Vereinbarung zur Verschwiegenheit

nach § 50a Wirtschaftsprüferordnung (WPO) mit Belehrung nach § 203 Strafgesetzbuch (StGB) – für die Nutzung der Anwendung „Prüfungsplaner“

Muster – vor Verwendung rechtlich prüfen lassen. Gelb markierte Stellen sind Platzhalter und von der Kanzlei auszufüllen. Diese Vereinbarung ersetzt nicht den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.

zwischen

Auftraggeber

[Name der Kanzlei / Wirtschaftsprüfungsgesellschaft]

[Anschrift]

– nachfolgend „Kanzlei“ –

Dienstleister

Johannes Hollenberg

Wißmarer Weg 44, 35396 Gießen

– nachfolgend „Dienstleister“ –

§ 1 Gegenstand

(1) Der Dienstleister stellt der Kanzlei die Web-Anwendung „Prüfungsplaner“ bereit und betreibt sie. Mit der Anwendung lädt die Kanzlei Bilanzen und Gewinn- und Verlustrechnungen ihrer Mandanten hoch, lässt Wesentlichkeit und Toleranzwesentlichkeit berechnen und erhält ausgefüllte Planungsdokumente.

(2) Bei Betrieb, Wartung und Fehlerbehebung kann der Dienstleister Zugang zu Tatsachen erhalten, die der Verschwiegenheitspflicht der Kanzlei nach § 43 WPO unterliegen („geschützte Informationen“). Diese Vereinbarung regelt den Umgang damit nach § 50a WPO.

§ 2 Verschwiegenheit

(1) Der Dienstleister verpflichtet sich, über alle geschützten Informationen, die ihm im Rahmen dieser Tätigkeit bekannt werden, Stillschweigen zu bewahren und sie weder zu offenbaren noch zu verwerten.

(2) Die Pflicht gilt gegenüber jedermann, auch gegenüber anderen Kunden des Dienstleisters, und besteht nach Ende der Zusammenarbeit unbefristet fort.

§ 3 Kenntnisnahme nur soweit erforderlich

(1) Der Dienstleister verschafft sich Kenntnis von geschützten Informationen nur, soweit dies zur Erfüllung des Auftrags erforderlich ist, insbesondere für Betrieb und Fehlerbehebung.

(2) Technisch ist sichergestellt, dass der Dienstleister als Gesamt-Administrator weder Mandantennamen noch Zahlen oder Dokumente sieht. Einblick erhält er nur, wenn ein Team-Administrator der Kanzlei ihn ausdrücklich, zeitlich begrenzt und für einen festgelegten Umfang freigibt. Jeder solche Zugriff wird protokolliert.

§ 4 Einsatz weiterer Personen und Unterauftragnehmer

(1) Der Dienstleister erbringt die Leistung persönlich. Weitere Personen (z. B. Mitarbeiter, freie Mitarbeiter) setzt er nur ein, wenn er sie zuvor in Textform zur Verschwiegenheit verpflichtet und über die strafrechtlichen Folgen belehrt hat.

(2) Die Kanzlei ist damit einverstanden, dass für den Betrieb folgende Anbieter eingesetzt werden:

- **Render Services, Inc.** – Betrieb von Server und Datenbank; Rechenzentrum in Frankfurt am Main.
- **Anthropic PBC** – KI-Dienst „Claude“ zur Zuordnung der Bilanz- und GuV-Posten; Verarbeitung in den USA.

(3) Beide Anbieter sind über ihre Vertragsbedingungen und Auftragsverarbeitungsverträge zur Vertraulichkeit verpflichtet. Weitere oder andere Unterauftragnehmer setzt der Dienstleister nur nach vorheriger Zustimmung der Kanzlei in Textform ein.

§ 5 Dienstleistungen im Ausland, Einwilligung der Mandanten

(1) Für den KI-Dienst werden Daten in die USA übermittelt. Um den Schutz der geschützten Informationen zu gewährleisten, gelten die in der Anlage beschriebenen Maßnahmen, insbesondere die Beschränkung auf Bilanz und GuV und die Schwärzung von Mandantennamen und Kontaktdaten vor dem Versand.

(2) Ob der Schutz im Sinne von § 50a Abs. 4 WPO vergleichbar ist oder der Geheimnisschutz die Übermittlung nicht gebietet, beurteilt die Kanzlei in eigener Verantwortung. Dient die Nutzung unmittelbar einem einzelnen Mandat, holt die Kanzlei die nach § 50a Abs. 5 WPO erforderliche Einwilligung des Mandanten ein. Die Anwendung kann so eingestellt werden, dass diese Einwilligung vor jedem Lauf bestätigt werden muss.

§ 6 Belehrung über die strafrechtlichen Folgen

Der Dienstleister wurde darüber belehrt, dass er als an der Berufsausübung mitwirkende Person bei einer Verletzung der Verschwiegenheit strafrechtlich verantwortlich ist:

- **§ 203 Abs. 4 StGB:** Wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
- **§ 203 Abs. 6 StGB:** Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, droht Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.
- **§ 204 StGB:** Wer ein solches Geheimnis unbefugt verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Die Strafbarkeit besteht auch nach Ende der Zusammenarbeit fort.

§ 7 Meldepflicht, Löschung, Beendigung

(1) Der Dienstleister informiert die Kanzlei unverzüglich, wenn er Anhaltspunkte für eine Verletzung der Verschwiegenheit oder einen unbefugten Zugriff hat.

(2) Nach Ende der Zusammenarbeit löscht der Dienstleister alle Daten der Kanzlei, soweit keine gesetzliche Aufbewahrungspflicht besteht, und bestätigt dies in Textform.

(3) Die Kanzlei kann die Zusammenarbeit fristlos beenden, wenn der Dienstleister gegen diese Vereinbarung verstößt (§ 50a Abs. 2 WPO).

§ 8 Datenschutz, Schlussbestimmungen

(1) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt. Die Verarbeitung personenbezogener Daten regelt ein gesonderter Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.

(2) Änderungen bedürfen der Textform. Die Anlage „Datenverarbeitung, KI und Schwärzung“ ist Bestandteil dieser Vereinbarung.

Ort, Datum: _____	Ort, Datum: _____
_____	_____
Kanzlei	Dienstleister
[Name, Funktion]	Johannes Hollenberg

Anlage: Datenverarbeitung, KI und Schwärzung

So geht der Prüfungsplaner mit den hochgeladenen Abschlüssen um.

1. Ablauf eines Laufs

1. Ein Teammitglied lädt Bilanz und GuV hoch – als zwei Dateien oder als ein Gesamt-PDF (z. B. Auszug aus dem Unternehmensregister).
2. Der Server (Frankfurt am Main) liest den Text aus. Bei einem Gesamt-PDF werden nur die Abschnitte Bilanz und GuV verwendet; Anhang, Lagebericht und Bestätigungsvermerk werden nicht an die KI übermittelt.
3. Vor dem Versand wird der Text geschwärzt (siehe Abschnitt 2). Eine Vorschau zeigt vorab genau, was an die KI geht.
4. Die KI ordnet die Posten den Zeilen der Vorlagen zu und kopiert die Beträge wörtlich. Sie rechnet nicht.
5. Alle Berechnungen und Kontrollen erfolgen auf dem Server: Wesentlichkeit, Toleranzwesentlichkeit und Nichtaufgriffsgrenze nach der Regel der Kanzlei; jeder Betrag muss im PDF vorkommen; Summen Aktiva, Passiva und Jahresergebnis müssen mit dem PDF übereinstimmen.
6. Der Prüfer legt die Wesentlichkeit fest; danach werden die Planungsdokumente erstellt.

2. Schwärzung vor dem Versand an die KI

Automatisch durch Platzhalter ersetzt werden:

- der Mandantenname, so wie er bei der Anlage des Laufs eingegeben wurde, sowie weitere vom Nutzer angegebene Begriffe;
- Firmennamen mit Rechtsform (z. B. „… GmbH“, „… GmbH & Co. KG“);
- Handelsregisternummern (HRA, HRB …), IBAN, E-Mail-Adressen, Telefonnummern und Anschriften.

Nicht geschwärzt werden die Beträge, Postenbezeichnungen und Jahreszahlen – sie werden für die Zuordnung benötigt. Ohne Namen und Kontaktdaten lassen sich die Zahlen in der Regel keinem Unternehmen zuordnen.

Grenzen: Die Schwärzung arbeitet mit Mustern. Ist der Name im Dokument anders geschrieben als eingegeben oder ohne Rechtsform genannt, kann er durchrutschen. Deshalb vor dem Start die Vorschau prüfen und ggf. zusätzliche Begriffe angeben.

3. Der KI-Dienst (Anthropic)

- Nutzung über die Programmierschnittstelle (API) mit kommerziellen Vertragsbedingungen und Auftragsverarbeitungsvertrag inkl. EU-Standardvertragsklauseln.
- Laut Anbieterbedingungen werden die übermittelten Daten nicht zum Training verwendet und innerhalb von 30 Tagen gelöscht.
- Die Übertragung erfolgt verschlüsselt (TLS).

4. Speicherdauer

- Hochgeladene PDFs: sofort nach der Auswertung durch die KI gelöscht.
- Ausgelesener Text von Bilanz und GuV: bis zur Festlegung der Wesentlichkeit, höchstens 24 Stunden.

- Ergebnisse (Excel-Dateien, Prüfprotokoll, KI-Antworten): automatisch nach 90 Tagen gelöscht. Die Anwendung ist kein Archiv – Ergebnisse gehören in die Prüfungsakte.
- Verwaltungsprotokoll (ohne Mandantennamen und Zahlen): nach 3 Jahren gelöscht.

5. Zugriff

- Jede Person sieht nur die Mandate ihrer eigenen Teams.
- Der Dienstleister sieht als Gesamt-Administrator keine Mandate, Zahlen oder Dokumente – außer nach ausdrücklicher, zeitlich begrenzter Freigabe durch einen Team-Administrator. Jeder Zugriff wird im Teamprotokoll vermerkt.
- Anmeldung mit persönlichem Passwort (nur als Hash gespeichert), Sperre nach fünf Fehlversuchen, automatische Abmeldung nach 30 Minuten Inaktivität.