IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Payhawk Limited

London

2023

Bericht gemäß IDW PS 880

über die Softwareprüfung der rechnungslegungsrelevanten Funktionen der Ausgabenverwaltungslösung **payhawk** hinsichtlich der Einhaltung der Ordnungsmäßigkeit und fachlicher Anforderungen sowie die Erteilung einer Softwarebescheinigung

payhawk Unternehmensausgaben (Version 6)

Inhaltsverzeichnis **Seite**

Verzeichnis der Anlagen

1. Prüfungsauftrag

[1] Mit Schreiben vom **26.10.2022** wurden wir von der

Payhawk Limited,

(im Folgenden „Payhawk" oder „Gesellschaft" genannt),

beauftragt, die Ordnungsmäßigkeit und Sicherheit der Software

„payhawk Unternehmensausgaben"

in der Version 6 vom **01.02.2023** (Web-Anwendung) bzw. **3.41.0** vom 23.12.2022 (App für iOS), im Folgenden auch **„Anwendung"** genannt),

gemäß dem Prüfungsstandard „Die Prüfung von Softwareprodukten" (IDW PS 880) zu prüfen.

[2] Die Gesellschaft hat uns in einer berufsüblichen **schriftlichen Vollständigkeitserklärung** vom 01.02.2023 bestätigt, dass sie uns sämtliche Informationen, Daten und schriftlichen Unterlagen, die für die Prüfung von Bedeutung waren, zur Verfügung gestellt hat.

[3] 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 unter IDW Prüfungsstandard 450 (IDW PS 450), erstellt.

2. Verantwortung

2.1 Verantwortlichkeiten der Payhawk Ltd.

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

[5] Eine Weitergabe des schriftlichen Prüfungsberichts gemäß IDW PS 880 durch Payhawk an andere Gesellschaften ist nur zulässig, wenn die jeweilige Gesellschaft als Drittbeteiligte vor Erhalt des Berichts die rechtsverbindliche schriftliche Erklärung abgibt, sich bezüglich etwaiger eigener Ansprüche gegenüber der IT AUDIT GmbH Wirtschaftsprüfungsgesellschaft, im Folgenden „IT AUDIT", Köln, mit der Geltung der Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 einverstanden erklärt sowie damit, den Bericht und alle darin enthaltenen Informationen ebenfalls vertraulich zu behandeln und nicht weiterzugeben. Hinsichtlich der Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers gelten Nr. 1 Abs. 2 und Nr. 9 der Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017. Danach gilt dieser Umfang auch im Verhältnis zu Dritten als vereinbart. Eine Kopie der Vereinbarung mit den jeweiligen Dritten ist IT AUDIT zuzusenden.

[6] Die vollständige Softwarebescheinigung kann seitens Payhawk deren Kunden oder weiteren Interessenten zur Verfügung gestellt werden. Die Gesellschaft darf die Tatsache der Prüfung sowie die Prüfungsergebnisse werblich verwenden. Namentliche Hinweise auf IT AUDIT sind in diesem Zusammenhang zu unterlassen.

2.2 Verantwortlichkeiten der IT AUDIT

[7] Unsere Prüfung erstreckt sich nicht auf Folgeversionen. Jede Übertragung unseres Prüfungsergebnisses auf eine zukünftige Version birgt grundsätzlich die Gefahr in sich, dass aufgrund

durchgeführter Softwareänderungen oder Änderungen gesetzlicher bzw. regulatorischer Vorgaben funktionale Anforderungen an die Software nicht mehr erfüllt werden.

[8] Die Software wird Anwendern zur Umsetzung eines Zahlungsservices („SaaS-Lösung") bereitgestellt. Technische Basis ist eine Entwicklungsumgebung, die seitens Payhawk im Rahmen agiler Softwareentwicklungsprozesse permanent angepasst wird. Unsere Prüfungsergebnisse beziehen sich damit auf die Umsetzung von Kernfunktionalitäten, die unter 4.3 und 4.4 beschrieben wurden.

2.3 Verantwortlichkeiten der Anwender

[9] Die sachgerechte Anwendung und der ordnungsmäßige Betrieb der Anwendung beinhalten insbesondere die Umsetzung der folgenden Maßnahmen bei den Anwendern:

- In Ergänzung zur Verfahrensdokumentation zur Anwendung sind die Anwender verpflichtet, den Einsatz der Anwendung in ihrem Verantwortungsbereich sachgerecht zu dokumentieren. Dies beinhaltet eine Beschreibung des tatsächlichen Einsatzes der Anwendung beim Anwender sowie der kundenindividuellen Umsetzung des Berechtigungsverfahrens.
- Die Anwender sind für eine sachgerechte Datensicherung der in der Anwendung erfassten und verarbeiteten Daten verantwortlich. Darüber hinaus müssen die Anwender eine vertragliche Vereinbarung über die Speicherung und im Falle von Datenverlusten über eventuelle Wiederherstellungsverfahren mit Payhawk treffen.
- Durch technische und organisatorische Maßnahmen ist seitens der Anwender sicherzustellen, dass die zu verarbeitenden Daten vollständig in die Anwendung übertragen werden.
- Der Anwender muss sachgerechte Maßnahmen im Bereich Zugriffsschutz ergreifen, dass seine für das System genutzte Anmeldekennung und das Anmeldepasswort ausschließlich den dafür befugten Mitarbeitern 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.

3. Auftragsinhalt und Auftragsdurchführung

3.1 Prüfungskriterien

[10] Prüfungsrelevant sind ausschließlich die rechnungslegungsrelevanten Funktionen der Anwendung **payhawk Unternehmensausgaben**.

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

[12] Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung mit hinreichender Sicherheit zu beurteilen, inwieweit die Funktionen der Anwendung bei sachgerechtem Einsatz eine Einhaltung der handelsrechtlichen Ordnungsmäßigkeitskriterien, der Grundsätze ordnungsmäßiger Buchführung (GoB), der vom Institut der Wirtschaftsprüfer in Deutschland e.V.

(IDW) herausgegebenen Stellungnahme zur Rechnungslegung "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1) sowie ergänzend die "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)" vom 28. November 2019 unterstützen.

[13] Die Anforderungen der **GoB** üben hierbei einen direkten Einfluss auf die Gestaltung von Softwareprodukten aus, indem die nachfolgenden gesetzlichen bzw. regulatorischen Vorgaben durch den Softwarehersteller umzusetzen sind:

- Allgemeine Grundsätze gemäß den §§ 238 ff. HGB,
- Prüfungsstandard IDW PS 880 (Stand: 11.03.2010),
- Die vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) herausgegebene Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)“,
- Ausgewählte grundlegende funktionale Grundlagen eines Buchführungsverfahrens (insbesondere die Beleg- und Journalfunktion) sowie
- Anforderungen zur Dokumentation und Archivierung.

[14] Darüber hinaus wurden die nachfolgenden Gesetze und Verordnungen des Steuerrechts als Prüfkriterien ergänzend beachtet:

- Gesetzliche Vorschriften des Steuerrechts (§§ 140 - 148 AO) sowie
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)[1].

[15] Weitere regulatorische, aufsichtsrechtliche oder aufgabenbezogene Anforderungen an die Gestaltung rechnungslegungsrelevanter Verarbeitungsfunktionen wurden nicht berücksichtigt.

[16] Der Einsatz der Anwendung beim Anwender, d.h. in einer konkreten Ablauforganisation, war nicht Untersuchungsgegenstand unserer Prüfung. Die Testverfahren im Rahmen unserer Prüfungshandlungen fanden in einer durch Payhawk zur Verfügung gestellten Testumgebung (Demo Account) unter Echtbedingungen statt.

[17] Aussagen zu organisatorischen Regelungen werden im Rahmen unserer Prüfungshandlungen nur insoweit getroffen, dass für selektive IT-gestützte Funktionen, welche im Funktionsumfang der Anwendung nicht enthalten sind, ergänzende organisatorische Maßnahmen seitens der Anwender erforderlich sind.

3.2 Prüfungshandlungen

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

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

[1] Schreiben des Bundesministeriums der Finanzen "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)" vom 28.11.2019.

[19] Anhand der vorgelegten Dokumentationsunterlagen, des zur Verfügung stehenden Demo-Account und in ergänzenden Gesprächen mit den zuständigen Mitarbeitern der Gesellschaft wurden

- das erforderliche IT-Systemumfeld (Hardware und Anwendungssoftware) aufgenommen,
- ein Überblick über den Arbeitsablauf innerhalb der Anwendung gewonnen,
- die Abgrenzung zu vor- und nachgelagerten Teilgebieten vorgenommen und
- die untersuchungsrelevanten Teilgebiete, Dateien und Auswertungen festgestellt.

[20] Die formellen Voraussetzungen für die Ordnungsmäßigkeit und Sicherheit der Anwendung wurden anhand der vorgelegten Dokumentation beurteilt.

[21] Im Rahmen unserer Prüfung untersuchten wir, inwieweit die Anwendung einen fehlerfreien Ablauf der Funktionalitäten ermöglicht.

[22] 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.

[23] Kein Gegenstand der Prüfung waren:

- 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 ergonomische Funktionalität 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 abweichenden Systemumgebung.

3.3 Prüfungsergebnisse

[24] Unsere Prüfungshandlungen und -aussagen basieren auf eigenen Prüfungstätigkeiten und Auswertungen im Testsystem, den uns seitens der Gesellschaft zur Verfügung gestellten Dokumenten und Unterlagen sowie den Auskünften von deren Mitarbeitern.

[25] Die erforderlichen Unterlagen standen uns im Verlauf der Prüfung uneingeschränkt zur Verfügung. Auskünfte und Nachweise wurden seitens der Gesellschaft in gewünschtem Umfang erteilt.

3.4 Beschreibung des Prüfungsgegenstands

3.4.1 Grundlegende Funktionalität

[26] Bei der zu prüfenden Softwareapplikation handelt es sich um **payhawk Unternehmensausgaben** in der **Version 6** (bezogen auf die Entwicklungsumgebung) vom 01.02.2023 für die Web-Anwendung sowie 3.41.0 vom 23.12.2022 für die iOS-App.

[27] **payhawk Unternehmensausgaben** wurde als Web-Anwendung konzipiert, auf die von jedem internetfähigen Endgerät zugegriffen werden kann. Hierbei mögliche Web-Adressen sind

www.payhawk.com sowie https://portal.payhawk.com. Darüber hinaus steht im Google-Playstore bzw. im Apple App Store die App „**Payhawk**" zur Verfügung. Gegenstand unserer Prüfung war die im App Store bereitgestellte Version für iOS.

[28] Die App dient der Freigabe von Zahlungen sowie der Einsicht in ein Rechnungs-Postfach, an das Rechnungen über die E-Mail-Adressen unpaid@payhawk.me (unbezahlte Rechnungen) bzw. paid@payhawk.me (bezahlte Rechnungen) gesandt werden können. Darüber hinaus können Rechnungen auch über die Portal-Adresse hochgeladen werden.

[29] Das für den Test herangezogene Gesamtsystem umfasste damit die Funktionen der Web-Anwendung bzw. des Portals sowie die Funktionen der App für iOS.

3.4.2 Verwendete Testumgebung

[30] Zur Untersuchung der Softwareapplikation **payhawk Unternehmensausgaben** wurde uns seitens Payhawk für den Zeitraum der Prüfung eine Testumgebung mit Zugriff auf die o. g. Anwendungen im Wesentlichen unter Echtbedingungen in der nachfolgend beschriebenen Konfiguration zur Verfügung gestellt:

- Softwareversion payhawk Web-Anwendung:
  verschiedene Versionsstände der Entwicklungsumgebung bis zum (aktuellen) Versionsstand 6.27
- Softwareversion Payhawk App für iOS:
  verschiedene Versionsstände der App für iOS bis zum (aktuellen) Versionsstand 3.42.0

[31] Unser Zugriff auf die Anwendung erfolgte mit folgenden Web-Browsern:

- Microsoft Edge 108.0.1462.54 (64-Bit)
- Google Chrome 108.0.5359.125 (64-Bit)
- Apple Safari der iOS-Version 16.2 bzw. der iPadOS-Version 16.2

4. Prüfungsergebnisse

4.1 Beurteilung des Softwareentwicklungsverfahrens

Anforderung

[32] Die Qualität der Softwareentwicklung soll die Beherrschung von Risiken und gleichzeitig eine sachgerechte Umsetzung der Programmfunktionen unterstützen. Dabei müssten sich standardisierte und normierte Entwicklungsprozesse, die Toolunterstützung von Routineaufgaben in der Entwicklung und eine vollständige und aktuelle Verfahrens- und Testdokumentationen fehlermindernd auswirken. Demgegenüber könnten sich unzureichende Softwareentwicklungsverfahren und der Umgang mit veralteten oder nicht ausgereiften Technologien fehlererhöhend auswirken.

[33] Die anlässlich der Programmentwicklung verwendeten Methoden und Verfahren sollten schriftlich dokumentiert sein. Zwecks Wiederverwendung bereits entwickelter Programme und Programmbestandteile sollten Anforderungen für den Programmaufbau, die Namenskonventionen und die Dokumentationsanforderungen in einer Programmierrichtlinie zusammengefasst sein. Die Nutzung einer geeigneten Entwicklungsumgebung ist dabei nachzuweisen.

[34] Ein derartiges Verfahren sollte zumindest die nachfolgenden Maßnahmen beinhalten:

- schriftliche Anforderung für eine Fehlerbeseitigung bzw. eine Funktionserweiterung
- Test einer fehlerkorrigierten Programmfunktion bzw. einer Funktionserweiterung sowie
- Integrationstests und Gesamtfreigabe der fehlerkorrigierten bzw. neuen Version.

Prüfungshandlungen der IT AUDIT

[35] Im Prüffeld Verfahren und Methoden der Softwareentwicklung untersuchten wir, ob

- die anlässlich der Programmentwicklung der Anwendung verwendeten Methoden und Verfahren schriftlich dokumentiert sind sowie
- Anforderungen für Programmstrukturen, die Namenskonventionen und die Dokumentationsanforderungen in einer Programmierrichtlinie zusammengefasst sind.

[36] Im Rahmen unserer Prüfungshandlungen prüften wir im Prüffeld **Anforderungen an Softwareentwicklungsverfahren**, ob

- für eine Fehlerbeseitigung bzw. eine Funktionserweiterung eine schriftliche Anforderung benötigt wird,
- fehlerkorrigierte Programmfunktionen bzw. Funktionserweiterungen vor deren Freigabe getestet werden sowie
- die Gesamtfreigabe einer fehlerkorrigierten bzw. neuen Version jeweils vorliegt.

[37] Im Prüffeld Test des Softwareentwicklungsverfahrens prüften wir

- nach welchen Kriterien bzw. Arten von Tests getestet wird sowie
- die als Tester eingesetzten Personen.

[38] Im Verlauf unserer Prüfungshandlungen untersuchten wir das Prüffeld **Funktionstrennung** dahingehend, inwieweit innerhalb der Organisation eine funktionale Trennung vorliegt:

- Softwareentwicklung,
- Qualitätssicherung bzw. Testumgebung sowie
- Anwender.

[39] Im Prüffeld **Qualitätssicherung** untersuchten wir, inwieweit angemessene und wirksame Verfahren zur Minimierung der mit einer Softwareentwicklung verbundenen Risiken innerhalb der Gesellschaft implementiert sind.

Prüfungsfeststellungen

[40] Im Prüffeld Verfahren und Methoden der Softwareentwicklung konnten wir feststellen, dass

- die Entwicklung von **payhawk Unternehmensausgaben** nach agilen Methoden vorgenommen wird, in die mehrstufige Testverfahren integriert sind, sowie
- die Anforderungen für Programmstrukturen, die Namenskonventionen einschließlich der Dokumentation allgemeinen Programmierrichtlinien der eingesetzten Entwicklungswerkzeuge JavaScript und TypeScript (JavaScript Library react für das front end sowie Node.js für das Backend).

[41] Im Rahmen unserer Prüfungshandlungen sowie in Gesprächen mit der Gesellschaft stellten wir im Prüffeld **Anforderungen an Softwareentwicklungsverfahren** fest, dass

- Fehlerbeseitigungen bzw. Funktionserweiterung innerhalb eines Sprints nach dessen Regeln durchgeführt werden.

- Neue Programmversionen mit einem Demo-Datenbestand im Payhawk-Testsystem im Rahmen von Integrationstests geprüft und ggf. wöchentlich ausgerollt werden.
- Nach erfolgreichem Test einer fehlerkorrigierten bzw. einer neuen Version erfolgt deren Gesamtfreigabe durch den Product Owner.

[42] Im Prüffeld **Test des Softwareentwicklungsverfahrens** gelangten wir zu der Erkenntnis, dass

- mittels Unit-Tests einzelne Komponenten einer Anwendung in der Testumgebung des **Payhawk-**Testsystems mit der Demo-Datenbank getestet werden, wobei diese in nachfolgenden System- und Integrationstest weiterverwendet werden kann,
- die korrigierte Version in das Payhawk-Testsystem übernommen wird,
- weitere Integrationstests auf den Testsystemen vorgenommen werden sowie
- nach erfolgreichen Tests durch Payhawk das Rollout der Softwareapplikation in das Produktivsystem erfolgt. Als Testpersonen fungierten Entwickler sowie die Projektmanager.

[43] Im Verlauf unserer Prüfungshandlungen konnten wir im Prüffeld **Funktionstrennung** anhand einer Übersicht über die Organisation die funktionelle Trennung der nachfolgenden Sparten feststellen:

- Softwareentwicklung sowie
- Test und Freigabe.

[44] Im Prüffeld **Qualitätssicherung** stellten wir in Gesprächen mit der Gesellschaft fest, dass Verfahren zur Minimierung der mit einer Softwareentwicklung verbundenen Risiken innerhalb der Gesellschaft über auch funktionale Trennungen implementiert sind:

- Trennung von z. B. Zahlungen, Zahlungsdaten, Datenexport
- Einheitliche Funktionsaufrufe aus dem Portal und der App über authorisierte API Calls.

Prüfungsurteil

[45] Die Anwendung **payhawk Unternehmensausgaben** erfüllt die Anforderungen an Softwareentwicklungsverfahren.

4.2 Auslagerung rechnungslegungsrelevanter Dienstleistungen

Anforderungen

[46] Ausgelagerte Dienstleistungen, welche für die Rechnungslegung relevant sind, müssen in geeigneter Weise ausgestaltet sein, um Daten über Geschäftsvorfälle, Ereignisse oder betriebliche Aktivitäten zu speichern oder zu verarbeiten, die entweder direkt in die Rechnungslegung einfließen oder dem Rechnungslegungssystem als Grundlage für Buchungen zur Verfügung gestellt werden.

[47] Dienstleistungen im Rahmen einer Auslagerung, die zur Speicherung bzw. Verarbeitung rechnungslegungsrelevanter Daten dienen, müssen ein Bestandteil des IT-Systems sowie des IT-gestützten Rechnungslegungssystems eines Unternehmens werden.

Prüfungshandlungen der IT AUDIT

[48] Wir untersuchten im Prüffeld **Rechenzentrumsbetrieb/Cloud Computing**, in welcher Form Dienstleistungen bei der Bereitstellung der Web-Anwendung **payhawk Unternehmensausgaben** seitens der Gesellschaft an Rechenzentren ausgelagert werden.

Prüfungsfeststellungen

[49] Wir konnten im Prüffeld feststellen, dass die Web-Anwendung in Form des **„Broad Network Access"** den Kunden zur Verfügung gestellt wird, indem diese mit einem beliebigen Endgerät über Standard-Webtechnologien einen Zugriff auf die Anwendung erhalten.

[50] Die Anwender nutzen **payhawk Unternehmensausgaben** dabei in der Cloud als **"Software as a Service (SaaS)",** wobei die erforderliche Infrastruktur vom Rechenzentrumsdienstleister Amazon Web Services zur Verfügung gestellt wird.

[51] Bezüglich der Auslagerung des Betriebs der Web-Anwendung an den oben genannten Rechenzentrumsbetreiber liegt uns ein Prüfungsbericht über eine Zertifizierung der Dienstleistung „Amazon Web Services System" gemäß SOC2 für den Zeitraum vom 01.04.2022 bis 30.09.2022 vor.

[52] Das Vorliegen der o. g. Bescheinigung sowie ihre Umsetzung bei Kunden der Gesellschaft stellt keine formale Erteilungsvoraussetzung für eine Softwarebescheinigung gemäß IDW PS 880 dar. Gleichwohl erhöht es die Sicherheit für die Einhaltung von Ordnungsmäßigkeitskriterien im laufenden Betrieb für Kunden der Gesellschaft.

[53] An welchen nationalen Standorten die Bereitstellung und Datenhaltung der Web-Anwendung erfolgt, war nicht Gegenstand unserer Prüfung.

[54] Wir weisen in diesem Zusammenhang aber darauf hin, dass gemäß § 146 Abs. 2a AO vor der Entscheidung über die Speicherung rechnungslegungsrelevanter Daten im (europäischen) Ausland die Zustimmung der Finanzverwaltung einzuholen ist.

Prüfungsurteil

[55] Die Web-Anwendung erfüllt in der uns vorliegenden Konfiguration die Anforderungen an die Auslagerung rechnungslegungsrelevanter Dienstleistungen.

4.3 Angemessenheit der Programmfunktionen

[56] Die Einhaltung der handelsrechtlichen Grundsätze ordnungsmäßiger Buchführung (GoB) ist durch die Anwendung angemessen zu unterstützen. Ergänzend sind die steuerrechtlichen Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) zu beachten.

[57] Deren Einhaltung kann durch Erfüllung der nachfolgenden notwendigen und speziellen Verarbeitungsfunktionen – sofern in der Anwendung vorhanden und relevant - belegt werden:

- Belegfunktion
- Journal- und Kontenfunktion
- Protokollierungsfunktion
- Dokumentation
- Zugriffsschutz sowie
- Datensicherungs- und Wiederanlaufverfahren.

4.3.1 Belegfunktion

Anforderungen

[58] Die nach § 238 Abs. 1 HGB geforderte Nachvollziehbarkeit der Buchführung vom Urbeleg zum Abschluss und vice versa setzt voraus, dass jede Buchung und ihre Berechtigung durch einen Beleg nachgewiesen wird (Grundsatz der Belegbarkeit). Die Web-Anwendung **payhawk Unternehmensausgaben** hat die Funktion eines Nebenbuches, dessen Informationen nach Bereitstellung an ein externes System mit Hauptbuchfunktionalität (z. B. DATEV) dort jeden Geschäftsvorfall urschriftlich belegen. Die Belegfunktion stellt die Grundvoraussetzung für die Beweiskraft der Buchführung und sonstiger erforderlicher Aufzeichnungen dar.

[59] Die Existenz und die Verarbeitungsberechtigung eines Sachverhalts müssen durch die Erfüllung der Belegfunktion nachgewiesen werden. Für die Web-Anwendung bedeutet dies, dass sämtliche Transaktionen lückenlos erfasst werden können.

Prüfungshandlungen der IT AUDIT

[60] Im Prüffeld **Belegbarkeit** untersuchten wir, ob

- jede Transaktion und ihre Berechtigung durch einen Beleg nachgewiesen werden sowie
- jeder Geschäftsvorfall urschriftlich belegt werden kann.

[61] Im Rahmen unserer Prüfungshandlungen prüften wir im Prüffeld **Nachvollziehbarkeit**, ob

- die programminternen Vorschriften zur Generierung von Transaktionsdaten nachvollziehbar sind,
- ein Nachweis der tatsächlichen Durchführung der einzelnen Transaktionen (Verarbeitung) erbracht werden kann sowie
- Transaktionen über entsprechende Auswertungen nachgewiesen werden.

[62] Im Prüffeld **Einhaltung des Radierverbots** gemäß § 239 Abs. 3 HGB bzw. § 146 Abs. 5 AO prüften wir, inwieweit

- Änderungen an einmal im System erzeugten und festgeschriebenen Daten auf konventionellem Wege nicht mehr zugelassen sind sowie
- Änderungen an Belegtexten in der Software erfasst werden.

[63] Im Verlauf unserer Prüfungshandlungen untersuchten wir das Prüffeld **Erfüllung des Ordnungsprinzips** dahingehend, ob

- für jede Transaktion systemseitig eine eindeutige Belegnummer vergeben wird,
- der erfasste Betrag einen Pflichtbestandteil jedes Vorgangs darstellt sowie
- der Zeitpunkt einer Transaktion (Belegdatum) erfasst werden.

[64] Im Prüffeld **Autorisierung der Transaktion** untersuchten wir, ob

- für jeden Benutzer eine entsprechende Berechtigungsvergabe vorliegt sowie
- die Benutzerkennung bei Transaktionen gespeichert wird.

Prüfungsfeststellungen

[65] Im Prüffeld **Belegbarkeit** konnten wir feststellen, dass

- im Anschluss an das Hochladen eines Belegs, der als mögliche Unternehmensausgabe klassifiziert, geprüft, freigegeben und bezahlt werden kann, jede Veränderung

und/oder Ergänzung nach dem Hochladen protokolliert wird („Ausgabenhistorie"). Hierzu gehören z. B. der Status eines Belegs, Anpassungen der Belegnummer sowie des Belegdatums, des Lieferanten sowie Adress- u. Steuerinformationen (Steuersätze).

[66] Im Rahmen unserer Prüfungshandlungen konnten wir im Prüffeld **Nachvollziehbarkeit** feststellen, dass

- nach der Archivierung von Ausgaben, die monatlich vorgenommen werden kann, Veränderungen an den der Ausgaben zugrunde liegenden Belegen nicht mehr möglich sind,
- mittels automatischer Festschreibung von Ausgaben nach dem Export an ein System mit Hauptbuchfunktionalität (ERP-Anbindung), deren tatsächliche Verarbeitung nachvollziehbar ist, sowie
- Ausgaben über entsprechende Auswertungen (wie z. B. einen Datenexport in das pdf-Format) nachgewiesen werden können.

[67] Derzeit ist eine Anbindung u. a. der ERP-Systeme DATEV, Netsuite und Microsoft Dynamics 365 möglich.

[68] Im Prüffeld Einhaltung des Radierverbots gemäß § 239 Abs. 3 HGB bzw. § 146 Abs. 5 AO stellten wir fest, dass

- im System festgeschriebene Belegdaten (z. B. Belege nach Archivierung, Zahlungen nach Export) nicht mehr verändert werden können und
- somit nachvollziehbar sind.

[69] Im Verlauf unserer Prüfungshandlungen gelangten wir im Prüffeld **Erfüllung des Ordnungsprinzips** zu der Erkenntnis, dass

- Belege, Ausgaben und Zahlungen

nach verschiedenen Kriterien ausgewertet werden können (wie z. B. Karte, Mitarbeiter, Ausgabentitel, Lieferant etc.).

[70] Bei den Ausgaben-Kategorien kann ein sog. „Konto-Code" hinzugefügt werden. Dieser muss allerdings nicht eindeutig sein, wodurch kontobezogene Auswertungen erschwert werden.

[71] Im Prüffeld **Autorisierung des Buchenden** konnten wir durch Gespräche mit Payhawk und über eigene Prüfungshandlungen feststellen, dass

- Benutzern vordefinierte Benutzer- und Berechtigungsbereiche (Administrator, Buchhalter, Mitarbeiter) vergeben werden müssen.
- Änderungen bezüglich der Berechtigungen können nur durch den Benutzer „Administrator" vorgenommen werden.

[72] Die Vergabe von Benutzerberechtigungen liegt nach Aussagen der Gesellschaft im Verantwortungsbereich der Anwender. Prüfungshandlungen bei Anwendern nahmen wir nicht vor.

Prüfungsurteil

[73] Die Anwendung erfüllt die Anforderungen an die Belegfunktion. Ein Zwang zur Vergabe eines eindeutigen Konto-Codes sollte geprüft werden.

4.3.2 Journalfunktion

Anforderung

[74] Die Journalfunktion verlangt, dass alle festgeschriebenen Sachverhalte zeitnah nach ihrer Entstehung vollständig und verständlich **in zeitlicher Reihenfolge** aufgezeichnet werden (Journal). Während durch die Erfüllung der Belegfunktion die Existenz und Verarbeitungsberechtigung eines Sachverhaltes nachgewiesen werden muss, hat die Journalfunktion den Nachweis der tatsächlichen und zeitgerechten Verarbeitung der Geschäftsvorfälle zum Gegenstand.

Prüfungshandlungen der IT AUDIT

[75] Da die Journalfunktion durch ein nachgelagertes System mit Hauptbuchfunktionalität, an das Transaktionen aus **payhawk Unternehmensausgaben** übergeben werden, abgebildet wird, nahmen wir keine weiteren Prüfungshandlungen vor.

Prüfungsurteil

[76] Die Journalfunktion muss in einem nachgelagerten System mit Hauptbuchfunktionalität, an das Ausgabentransaktionen übertragen werden, wahrgenommen werden.

4.3.3 Kontenfunktion

Anforderung

[77] Die Kontenfunktion verlangt, dass die im Journal in zeitlicher Reihenfolge aufgezeichneten Geschäftsvorfälle auch in sachlicher Ordnung auf Konten abgebildet werden. Bei computergestützten Buchführungsverfahren werden Journal- und Kontenfunktion in der Regel gemeinsam wahrgenommen, indem bereits bei der erstmaligen Erfassung des Geschäftsvorfalls alle für die sachliche Zuordnung notwendigen Angaben erfasst werden.

Prüfungshandlungen der IT AUDIT

[78] Auch die Kontenfunktion muss in einem nachgelagerten System mit Hauptbuchfunktionalität abgebildet werden. Daher nahmen wir keine weiteren umfänglichen Prüfungshandlungen vor.

Prüfungsfeststellungen

[79] Die Anwendung **payhawk Unternehmensausgaben** erlaubt die Zuordnung von Transaktionen zu Ausgaben-Kategorien wie z. B. Werbung u. Marketing, Prüfung u. Buchführung, Beratung u. Steuern. Jede Ausgaben-Kategorie kann (optional) einen Konto-Code erhalten, wobei die mehrfache Verwendung des gleichen Konto-Codes für verschiedene Ausgaben-Kategorien möglich ist

[80] Systemseitig lässt sich einstellen, dass bei der Einreichung von Ausgaben eine Ausgaben-Kategorie zwingend mitgegeben werden muss. In Verbindung mit einem eindeutigen Konto-Code lassen sich sämtliche Ausgaben so sachlich in Kontenform darstellen. Die Verwendung unterschiedlicher Kontenpläne ist nicht vorgesehen.

Prüfungsurteil

[81] Die Anwendung erfüllt selbst einzelne Anforderungen an die Kontenfunktion.

4.3.4 Protokollierungsfunktion

Anforderung

[82] Bei programmgenerierten bzw. programmgesteuerten Buchungen, wie bspw. bei automatisierten Belegen, sind Änderungen an den einer Buchung zugrunde 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 Stamm- bzw. Bewegungsdaten.

Prüfungshandlungen der IT AUDIT

[83] Im Prüffeld Aufzeichnung von Datenänderungen untersuchten wir, ob

- programmgenerierte bzw. programmgesteuerte Änderungen an den zu einem Beleg gehörigen Generierungs- und Steuerungsdaten aufgezeichnet werden,
- rechnungslegungsrelevante Änderungen von Stammdaten protokolliert werden sowie
- Änderungen an Parametern in Änderungsprotokollen der Anwendung nachvollziehbar sind.

Prüfungsfeststellungen

[84] Systemeinstellungen u. -parameter werden in der Anwendung im jeweiligen Account gespeichert. Sie sind für den Anwender nicht einsehbar, können aber auf Datenbankebene ausgelesen werden.

[85] Ausgabenbezogene Informationen werden belegbezogen in einem sog. „Verlauf" gespeichert, wobei protokolliert wird, welcher User auf einen Beleg zugegriffen und welche Informationen neu eingegeben oder geändert wurden. Wir konnten im Prüffeld **Aufzeichnung von Datenänderungen** auf Basis eigener Prüfungshandlungen feststellen, dass so

- rechnungslegungsrelevante Änderungen von Daten in der Anwendung protokolliert werden sowie
- Änderungen an Parametern in Änderungsprotokollen gespeichert werden, wodurch sie mittels einer Historienfunktion („Verlauf") nachvollziehbar sind.

Prüfungsurteil

[86] Die Anwendung erfüllt die Anforderungen an die Protokollierungsfunktion.

4.3.5 Dokumentation

Anforderung

[87] Voraussetzung für die Nachvollziehbarkeit des Buchführungs- bzw. Rechnungslegungsverfahrens ist eine ordnungsgemäße Verfahrensdokumentation, die die Beschreibung aller zum Verständnis der Rechnungslegung erforderlichen Verfahrensbestandteile enthalten muss.

[88] Die GoB sowie ergänzend die GoBD verlangen das Vorhandensein einer Dokumentation, um einem sachverständigen Dritten innerhalb angemessener Zeit ein Verständnis der Buchhaltung zu verschaffen.

[89] Die Anforderung an den Umfang und Detaillierungsgrad der Dokumentation ist davon abhängig, inwieweit die ausgedruckte bzw. ausdruckbereite Buchführung aus sich heraus verständlich ist.

[90] Die Dokumentation soll in der Art gestaltet sein, dass sie

- den innerbetrieblichen Anforderungen im Hinblick auf Aufbau, Ablauf und wirtschaftliche Pflege des Verfahrens genügt und Unabhängigkeit von Detailkenntnissen bestimmter Personen gewährleistet sowie
- einen sachverständigen Dritten in die Lage versetzt, die IT-technische Abwicklung anhand der Dokumentation in angemessener Zeit zu prüfen.

[91] Die Verfahrensdokumentation eines Systems für eine IT-gestützte Rechnungslegung besteht aus der Anwenderdokumentation und der technischen Systemdokumentation sowie der Betriebsdokumentation.

[92] 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.

[93] Die technische Systemdokumentation soll über folgende – hier relevante - Bereiche informieren:

- Aufgabenstellung der IT-Anwendung im Kontext der eingesetzten Module oder Funktionalitäten
- Datenorganisation und Datenstrukturen (Datensatzaufbau)
- programmierte Verarbeitungsregeln einschließlich der implementierten Eingabe- und Verarbeitungskontrollen
- programminterne Fehlerbehandlungsverfahren sowie
- Schnittstellen zu anderen Systemen.

[94] Die Betriebsdokumentation dient der Dokumentation der ordnungsgemäßen Anwendung des Verfahrens. Dies betrifft u.a.

- Datensicherungsverfahren sowie
- Verarbeitungsnachweise (Verarbeitungs- und Abstimmprotokolle).

Prüfungshandlungen der IT AUDIT

[95] Im Verlauf unserer Prüfungshandlungen untersuchten wir, inwieweit die uns durch die Gesellschaft zur Verfügung gestellten Dokumentationsunterlagen hinsichtlich Inhalt, Umfang und Qualität den aus den GoB sowie ergänzend den GoBD abzuleitenden Anforderungen entsprechen.

[96] Im Prüffeld Ordnungsmäßigkeit der Dokumentation untersuchten wir, ob

- die Dokumentation derart beschaffen ist, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit ein Verständnis der Buchhaltung verschaffen kann sowie
- aus einer Anwenderdokumentation, einer technischen Systemdokumentation und einer Betriebsdokumentation besteht.

[97] Des Weiteren prüften wir, inwieweit die Dokumentationen die Anforderungen an

- die sachlogische Lösung
- die programmtechnische Lösung

- die Einhaltung der Programm- und Daten-Identität erfüllen sowie
- Arbeitsanweisungen für die Anwender beinhalten.

[98] Unserer Prüfung lagen nachfolgende durch die Gesellschaft erstellte Dokumentationen zugrunde:

- Per E-Mail übermittelte technische Informationen zu einzelnen Funktionalitäten der Anwendung,
- themenbezogene Darstellung des Einsatzes der payhawk Ausgabenverwaltung in Form von FAQ‘s
- technische Hintergrundinformationen (z. B. zur Anbindung von ERP-Systemen) in Form von FAQ‘s
- Installations- und Einführungshinweise in Form von FAQ’s sowie
- Erläuterung der Schnittstellen zur Anwendung oder zum Export aus der Anwendung in Form von FAQ’s sowie
- aus den FAQ’s ableitbare Informationen zur Erstellung einer Betriebsdokumentation.

Prüfungsfeststellungen

[99] Wir konnten im Prüffeld **Ordnungsmäßigkeit der Dokumentation** feststellen, dass

- eine in sich geschlossene, vollständige Dokumentation nicht vorliegt und
- hierfür notwendige diesbezügliche Informationen nicht vollumfänglich, sondern nur mehrheitlich aus den FAQ’s abgeleitet werden konnten.

[100] Bedingt durch die permanente Ergänzung der FAQ’s liegt eine Historisierung der Dokumentation anbieterseitig nicht vor, kann durch den Anwender durch regelmäßige Speicherung der FAQ’s aber erreicht werden.

[101] Analog zur Dokumentation der Gesellschaft weisen wir darauf hin, dass der Anwender beim Einsatz der Anwendung weitere benutzerspezifische (Verfahrens-)Dokumentationen benötigt, welche sich im Verantwortungsbereich des Anwenders befinden. Hierzu gehört die eigene Erstellung einer Dokumentation aus den FAQ’s.

Prüfungsurteil

[102] Die Anwendung erfüllt nur mit Einschränkungen die Anforderungen an eine Dokumentation.

4.3.6 Zugriffsschutz

Anforderung

[103] Die Vorgaben u. a. der Finanzverwaltung erfordern zum Schutz rechnungslegungsrelevanter Daten wirksame Zugriffsberechtigungskontrollen (auch) zur Einhaltung der Funktionstrennung.

[104] Zugriffsmöglichkeiten zu **payhawk Unternehmensausgaben** sind nach anerkannten Sicherheitsrichtlinien in der Weise zu gestalten, dass eingerichtete Zugriffsschutzverfahren nicht umgangen werden können.

Prüfungshandlungen der IT AUDIT

[105] Im Prüffeld **Berechtigungsverfahren** untersuchten wir, ob geeignete Sicherheitsrichtlinien in der Weise eingerichtet sind, dass bestehende Zugriffsschutzverfahren nicht umgangen werden können. Wir prüften

- die Funktionen des Zugriffsschutzsystems auf Anwenderebene,
- die Geheimhaltung von Passwortdateien bzw. die Geheimhaltung bei Eingabe von Passwörtern,
- die Einrichtung individueller Nutzerrechte,
- die Erfüllung der Anforderungen an die Passwortkomplexität bzw. regelmäßige Änderungen von Passwörtern sowie
- die Behandlung von Zugriffsverletzungen durch Eingabe inkorrekter Passwörter.

[106] Im Rahmen unserer Prüfungshandlungen untersuchten wir im Prüffeld **Dokumentation des Berechtigungsverfahrens**, ob ein dokumentiertes Berechtigungsverfahren vorliegt, in welchem

- die Erfüllung der Anforderungen an Passwortkomplexität bzw. regelmäßige Änderungen von Passwörtern sowie
- die Behandlung von Zugriffsverletzungen durch Eingabe inkorrekter Passwörter beschrieben und dokumentiert ist.

Prüfungsfeststellungen

[107] Wir konnten im Prüffeld **Berechtigungsverfahren** auf Basis eigener Prüfungshandlungen feststellen, dass

- Passwörter bei Eingabe am Bildschirm nicht sichtbar sind,
- inkorrekte Passworteingaben durch das System abgewiesen wurden sowie
- für jeden Nutzer individuelle Berechtigungen aus Berechtigungsgruppen vergeben werden.

[108] Die Vergabe von Berechtigungen, die Einrichtung von Passwörtern sowie systemseitige Parametrisierungen bezüglich des Zugangs zur Anwendung liegen im Verantwortungsbereich der Anwender, wobei wir keine Prüfungshandlungen auf Seiten der Anwender vornahmen

[109] Im Rahmen unserer Prüfungshandlungen wurde uns im Prüffeld **Dokumentation des Berechtigungsverfahrens** kein dokumentiertes Berechtigungsverfahren zur Verfügung gestellt. Funktionalitäten zur Vergabe von Berechtigungen können aus den FAQ's abgeleitet werden. Die

- Anforderungen an Passwortkomplexität sowie
- die Behandlung von Zugriffsverletzungen durch Eingabe inkorrekter Passwörter sind dort sachgerecht dokumentiert.

Prüfungsurteil

[110] Die Anwendung erfüllt bei sachgerechter Anwendung noch die Anforderungen an den Zugriffsschutz.

4.3.7 Datensicherungs-, Archivierungs- und Wiederanlaufverfahren

Anforderung

[111] Die Anwendung muss über geeignete Datensicherungsverfahren die Möglichkeit bieten, Daten und Programme regelmäßig zu sichern. Neben den von der verwendeten Datenbank vorgesehenen Maßnahmen (z.B. Transaktionssteuerung) können ggf. auch die im technischen und organisatorischen Umfeld verfügbaren Datensicherungsverfahren verwendet werden.

[112] Rechnungslegungsrelevante Daten und Unterlagen sind unter Berücksichtigung handelsrechtlicher Vorgaben geordnet aufzubewahren. Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Handelsbuch gemacht, die Eröffnungsbilanz oder der Jahresabschluss festgestellt, ein Handelsbrief empfangen bzw. abgesandt oder ein Buchungsbeleg entstanden ist.

Prüfungshandlungen der IT AUDIT

[113] Im Prüffeld **Datensicherung** prüften wir, durch welches Sicherungskonzept Transaktionen und Daten der Anwendung regelmäßig gesichert werden können.

[114] Im Rahmen unserer Prüfungshandlungen prüften wir im Prüffeld **Datenarchivierung**, ob die Gesellschaft den Anwendern eine Online-Speicherung aufzeichnungspflichtiger Daten über den Zeitraum der gesetzlichen handelsrechtlichen Aufbewahrungsfrist ermöglicht.

Prüfungsfeststellungen

[115] In Gesprächen mit der Gesellschaft sowie durch ergänzende Prüfungsnachweise konnten wir im Prüffeld **Datensicherung** feststellen, dass die Sicherung von Transaktionen und Daten der Anwendung ohne Einflussmöglichkeit des Anwenders durch den Betreiber der Cloud-Lösung umgesetzt werden muss. Dies gilt auch für die Archivierung.

[116] Da sich Datensicherung und -archivierung im Verfügungsbereich der Anwender befinden, nahmen wir in diesem Prüffeld keine weiteren Prüfungshandlungen vor.

Prüfungsurteil

[117] Bei sachgerechter Anwendung können die Anforderungen an Datensicherungs-, Archivierungs- und Wiederanlaufverfahren erfüllt werden. Dies setzt regelmäßige Datensicherungen durch den Anbieter der Cloud-Lösung sowie eine Datenarchivierung voraus.

4.4 Funktionsfähigkeit der Programmfunktionen

[118] Die Prüfung der programminternen Verarbeitungsregeln bzw. Parameter zur Verarbeitungssteuerung in der Anwendung erstreckt sich auf die Untersuchung der Korrektheit der Programmabläufe, der sachlogischen Richtigkeit der programmierten Verarbeitungsregeln sowie auf die Wirksamkeit der im Programm enthaltenen Plausibilitätskontrollen. Diese bestehen insbesondere aus Eingabe- und Verarbeitungskontrollen.

[119] Des Weiteren ist die Datenintegrität und -konsistenz sowohl auf datentechnischer Ebene als auch aus fachlicher und logischer Sicht durch entsprechende Verarbeitungskontrollen sicherzustellen, um fehlerhafte Datenkonstellationen zu verhindern.

4.4.1 Eingabekontrollen

Anforderungen

[120] Seitens der Anwendung sind bei der Dateneingabe und -erfassung programmierte Kontrollen vorzunehmen, die sicherstellen, dass nur sachlogisch korrekte und vollständige Daten mit zulässigem Format innerhalb bestimmter Mindest- und Höchstwerte in die weitere Verarbeitung übernommen werden.

[121] Eine Untersuchung der programmierten Kontrollen bei der Dateneingabe soll des Weiteren Informationen darüber liefern, inwieweit Prüfungen hinsichtlich fehlerhafter Dateneingaben in

der Softwareapplikation systemseitig durchgeführt werden und festgestellte Fehler eine zwangsläufige Fehlerberichtigung auslösen.

[122] Darüber hinaus sollen die Eingabekontrollen dazu beitragen, dass bereits festgeschriebene Daten nicht gelöscht oder verändert werden können.

Prüfungshandlungen der IT AUDIT

[123] Zur Prüfung der Angemessenheit der programmierten Eingabekontrollen führten wir Einzelfeldprüfungen unter Berücksichtigung nachfolgender Kriterien durch:

- Vollständigkeitsprüfungen
- Prüfungshandlungen bezüglich einer zwingenden Eingabe in erforderliche Datenfelder bzw. Mussfelder.
- Formatprüfungen
- Prüfungshandlungen, inwieweit nur Daten mit zulässigem Format (alphabetisch, numerisch oder alphanumerisch) eingegeben werden können.
- Grenzwertprüfungen
- Prüfungshandlungen, inwieweit nur Daten innerhalb bestimmter Mindest- und Höchstwerte eingegeben werden können.
- Zulässigkeitsprüfungen
- Prüfungshandlungen, inwieweit eine Prüfung der einzelnen Felder auf zulässige Eingaben erfolgt.

[124] Die Prüfung erfolgte anhand der Testfallmethode durch Eingabe korrekter sowie inkorrekter Daten im zugrundeliegenden Demo-Account.

[125] Im Prüffeld **Eingabekontrollen** untersuchten wir, ob

- programmierte Kontrollen bei der Dateneingabe und -erfassung bestehen,
- festgestellte Fehler eine zwangsläufige Abweisung von Daten auslösen sowie
- Eingabekontrollen verhindern, dass bereits festgeschriebene Daten gelöscht oder verändert werden können.

Prüfungsfeststellungen

[126] Wir konnten im Prüffeld **Berechtigungsverfahren** auf Basis eigener Prüfungshandlungen feststellen, dass

- dass inkonsistente Daten bei Dateneingabe und -erfassung systemseitig abgewiesen werden und in korrigierter Form erneut in die Anwendung eingegeben werden müssen sowie, dass
- Daten nach Archivierung nicht mehr gelöscht oder verändert werden.

Prüfungsurteil

[127] Die Softwareapplikation **payhawk Ausgabenverwaltung** erfüllt die Anforderungen an Eingabekontrollen.

4.4.2 Verarbeitungskontrollen

Anforderung

[128] Im Kontext der Verarbeitungskontrollen soll eine Aussage über die ordnungsmäßige Verarbeitung von Daten und der logischen Verknüpfungen im Hinblick auf die Richtigkeit der Ergebnisse getroffen werden. Es ist deshalb zu prüfen, ob die eingegebenen Daten richtig bearbeitet ausgegeben werden.

Prüfungshandlungen der IT AUDIT

[129] Im Prüffeld programminterne Verarbeitungsregeln untersuchten wir, ob

- Aussagen über die ordnungsmäßige Verarbeitung von Daten und logische Verknüpfungen im Hinblick auf die Richtigkeit der Ergebnisse getroffen werden können sowie
- eingegebene Daten richtig bearbeitet und korrekt zugeordnet werden.

[130] Im Verlauf unserer Prüfungshandlungen untersuchten wir das Prüffeld **Fehlerbehaftete Daten** dahingehend, ob

- fehlerhafte Datenkombinationen bezüglich der Modifikation von Beleginformationen vom System grundsätzlich erkannt und abgewiesen werden sowie,
- ob die payhawk Ausgabenverwaltung eine fehlerhafte Verarbeitung von Beleg- und Ausgabeninformationen zulässt.

Prüfungsfeststellungen

[131] Im Prüffeld **programminterne Verarbeitungsregeln** konnten wir in Gesprächen mit der Gesellschaft feststellen, dass

- der Softwareapplikation ein internes Kontrollsystem zugrunde liegt. Dies konnten wir im Rahmen unserer Prüfungshandlungen verifizieren. Eine Dokumentation hierzu liegt nicht vor.
- Belegtransaktionen im Rahmen eigener Prüfungshandlungen wurden korrekt in der Softwareapplikation erfasst und weitere Transaktionen (wie z. B. Zahlungsanfragen) ausgelöst.

[132] Wir konnten im Prüffeld **Fehlerbehaftete Daten** auf Basis eigener Prüfungshandlungen feststellen, dass

- fehlerhafte Stammdaten in der payhawk Ausgabenverwaltung nicht verarbeitet werden sowie
- Transaktionen mit fehlerhaften Daten systemseitig abgewiesen werden.

Prüfungsurteil

[133] Die Softwareapplikation payhawk Ausgabenverwaltung erfüllt die Anforderungen an die Verarbeitungskontrollen.

4.5 Besondere Anforderungen nach der Abgabenordnung

Anforderung

[134] Seit dem 01.01.2002 müssen Datenzugriffs- und Datenauswertungsmöglichkeiten für die Finanzverwaltung im Rahmen von Außenprüfungen geschaffen werden.

[135] Eine Softwareapplikation sollte hierzu über die nachfolgenden Funktionalitäten verfügen:

- Ein detailliertes Zugriffsberechtigungsverfahren, das die Möglichkeit des lesenden Zugriffs auf die zu prüfenden Daten ermöglicht,
- die Erfüllung der Datenträgerüberlassung sowie
- Schnittstellen für den Datenexport zur Weitergabe sämtlicher Daten (Stamm- und Bewegungsdaten) in gängigen Datenformaten.

[136] Zur Einhaltung von Datenzugriffs- und Datenauswertungsmöglichkeiten für die Finanzverwaltung sollte eine Softwareapplikation die Online-Speicherung von Daten über den Zeitraum der gesetzlichen steuerlichen Aufbewahrungsfrist ermöglichen.

Prüfungshandlungen der IT AUDIT

[137] Im Prüffeld **Datenzugriff** prüften wir, ob die Ausgabenverwaltung über ein Zugriffsberechtigungsverfahren verfügt, welches einem Betriebsprüfer fakultativ

- durch einen unmittelbaren Zugriff auf die zu prüfenden Daten,
- mittels maschineller Auswertung der zu prüfenden Daten durch den Steuerpflichtigen oder einen beauftragten Dritten nach den Vorgaben des Betriebsprüfers sowie
- in Form der Überlassung der zu prüfenden Daten auf einem elektronischen Datenträger

die Möglichkeit eines lesenden Zugriffs auf die zu prüfenden Daten ermöglicht.

[138] Wir prüften im Prüffeld **Schnittstellen**, ob Schnittstellen für den Datenexport implementiert sind.

[139] Im Rahmen unserer Prüfungshandlungen prüften wir im Prüffeld **Archivierung**, ob die payhawk Ausgabenverwaltung eine Online-Speicherung aufzeichnungspflichtiger Daten über den Zeitraum der gesetzlichen steuerlichen Aufbewahrungsfrist ermöglicht.

Prüfungsfeststellungen

[140] Wir konnten durch eigene Prüfungshandlungen im Prüffeld **Datenzugriff** klären**,** dass bezüglich der zu prüfenden Daten

- einem Betriebsprüfer ein lesender Zugriff in eingerichtet werden kann,
- eine maschinelle Auswertung nach den Vorgaben eines Betriebsprüfers möglich ist sowie
- eine Extraktion auf einen mobilen Datenträger durchgeführt werden kann.

[141] Die Einrichtung eines Datenzugriffs für einen Betriebsprüfer befindet sich im Verfügungsbereich der Anwender. Prüfungshandlungen auf Seiten der Anwender nahmen wir nicht vor.

[142] Wir konnten im Prüffeld **Schnittstellen** im Verlauf unserer Prüfungshandlungen feststellen, dass in Schnittstellen für den Datenexport zur Weitergabe von unterschiedlichen Daten (z. B. Beleginformationen, Belegbilder etc.) in gängigen Datenformaten implementiert sind.

[143] Im Prüffeld **Archivierung** stellten wir in Gesprächen mit der Gesellschaft fest, dass

- die Datenbank, welche den Anwendern der Payhawk Ausgabenverwaltung zur Verfügung gestellt wird, eine revisionssichere Archivierung von Daten unter Einhaltung der steuerlichen Aufbewahrungsfristen ermöglicht.

[144] Die Archivierung von Daten befindet sich im Verfügungsbereich der Anwender. Prüfungshandlungen auf Seiten der Anwender nahmen wir nicht vor.

Prüfungsurteil

Die Softwareapplikation payhawk Ausgabenverwaltung erfüllt bei sachgerechter Anwendung der Softwareapplikation durch die Anwender die Anforderungen nach der Abgabenordnung.

5. Zusammengefasstes Prüfungsergebnis und Softwarebescheinigung

[145] Gemäß dem uns am 26.10.2022 erteilten Auftrag der Payhawk Ltd., London, prüften wir die Ordnungsmäßigkeit und Sicherheit der Anwendung:

„payhawk Unternehmensausgaben" in der Version 6 vom 01.02.2023

[146] 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 der Grundlage der von uns durchgeführten Prüfung eine Beurteilung über das Softwareprodukt abzugeben.

[147] Wir haben unsere Prüfung unter Beachtung des vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) veröffentlichten 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 entsprechende Indizierung, Speicherung und Abfrage von elektronischen Dokumenten ermöglicht und den auftragsgemäß zugrunde gelegten Kriterien entspricht. Dies umfasst unsere Beurteilung, ob die Kriterien durch die Verarbeitungsfunktionen und durch das programmierte Kontrollsystem angemessen umgesetzt sind sowie ob eine aussagefähige Verfahrensdokumentation vorliegt. Die Wirksamkeit der Programmfunktionen wird anhand von Testfällen beurteilt.

[148] Unserer Prüfung haben wir auftragsgemäß die folgenden handelsrechtlichen Kriterien und Prüfungsnormen zugrunde gelegt:

- die gesetzlichen Vorschriften des Handelsrechts (§§ 238 ff. HGB),
- die Grundsätze ordnungsmäßiger Buchführung (GoB),
- den Prüfungsstandard „Die Prüfung von Softwareprodukten" (IDW PS 880) sowie
- die vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) herausgegebene Stellungnahme zur Rechnungslegung "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)".

[149] Die "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)" wurden als Verordnung des Steuerrechts ergänzend beachtet.

[150] 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.

[151] Wir haben die rechnungslegungsrelevanten Funktionen innerhalb der Anwendung **payhawk Unternehmensausgaben** hinsichtlich der Einhaltung von Ordnungsmäßigkeits- und Sicherheitsanforderungen geprüft. Die Prüfung bezog sich auf die Anwendung in der Version 6 vom 01.02.2023.

[152] Wir haben die rechnungslegungsrelevanten Prozessfunktionen geprüft. Hierzu haben wir sowohl falsche als auch inkonsistente Daten eingegeben, um systemseitige Eingabe- und Plausibilitätskontrollen zu prüfen. Unsere durchgeführten Transaktionen wurden systemseitig vollständig und richtig abgebildet. Durchgeführte Transaktionen waren in Form von "Audit Trails" nachvollziehbar. Die Veränderung und Löschung von bereits erfassten Transaktionen oder Konten, konnte systemseitig durch entsprechende Parametrisierung und Berechtigungsvergaben unterbunden werden.

[153] Die Softwareapplikation **payhawk Unternehmensausgaben** konnte die Anforderungen an die Belegfunktion, Journalfunktion, Kontenfunktion, Protokollierungsfunktion, Dokumentation, Zugriffsschutz sowie Datensicherungs-, Archivierungs- und Wiederanlaufverfahren erfüllen. Eine Funktionstrennung kann systemseitig durch Vergabe von Benutzer-IDs, Passwortschutz und eine entsprechende Berechtigungsvergabe umgesetzt werden. Unautorisierte Zugriffe wurden von der Anwendung zurückgewiesen.

[154] Die innerhalb der Anwendung **payhawk Unternehmensausgaben** abgebildeten Prozesse haben wir auf ihre logische Richtigkeit geprüft, ebenso wie auf programmierte Verarbeitungsregeln zur Eingabe- und Verarbeitungskontrolle.

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

[156] Nach unserer Beurteilung auf Grund der bei der Prüfung gewonnenen Erkenntnisse, über die wir mit Datum vom 03.02.2023 gesondert Bericht erstattet haben, ermöglicht die von uns geprüfte Softwarelösung **payhawk Unternehmensausgaben** in der Version 6 vom 01.02.2023 mit hinreichender Sicherheit und bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung und entspricht den vorstehend aufgeführten Kriterien.

[157] Wir erteilen diese Bescheinigung auf Grundlage des mit der Payhawk Ltd. geschlossenen Vertrags. Dieser Bescheinigung liegen mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde. Die in den Allgemeinen Auftragsbedingungen enthaltenen Höchstgrenzen gelten gegenüber allen Personen, welche diese Bescheinigung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich.

Köln, den 23.02.2023

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Alexander Neu
24.02.2023 11:52:38 [UTC+1]

Neu
Wirtschaftsprüfer

Thomas Grigo
24.02.2023 11:48:18 [UTC+1]

Grigo
CRISC, CISA, CISM, CDPSE, CIA

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Payhawk Limited

London

2023

Anlage 1

Softwarebescheinigung

Bescheinigung über die Durchführung einer Softwareprüfung

An die gesetzlichen Vertreter der Payhawk Limited

Payhawk Limited, London, hat uns am 26.10.2022 beauftragt, eine Prüfung des Softwareprodukts

„payhawk"

Version 6 vom 01.02.2023

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 der Grundlage der von uns durchgeführten Prüfung eine Beurteilung über das Softwareprodukt abzugeben.

Wir haben unsere Prüfung unter Beachtung des vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) veröffentlichten 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 entsprechende Indizierung, Speicherung und Abfrage von elektronischen Dokumenten ermöglicht und den auftragsgemäß zugrunde gelegten Kriterien entspricht. Dies umfasst unsere Beurteilung, ob die Kriterien durch die Verarbeitungsfunktionen und durch das programmierte Kontrollsystem angemessen umgesetzt sind und eine aussagefähige Verfahrensdokumentation vorliegt. Die Wirksamkeit der Programmfunktionen wird anhand von Testfällen beurteilt.

Unserer Prüfung haben wir auftragsgemäß die nachfolgenden Kriterien zugrunde gelegt:

- die gesetzlichen Vorschriften des Handelsrechts (§§ 238 ff. HGB),
- die Grundsätze ordnungsmäßiger Buchführung (GoB),
- die vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) herausgegebene Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)",
- die vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) herausgegebene Stellungnahme zur Rechnungslegung: „Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)" sowie
- die vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) herausgegebene Stellungnahme zur Rechnungslegung: „Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing (IDW RS FAIT 5)".

Die nachfolgenden Gesetze und Verordnungen des Steuerrechts wurden als Prüfkriterien ergänzend beachtet:

- Gesetzliche Vorschriften des Steuerrechts (§§ 140 - 148 AO) sowie
- das Schreiben des Bundesministeriums der Finanzen „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)" vom 28. November 2019.

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 haben die rechnungslegungsrelevanten Funktionen innerhalb der Anwendung payhawk hinsichtlich der Einhaltung von Ordnungsmäßigkeits- und Sicherheitsanforderungen geprüft. Die Prüfung bezog sich auf das Release 6 vom 01.02.2023.

Für die Prüfung der rechnungslegungsrelevanten Prozessfunktionen haben wir sowohl inkorrekte als auch inkonsistente Daten verwendet, um systemseitige Eingabe- und Plausibilitätskontrollen zu prüfen. Die von uns durchgeführten Transaktionen wurden systemseitig vollständig und richtig abgebildet.

Durchgeführte Transaktionen waren anhand einer durchgängigen Belegnummernsystematik nachvollziehbar. Die Veränderung oder Löschung von bereits erfassten Transaktionen und Stammdaten wird systemseitig unterbunden.

Die Softwareapplikation payhawk konnte die Anforderungen an die Belegfunktion, die Journalfunktion, die Kontenfunktion, die Protokollierungsfunktion, die Dokumentation, den Zugriffsschutz sowie die Datensicherungs-, Archivierungs- und Wiederanlaufverfahren erfüllen.

Die innerhalb der Anwendung payhawk abgebildeten Prozesse haben wir auf ihre logische Richtigkeit geprüft, ebenso wie auf programmierte Verarbeitungsregeln zur Eingabe- und Verarbeitungskontrolle.

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

Ohne diese Beurteilung einzuschränken, weisen wir auf folgende Sachverhalte hin:

- Auf Grund immanenter Grenzen einer Softwareprüfung besteht ein unvermeidbares Risiko, dass wesentliche Fehler oder Fehlfunktionen im Rahmen unserer Prüfung unentdeckt bleiben.
- 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 oder regulatorischer Vorgaben funktionale Anforderungen nicht mehr erfüllt werden.

Klarstellend weisen wir des Weiteren darauf hin, dass die sachgerechte Anwendung und der ordnungsmäßige Betrieb von payhawk insbesondere die Umsetzung der folgenden Maßnahmen beim Kunden beinhalten sollte:

- Es ist durch technische und organisatorische Maßnahmen sicherzustellen, dass die zu verarbeiteten Daten vollständig in payhawk übertragen werden.
- Der Anwender hat sicher zu stellen, dass seine für das System genutzte Anmeldekennung und das Anmeldepasswort ausschließlich den dafür befugten Mitarbeitern bekannt sind.
- Es ist durch organisatorische Maßnahmen 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.

Die Gesellschaft sollte die bestehenden Teile der Verfahrensdokumentation, die nur als FAQ's vorliegen, in eine einheitliche und in sich geschlossene Dokumentation zusammenführen und die Dokumentation inhaltlich noch ergänzen.

Nach unserer Beurteilung, auf Grund der bei der Prüfung gewonnenen Erkenntnisse, über die wir mit Datum vom 06.02.2023 gesondert Bericht erstattet haben, ermöglicht die von uns geprüfte Softwarelösung **payhawk Unternehmensausgaben** Release 6 vom 01.02.2023 bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung und entspricht den vorstehend aufgeführten Kriterien.

Wir erteilen diese Bescheinigung auf Grundlage des mit **Payhawk Ltd, London**, 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 bestehen.

Köln, den 23.02.2023

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Alexander Neu
24.02.2023 11:52:40 [UTC+1]

Neu
Wirtschaftsprüfer

Thomas Grigo
24.02.2023 11:48:20 [UTC+1]

Grigo
CRISC, CISA, CISM, CDPSE, CIA

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Payhawk Limited

London

2023

Anlage 2

Vollständigkeitserklärung

Letter of representation

Payhawk Ltd.
Polygraphia Office Center
47 Tsarigardsko Shose Blvd
1124 Sofia

Bulgarien

Sofia (Location), the 2023 01 31

To IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft
Im MediaPark 5a
D-50670 Köln

(company)

Audit of software products in accordance with the *IDW Auditing Standard: The Audit of Software Products (IDW PS 880)* [1]

The subject of the test of the software product payhawk corporate expenses is the release/version no. 6 from 2023 02 01 with the modules App for iOS 3.41.

I / we, as the legal representative(s) (board member(s) / managing director(s) /) / managing partner(s) / owner /
_____ of the company the following:

A. Clarifications and evidence

I / we have provided you with the clarifications and evidence required for your examination of the above-mentioned software product and those requested by you in full and to the best of our knowledge and belief. I / we have named the persons listed below as persons providing information:

Thomas Westerhoven, Miglen Evlogiev

These persons have been instructed by me / us to provide you with all necessary and all requested information and evidence correctly and completely.

B. Software development procedures and procedural documentation

1. I am / We are responsible for establishing, maintaining and documenting a software development process suitable for identifying, managing and monitoring the risks arising from software development.

2. I / we have named the criteria used in software development as a yardstick for the implementation of the functional requirements for the software product or, in the case of self-developed criteria, have made them available to you in full.

1 Please delete non-applicable items or make applicable additions. Please delete non-applicable numbers or text passages.

☐ Please mark with a cross where applicable.

3. I / we have made available to you in full the procedural, test and acceptance documentation for the software as well as all other information relevant to the audit (in particular technical concepts). The documentation comprises the components listed in the annex.

4. I / we have provided you with the complete and up-to-date programmes, modules and interfaces (internal and external) required for the use and assessment of the software product. A compilation of the programmes, modules and interfaces (internal and external) is attached.

5. For testing purposes, I / we have provided you with the following test environment:

   Hardware/Network:

   Mobile Devices with Internet Access

   Software/data:

   Microsoft Edge 109.0.1518.78 (64Bit) for Windows 11 Pro,
   Google Chrome 108.0.5359.125 (64Bit)

   Apple Safari for iOS 16.2, Payhawk App Vers. 3.42 for iOS

6. Defects or impairments of the software product, the software development procedure (including the procedure, test and acceptance documentation) or the technical concept.

   ☐ are currently not available.

   ☐ have been communicated to you in full in writing or are listed in the annex. _listed.

7. Changes to the software, the software development procedure (including the procedure, test and acceptance documentation) or the technical concept that affect your audit have not been made by me / us without your knowledge.

8. The results of previous audits of the software product or parts or modules (e.g. by internal audit, other auditors), the associated reports, certificates, etc., as well as the resulting measures taken by the company.

   ☐ have been submitted to you in writing in their

   ☐ entirety. Previous audits have not taken place.

C. Additions and remarks

DocuSigned by:
3F4A220E90A7469...

Hristo Borisov,
manager

Company stamp and signatures

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Payhawk Limited

London

2023

Anlage 3

Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften

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.