von EFSTA zu geben.

Prüfungsergebnis

Die Anforderungen an eine Anwenderdokumentation sind erfüllt. In Bezug auf die einzelnen Empfehlungen wird auf die oben beschriebenen Feststellungen verwiesen.

4.3.4 Technische Systemdokumentation

Anforderungen

Die technische Systemdokumentation enthält eine technische Darstellung der IT-Anwendung. Sie ist Grundlage für die Einrichtung eines sicheren und geordneten IT-Betriebs sowie für die Wartung der IT-Anwendung durch den Programmersteller. Art und Umfang der technischen Dokumentation sind abhängig von der Komplexität der IT-Anwendung. Die Dokumentationstechnik und formale Gestaltung der technischen Dokumentation liegen im Ermessen des Programmerstellers.

Die Dokumentation muss in einer Weise zur Verfügung gestellt werden, die einem sachverständigen Dritten den Nachvollzug der programminternen Verarbeitung, insbesondere der Verarbeitungsfunktionen und -regeln, in angemessener Zeit ohne Kenntnis der Programmiersprache erlaubt. Angesichts der Vielzahl von Programmiersprachen ist eine nur auf den Programm-Quellcode gestützte Dokumentation zur Sicherstellung der Nachvollziehbarkeit des Buchführungs- bzw. Rechnungslegungsverfahrens nicht ausreichend.

Feststellungen

Die technische Systemdokumentation der Anwendung SecuTix ist als Web-Dokumentation in der Entwicklungsumgebung (Confluence) eingebunden. Dort werden die jeweiligen Softwareimplementierungsphasen wie Design, Entwicklung (Entwicklung IT-Umgebungsspezifikation, Projektspezifikation, Entwicklungsstandards und Anforderungen), Test und Einsatz sowie die Nacharbeit dokumentiert. Die technische Systemdokumentation wird in regelmäßigen Abständen entsprechend aktualisiert. Die Änderungen an der technischen Systemdokumentation werden durch die sog. „Versionierungsfunktion“ von Confluence protokolliert und vom Leiter/Experten der jeweiligen SecuTix-Komponenten regelmäßig überprüft.

Prüfungsergebnis

Die Anforderungen an eine technische Systemdokumentation sind erfüllt.

4.3.5 Betriebsdokumentation

Anforderungen

Die Betriebsdokumentation dient der Dokumentation der ordnungsgemäßen Anwendung des

Verfahrens. Dies betrifft u.a.

- Datensicherungs- und Wiederanlaufverfahren,
- Verarbeitungsnachweise (Verarbeitungs- und Abstimmprotokolle),
- Art und Inhalt des Freigabeverfahrens für neue und geänderte Programme,
- Auflistung der verfügbaren Programme mit Versionsnachweisen.

Feststellungen

Eine Betriebsdokumentation sowie die Beschreibung des Entwicklungsprozesses sind ausführlich als Web-Dokumentation in der Entwicklungsumgebung (Confluence) eingebunden. Die Programmänderungsverfahren („Change Management“) sowie die Qualitätssicherungsverfahren werden auch in dieser Web-Dokumentation sachgerecht dokumentiert. Die Informationen zu den Releases werden von SecuTix in Form von einem Online-Installationskalender festgelegt und dort dokumentiert.

Die Informationen zu den Datensicherungs- und Wiederanlaufverfahren wurden uns im Laufe der Prüfung von Zuständigen aus verschiedenen internen und externen Quellen zusammengefasst und zur Verfügung gestellt:

1. SecuTix - Disaster Recovery Plan Cloud Operations
2. SecuTix – Architecture Overview (Auszug aus der Web-Dokumentation)
3. Amazon Relational Database Service User Guide
4. AWS Database Blog: Architect a Managed Disaster Recovery on Amazon RDS for SQL Server: Part 1.

Prüfungsergebnis

Die Anforderungen an eine Betriebsdokumentation sind erfüllt.

5. Zusammenfassendes Ergebnis und Wiedergabe der Bescheinigung

Im Auftrag von SecuTix Deutschland GmbH, München, haben wir die Anwendungssoftware

SecuTix
Version Bishorn V3.18

auf Ordnungsmäßigkeit und Sicherheit geprüft.

Gegenstand unserer Prüfung war die Beurteilung des Softwareprodukts mit den für die Finanzbuchhaltung und Kassenbuchführung implementierten Funktionen im Hinblick auf die Einhaltung der Anforderungen der Grundsätze ordnungsmäßiger Buchführung (GoB) einschließlich der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) sowie der Kassensicherungsverordnung (KassenSichV) wie sie sich aus den handels- und steuerrechtlichen Vorschriften ableiten. Bei der Prüfung standen die Erfordernisse hinsichtlich Vollständigkeit, Richtigkeit, Zeitgerechtheit, Ordnung, Prüfbarkeit und Unveränderbarkeit im Vordergrund.

Die gesetzlichen Vertreter der Gesellschaft sind für das Softwareprodukt sowie die Planung, Durchführung und Überwachung der Softwareentwicklung verantwortlich. Diese Verantwortung wird von unserer 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 den Grundsätzen ordnungsmäßiger Buchführung - was die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) einschließt - entsprechende Rechnungslegung ermöglicht und den auftragsgemäß zugrunde gelegten Kriterien entspricht.

Die Prüfung erfolgte auf Grundlage des IDW-Prüfungsstandards „Die Prüfung von Softwareprodukten (IDW PS 880)“.

Der Prüfung lagen folgende Prüfkriterien zu Grunde:

- Gesetzliche Vorschriften des Handels- und Steuerrechts (§§ 238 ff. HGB, SS 140 ff. AO),
- IDW-Prüfungsstandard „Die Prüfung von Softwareprodukten“ (IDW PS 880, Stand 11. März 2010),
- IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1, Stand 24. September 2002) sowie

- das Schreiben des Bundesministeriums der Finanzen über die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) vom 28. November 2019,
- Kassensicherungsverordnung (KassenSichV) vom 26. September 2017 sowie
- die Verordnung zur Änderung der Kassensicherungsverordnung (KassenSichV) vom 30. Juli 2021.

Spezielle regulatorische, aufsichtsrechtliche oder aufgabenbezogene Anforderungen an die Gestaltung rechnungslegungsrelevanter Verarbeitungsfunktionen wurden nicht berücksichtigt.

Die Anforderungen der Grundsätze ordnungsmäßiger Buchführung haben hierbei direkten Einfluss auf die Gestaltung von Softwareprodukten, indem

- die allgemeinen Grundsätze gemäß §§ 238 und 239 HGB,
- die funktionalen Grundlagen eines Buchführungsverfahrens (Beleg-, Journal-, Kontenfunktion) sowie
- die Anforderungen zur Dokumentation und Archivierung von dem Softwarehersteller umzusetzen sind.

Bei unserem Prüfungsurteil ist zu berücksichtigen, dass die Ordnungsmäßigkeit eines Systems nur am konkreten Einzelfall entschieden werden kann. Neben dem eingesetzten Buchführungssystem ist die Einbettung des Systems in die Organisation des Unternehmens und die Gestaltung der Arbeits- und Belegabläufe maßgebend (Internes Kontrollsystem).

Deshalb kann aus dem Ergebnis der Prüfung nicht auf die Ordnungsmäßigkeit und Sicherheit der mit der Anwendung SecuTix (Version Bishorn V3.18) erzielten Verarbeitungsergebnisse geschlossen werden, sondern vielmehr darauf, ob die Anwendung den Anforderungen an maschinelle Abrechnungssysteme entspricht, mit denen ordnungsgemäße Verarbeitungsergebnisse erzielt werden können.

Aufgrund der unserer Prüfung zugrunde gelegten Standards (Prüfkriterien) ergibt sich zusammengefasst folgende Stellungnahme zur Ordnungsmäßigkeit und Sicherheit der Anwendung SecuTix (Version Bishorn V3.18):

„Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet. Unsere Prüfung hat mit Ausnahme der folgenden Einschränkung zu keinen Einwendungen geführt:

- KassenSichV-Anforderungen an den Beleg:
  Im Laufe der Prüfung haben wir festgestellt, dass die Kassenbons bzw. Kassenbelege keine Informationen zur Seriennummer des elektronischen Aufzeichnungssystems (Kasse) sowie des Sicherheitsmoduls (TSE) enthalten.
- Beschreibung der Kassenbuchführung in der Anwenderdokumentation:

Im Laufe der Prüfung wurde festgestellt, dass der Aufbau eines Kassenbelegs und die Logik der Nummernvergabe in der SecuTix-Anwenderdokumentation nicht beschrieben war sowie kein Verweis auf die technischen Dokumentationen von EFSTA gegeben war.

Mit dieser Einschränkung ermöglicht das von uns geprüfte Softwareprodukt (Version Bishorn V3.18) nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung und entspricht den vorstehend aufgeführten Kriterien."

Im Einzelfall muss für unser Urteil nachweisbar sein, dass die eingesetzte Softwareversion mit der von uns geprüften Version übereinstimmt und keine individuellen Veränderungen am Programm vorgenommen wurden, die in der Dokumentation erläuterten Anwendungsvorschriften eingehalten und sachgerecht angewendet werden, die Programme in zeitlich und sachlich richtigem Zusammenhang eingesetzt werden, die im organisatorischen Umfeld des Programmsystems geltenden handels- und steuerrechtlichen Vorschriften eingehalten werden und das interne Kontrollsystem beim Anwender eine zuverlässige und sichere Anwendung der Software gewährleistet.

Wir erteilen diese Bescheinigung auf Grundlage des mit der SecuTix Deutschland GmbH, München, geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Bescheinigung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.

Wir weisen darauf hin, dass künftige Programmänderungen die Ordnungsmäßigkeit und Sicherheit der Software beeinflussen können.

Heidelberg, 15.12.2021

FALK IT Audit & Consulting GmbH
Wirtschaftsprüfungsgesellschaft

(Dr. Jonas Tritschler)
Wirtschaftsprüfer

(Togzhan Sadyk)

(Almira Kusmanova)
CISA

Anlagen

Softwarebescheinigung

Im Auftrag von SecuTix Deutschland GmbH, München, haben wir die Anwendungssoftware

SecuTix
Version Bishorn V3.18

auf Ordnungsmäßigkeit und Sicherheit geprüft.

Gegenstand unserer Prüfung war die Beurteilung des Softwareprodukts mit den für die Finanzbuchhaltung und Kassenbuchführung implementierten Funktionen im Hinblick auf die Einhaltung der Anforderungen der Grundsätze ordnungsmäßiger Buchführung (GoB) einschließlich der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) sowie der Kassensicherungsverordnung (KassenSichV) wie sie sich aus den handels- und steuerrechtlichen Vorschriften ableiten. Bei der Prüfung standen die Erfordernisse hinsichtlich Vollständigkeit, Richtigkeit, Zeitgerechtheit, Ordnung, Prüfbarkeit und Unveränderbarkeit im Vordergrund.

Die gesetzlichen Vertreter der Gesellschaft sind für das Softwareprodukt sowie die Planung, Durchführung und Überwachung der Softwareentwicklung verantwortlich. Diese Verantwortung wird von unserer 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 den Grundsätzen ordnungsmäßiger Buchführung - was die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) einschließt - entsprechende Rechnungslegung ermöglicht und den auftragsgemäß zugrunde gelegten Kriterien entspricht.

Die Prüfung erfolgte auf Grundlage des IDW-Prüfungsstandards „Die Prüfung von Softwareprodukten (IDW PS 880)“.

Der Prüfung lagen folgende Prüfkriterien zu Grunde:

- Gesetzliche Vorschriften des Handels- und Steuerrechts (§§ 238 ff. HGB, SS 140 ff. AO),
- IDW-Prüfungsstandard „Die Prüfung von Softwareprodukten“ (IDW PS 880, Stand 11. März 2010),
- IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1, Stand 24. September 2002) sowie
- das Schreiben des Bundesministeriums der Finanzen über die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) vom 28. November 2019,

- Kassensicherungsverordnung (KassenSichV) vom 26. September 2017 sowie
- die Verordnung zur Änderung der Kassensicherungsverordnung (KassenSichV) vom 30. Juli 2021.

Spezielle regulatorische, aufsichtsrechtliche oder aufgabenbezogene Anforderungen an die Gestaltung rechnungslegungsrelevanter Verarbeitungsfunktionen wurden nicht berücksichtigt.

Die Anforderungen der Grundsätze ordnungsmäßiger Buchführung haben hierbei direkten Einfluss auf die Gestaltung von Softwareprodukten, indem

- die allgemeinen Grundsätze gemäß §§ 238 und 239 HGB,
- die funktionalen Grundlagen eines Buchführungsverfahrens (Beleg-, Journal-, Kontenfunktion) sowie
- die Anforderungen zur Dokumentation und Archivierung von dem Softwarehersteller umzusetzen sind.

Bei unserem Prüfungsurteil ist zu berücksichtigen, dass die Ordnungsmäßigkeit eines Systems nur am konkreten Einzelfall entschieden werden kann. Neben dem eingesetzten Buchführungssystem ist die Einbettung des Systems in die Organisation des Unternehmens und die Gestaltung der Arbeits- und Belegabläufe maßgebend (Internes Kontrollsystem).

Deshalb kann aus dem Ergebnis der Prüfung nicht auf die Ordnungsmäßigkeit und Sicherheit der mit der Anwendung SecuTix (Version Bishorn V3.18) erzielten Verarbeitungsergebnisse geschlossen werden, sondern vielmehr darauf, ob die Anwendung den Anforderungen an maschinelle Abrechnungssysteme entspricht, mit denen ordnungsgemäße Verarbeitungsergebnisse erzielt werden können.

Aufgrund der unserer Prüfung zugrunde gelegten Standards (Prüfkriterien) ergibt sich zusammengefasst folgende Stellungnahme zur Ordnungsmäßigkeit und Sicherheit der Anwendung SecuTix (Version Bishorn V3.18):

„Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet. Unsere Prüfung hat mit Ausnahme der folgenden Einschränkung zu keinen Einwendungen geführt:

- KassenSichV-Anforderungen an den Beleg:
  Im Laufe der Prüfung haben wir festgestellt, dass die Kassenbons bzw. Kassenbelege keine Informationen zur Seriennummer des elektronischen Aufzeichnungssystems (Kasse) sowie des Sicherheitsmoduls (TSE) enthalten.
- Beschreibung der Kassenbuchführung in der Anwenderdokumentation:
  Im Laufe der Prüfung wurde festgestellt, dass der Aufbau eines Kassenbelegs und die Logik der Nummernvergabe in der SecuTix-Anwenderdokumentation nicht beschrieben war sowie kein Verweis auf die technischen Dokumentationen von EFSTA gegeben war.

Mit dieser Einschränkung ermöglicht das von uns geprüfte Softwareprodukt (Version Bishorn V3.18) nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung und entspricht den vorstehend aufgeführten Kriterien."

Im Einzelfall muss für unser Urteil nachweisbar sein, dass die eingesetzte Softwareversion mit der von uns geprüften Version übereinstimmt und keine individuellen Veränderungen am Programm vorgenommen wurden, die in der Dokumentation erläuterten Anwendungsvorschriften eingehalten und sachgerecht angewendet werden, die Programme in zeitlich und sachlich richtigem Zusammenhang eingesetzt werden, die im organisatorischen Umfeld des Programmsystems geltenden handels- und steuerrechtlichen Vorschriften eingehalten werden und das interne Kontrollsystem beim Anwender eine zuverlässige und sichere Anwendung der Software gewährleistet.

Wir erteilen diese Bescheinigung auf Grundlage des mit der SecuTix Deutschland GmbH, München, geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Bescheinigung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.

Wir weisen darauf hin, dass künftige Programmänderungen die Ordnungsmäßigkeit und Sicherheit der Software beeinflussen können.

Heidelberg, 15.12.2021

FALK IT Audit & Consulting GmbH
Wirtschaftsprüfungsgesellschaft

(Dr. Jonas Tritschler)
Wirtschaftsprüfer

(Togzhan Sadyk)

(Almira Kusmanova)
CISA

Allgemeine Auftragsbedingungen

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2017

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.

(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.