

Vereinbarung über die Verschwiegenheit mitwirkender Personen

für Rechtsanwälte, Steuerberater, Notare und Wirtschaftsprüfer

Art dieses Dokuments	Muster - Ansichtsstueck, auf niemanden ausgestellt
Fassung	schweigepflicht-rb-2026-11
Stand	18. Oktober 2026
Pruefsumme des Wortlauts	sha256:65230c1b883b87784e2565e8433b24e4b245811ae28a8d2904f3fe5803934606
Ausgestellte Fassung	entsteht bei der Annahme im Konto; sie traegt Name und Datum des Auftraggebers und wird ihm per E-Mail zugestellt.
Herausgeber	TitanCore24 - Robin Knecht

Inhalt dieses Dokuments

1. Vereinbarung über die Verschwiegenheit mitwirkender Personen
2. Anlage 1 — Leistungsbeschreibung
3. Anlage 2 — Mitwirkende Personen
4. Anlage 3 — Technische und organisatorische Maßnahmen
5. Anlage 4 — Auftragsverarbeitungsvertrag (Art. 28 DSGVO)
6. Anlage 5 — Wortlaute der maßgeblichen Vorschriften

Muster, unverbindlich. Kein Rechtsrat. Verbindlich ist allein die Fassung, die dem Auftraggeber nach seiner Annahme im Konto ausgestellt und per E-Mail zugestellt wird; sie traegt seinen Namen und das Datum der Annahme. Herausgeber: TitanCore24 · OBI-Systems, Robin Knecht.

Vereinbarung über die Verschwiegenheit mitwirkender Personen

für Rechtsanwälte, Steuerberater, Notare und Wirtschaftsprüfer nach § 43e BRAO, § 62a StBerG, § 26a BNotO, § 50a WPO in Verbindung mit § 203 StGB

Fassung: schweigepflicht-rb-2026-11 · **Stand:** 18. Oktober 2026 **Textform nach § 126b BGB** · gilt neben dem Auftragsverarbeitungsvertrag (Anlage 4), nicht statt seiner

In einfachen Worten. Ihr Berufsrecht erlaubt Ihnen, uns als Dienstleister einzuschalten — aber nur, wenn wir in Textform zur Verschwiegenheit verpflichtet sind und über die strafrechtlichen Folgen belehrt wurden. Genau das leistet dieses Dokument. Der Auftragsverarbeitungsvertrag (Anlage 4) schützt Ihre Mandanten nach Datenschutzrecht; er ersetzt diese Verpflichtung **nicht**, weil er das Strafrecht nicht abdeckt. Beide Papiere gelten nebeneinander.

Was dieses Dokument nicht tut. Es macht Ihre Nutzung des Dienstes nicht von sich aus berufsrechtskonform. Ob und wie Sie einen externen Dienstleister einsetzen dürfen — und ob Sie die Einwilligung Ihres Mandanten brauchen (dazu die Muster-Einwilligung) — entscheidet sich in Ihrer Kanzlei, nicht hier. Dieses Dokument stellt Ihnen bereit, was das Gesetz **von uns** verlangt.

§ 1 Parteien und Gegenstand

(1) Diese Vereinbarung wird geschlossen zwischen

- dem **Auftraggeber** — der Rechtsanwältin, dem Rechtsanwalt, der Steuerberaterin, dem Steuerberater, der Notarin, dem Notar, der Wirtschaftsprüferin oder dem Wirtschaftsprüfer, die oder der den Dienst nutzt (im Folgenden „Auftraggeber“) — und
- **Robin Knecht, TitanCore24** (im Folgenden „Dienstleister“), Anschrift und Kontaktangaben nach dem Impressum des Dienstes.

(2) Der Auftraggeber ist Berufsgeheimnisträger im Sinne des § 203 Abs. 1 Nr. 3 StGB. Der Dienstleister ist eine an der beruflichen Tätigkeit des Auftraggebers **mitwirkende Person** im Sinne des § 203 Abs. 3 Satz 2 StGB und der genannten berufsrechtlichen Vorschriften.

(3) Gegenstand ist die Verpflichtung des Dienstleisters zur Verschwiegenheit über fremde Geheimnisse, die ihm bei der Erbringung der beauftragten Leistungen bekannt werden. Welche Verarbeitungsarten die beauftragten Leistungen umfassen, beschreibt **Anlage 1** (Leistungsbeschreibung). Diese Vereinbarung ist als Anlage änderbar gehalten: Ein späterer neuer Leistungsbestandteil führt zu einem Wechsel der betroffenen Anlage, nicht zu einem neuen Vertrag.

§ 2 Verschwiegenheit und Belehrung über die strafrechtlichen Folgen

(1) Der Dienstleister verpflichtet sich, über alle fremden Geheimnisse, die ihm im Rahmen der Leistungserbringung bekannt werden — insbesondere Tatsachen aus dem Mandats-, Beratungs- oder Amtsverhältnis des Auftraggebers und die Identität der betroffenen Personen —, **Verschwiegenheit zu wahren**. Er offenbart sie nicht und verwertet sie nicht.

(2) Die Verschwiegenheitspflicht gilt **zeitlich unbegrenzt** und **über die Beendigung dieser Vereinbarung und des zugrunde liegenden Vertragsverhältnisses hinaus**.

(3) **Belehrung (§ 43e Abs. 3 Satz 2 Nr. 1 BRAO und die entsprechenden Vorschriften).** Der Dienstleister ist darüber belehrt, dass die unbefugte Offenbarung eines fremden Geheimnisses durch eine mitwirkende Person nach **§ 203 Abs. 4 Satz 1 StGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe** bestraft wird. Er ist ferner darüber belehrt, dass ihn nach **§ 203 Abs. 4 Satz 2 Nr. 2 StGB** eine eigene Strafbarkeit trifft, wenn er sich einer weiteren mitwirkenden Person bedient und nicht dafür Sorge trägt, dass auch diese zur Geheimhaltung verpflichtet wird. Der Wortlaut der genannten Vorschriften liegt als **Anlage 5** bei; die Belehrung ist erst mit dieser Anlage vollständig.

(4) Der Dienstleister bestätigt, dass er diese Belehrung zur Kenntnis genommen hat, und nimmt die Verpflichtung an. Die Annahme des Auftraggebers erfolgt in Textform durch die im Konto dokumentierte Zustimmung zu dieser Fassung.

§ 3 Beschränkung auf das Erforderliche · keine Auswertung, kein Training

(1) **Erforderlichkeit (§ 43e Abs. 3 Satz 2 Nr. 2 BRAO).** Der Dienstleister verschafft sich nur insoweit Kenntnis von fremden Geheimnissen, als dies zur Erfüllung der beauftragten Leistung erforderlich ist. Ein weitergehender Zugriff findet nicht statt.

(2) **Keine Zweckentfremdung.** Der Dienstleister verarbeitet die Inhalte des Auftraggebers ausschließlich zur Erbringung der jeweils gebuchten Aufgabe. Eine Auswertung zu eigenen Zwecken, eine Zusammenführung mit anderen Beständen oder eine Weitergabe zu Werbe- oder Analysezwecken findet nicht statt.

(3) **Kein Training.** Inhalte des Auftraggebers werden **nicht zum Training oder zur Weiterentwicklung von Modellen künstlicher Intelligenz verwendet** — weder durch den Dienstleister noch durch die in Anlage 2 genannten mitwirkenden Personen. Gegenüber dem Betreiber der eingesetzten Erkennungs- und Sprachdienste ist die Nutzung von Inhalten zur Weiterentwicklung dieser Dienste ausdrücklich abbestellt („AI services opt-out“); Inhalte verlassen dadurch auch zu diesem Zweck nicht den vereinbarten Verarbeitungsraum (§ 5).

§ 4 Weitere mitwirkende Personen (Unterauftragnehmer)

(1) **Namentliche Nennung (§ 43e Abs. 3 Satz 2 Nr. 3 BRAO).** Der Dienstleister ist befugt, zur Erfüllung des Vertrags weitere Personen heranzuziehen. Diese sind in **Anlage 2** namentlich benannt. Der Dienstleister ist verpflichtet und hat sichergestellt, dass jede dieser Personen in Textform zur Verschwiegenheit verpflichtet ist.

(2) **Anzeige bei eigenen direkten Dienstleistern.** Beabsichtigt der Dienstleister, einen **eigenen direkten** weiteren Dienstleister neu hinzuzuziehen oder auszutauschen, zeigt er dies dem Auftraggeber **mindestens 30 Tage vorher** in Textform an die im Konto hinterlegte Adresse an.

(3) **Kette unterhalb des Betreibers.** Für die von der Amazon Web Services EMEA SARL ihrerseits eingesetzten Unterauftragnehmer verweist der Dienstleister auf die **öffentliche Unterauftragnehmerliste** des Betreibers (Anlage 2). Der Betreiber aktualisiert diese Liste nach seinen Angaben mindestens 30 Tage, bevor er einen neuen Unterauftragnehmer einsetzt.

(4) **Widerspruch.** Widerspricht der Auftraggeber einer angezeigten Änderung nach Absatz 2 oder Absatz 5 aus einem berufs- oder datenschutzrechtlichen Grund in Textform, so kann er den Vertrag zum Zeitpunkt der geplanten Umstellung **kündigen**; nicht verbrauchtes Guthaben wird in diesem Fall vollständig ausgezahlt. Ein Anspruch auf Umbau der Infrastruktur des Dienstleisters besteht nicht.

(5) **Erweiterung des EU-Regionskreises der KI-Verdichtung.** Der Kreis der EU-Regionen, in denen die gebuchte KI-gestützte Verdichtung berechnet werden kann (§ 5 Absatz 2, Anlage 2), wird durch das verwendete Inferenzprofil des Betreibers bestimmt; der Dienstleister setzt ihn nicht selbst. Nimmt der Betreiber eine weitere EU-Region in dieses Profil auf, so behandelt der Dienstleister dies **wie den Wechsel eines Unterauftragnehmers** und zeigt es dem Auftraggeber **mindestens 30 Tage vorher** in Textform an; Absatz 4 gilt entsprechend.

§ 5 Ort der Verarbeitung

(1) Die Verarbeitung der Inhalte des Auftraggebers erfolgt **ausschließlich in einem Rechenzentrum in Frankfurt am Main (Region eu-central-1)**. Alle Funktionen, die Inhalte des Auftraggebers verarbeiten, sind durch eine Berechtigungssperre auf diese Region begrenzt; ausgenommen sind Dienste ohne Regionsbindung und die gesondert gebuchte KI-gestützte Verdichtung nach Absatz 2 (Anlage 3, Schutzmaßnahmen). Diese Sperre ist an den Berechtigungen dieser Funktionen hinterlegt; aufheben kann sie nur, wer die Berechtigungen des Kontos verwaltet. Für die KI-gestützte Verdichtung (Absatz 2) gilt eine eigene Berechtigungssperre: Ihre Aufrufe sind auf die EU-Inferenzprofile in Mitgliedstaaten der Europäischen Union begrenzt. Der Dienstleister weist die wirksame Konfiguration auf Anforderung nach.

(2) **Ausnahme für die KI-gestützte Verdichtung.** Bucht der Auftraggeber die gesondert ausgewiesene KI-gestützte Verdichtung, so kann die zugehörige Berechnung innerhalb der **Europäischen Union** erfolgen; sie ist auf einen benannten Kreis von EU-Regionen begrenzt (Anlage 2; heutiger Stand sechs Regionen, eine Erweiterung wird nach § 4 Absatz 5 angezeigt). Für jeden solchen Aufruf weist der Dienstleister die **tatsächlich verwendete Region** protokollarisch aus. Außerhalb dieser gebuchten Ausnahme bleibt es bei Absatz 1; die in Absatz 3 gesondert benannten Vorgänge bleiben unberührt.

(3) **Die Inhalte verlassen die Europäische Union nicht.** Die Inhalte des Auftraggebers — die hochgeladenen Dateien, die daraus erzeugten Ergebnisse und die Auftragsberichte — werden durch den Dienstleister und durch die

in Anlage 2 als Auftragsverarbeiter benannten Personen **weder außerhalb der Europäischen Union verarbeitet noch außerhalb der Europäischen Union gespeichert**. Von diesem Satz **und von den Absätzen 1 und 2** zu unterscheiden und deshalb hier einzeln benannt sind die folgenden **sechs** Vorgänge; sie gehen den Absätzen 1 und 2 als besondere Regelung vor. Bei ihnen kann ein Bezug zu einem Staat außerhalb der Europäischen Union bestehen:

a) **Die gebuchte KI-gestützte Verdichtung.** Sie bleibt innerhalb der Europäischen Union und richtet sich allein nach Absatz 2; Satz 1 dieses Absatzes engt Absatz 2 nicht ein.

b) **Die Zahlungsabwicklung.** Lädt der Auftraggeber Guthaben auf, so übermittelt der Dienstleister an den in Anlage 2 Abschnitt 3 benannten Zahlungsdienstleister ausschließlich die pseudonyme Kennung des Kundenkontos, den Betrag, die Währung, die Zahl der gutzuschreibenden Einheiten und — wenn der Auftraggeber einen solchen einsetzt — einen Aktionscode. Seine Zahlungs- und Kontaktdaten gibt der Auftraggeber unmittelbar beim Zahlungsdienstleister ein. **Inhalte werden dabei nicht übermittelt.** Der Zahlungsdienstleister kann die bei ihm anfallenden Daten auch in den Vereinigten Staaten verarbeiten; die Grundlage dafür weist Anlage 2 aus.

c) **Verwaltung und Unterstützung beim Betreiber der Infrastruktur.** Verwaltungs-, Abrechnungs- und Unterstützungsvorgänge des in Anlage 2 Abschnitt 1 benannten Betreibers können einen Bezug zu anderen Staaten haben. Der Dienstleister übermittelt dem Betreiber zu solchen Zwecken **keine Inhalte** und nimmt keine Unterstützungsleistung in Anspruch, für die er Inhalte offenlegt. Eine Aussage darüber, welche Zugriffsmöglichkeiten der Betreiber als Betreiber der Infrastruktur technisch hat, trifft der Dienstleister nicht; hierzu Buchstabe f und Anlage 3.

d) **Vom Auftraggeber selbst bestimmte Ziele und Quellen.** Bucht der Auftraggeber eine Aufgabe, die fertige Ergebnisse an ein von ihm angegebenes Ziel ausliefert, eine Fertigmeldung an ein von ihm angegebenes System sendet oder Dateien von einer von ihm angegebenen Quelle abholt, so bestimmt **der Auftraggeber** dieses Ziel oder diese Quelle und damit deren Ort. Liegt ein solches Ziel außerhalb der Europäischen Union, so verlassen die dorthin ausgelieferten Inhalte auf seine Veranlassung die Europäische Union; für den Ort eines vom Auftraggeber bestimmten Ziels kann der Dienstleister nicht eintreten. Satz 1 dieses Absatzes betrifft die Verarbeitung durch den Dienstleister und die in Anlage 2 benannten Personen, nicht die vom Auftraggeber selbst veranlasste Auslieferung an ihn oder an einen von ihm benannten Empfänger.

e) **Die gebuchte Abfrage öffentlicher Drittdienste.** Auf Übermittlungen, die sich aus einer vom Auftraggeber ausdrücklich gebuchten Abfrage öffentlicher Drittdienste ergeben, weist Anlage 2 Abschnitt 4 gesondert hin. Übermittelt werden dabei die dort benannten Angaben, **nicht die Datei**.

f) **Erzwungener Zugriff aufgrund behördlicher Anordnung.** Der Betreiber der Infrastruktur gehört zu einem US-Konzernverbund. US-Recht kann ihn verpflichten, herausverlangte Daten offenzulegen, **auch wenn sie in der Europäischen Union gespeichert sind**. Dieses Restrisiko lässt sich vertraglich nicht beseitigen; der Dienstleister bestreitet es nicht, sondern begrenzt es durch den Verarbeitungsort, durch Zugriff nur nach dem Erforderlichkeitsprinzip und durch die Unterrichtung nach § 6. **Für einen so erzwungenen Zugriff gibt Satz 1 dieses Absatzes keine Zusage.**

§ 6 Behördliche Anfragen

(1) Erhält der Dienstleister eine behördliche Anordnung, die auf die Herausgabe oder Offenlegung von Inhalten des Auftraggebers gerichtet ist, so **unterrichtet** er den Auftraggeber hierüber, soweit ihm dies rechtlich erlaubt ist.

(2) Der Dienstleister führt über solche Anfragen einen internen Nachweis (Anzahl, Datum, Art, betroffenes Konto, Ausgang) und erteilt dem Auftraggeber hierüber **auf Anfrage Auskunft**. Eine Pflicht zur regelmäßigen Veröffentlichung übernimmt der Dienstleister nicht; eine freiwillige Veröffentlichung bleibt ihm unbenommen.

§ 7 Nachweise und Prüfrecht des Auftraggebers

(1) Der Dienstleister stellt dem Auftraggeber die Unterlagen zur Verfügung, die dieser für seine eigene Auswahl- und Sorgfaltsprüfung benötigt (insbesondere Anlage 3, Schutzmaßnahmen).

(2) **Prüfrecht.** Der Auftraggeber kann die Einhaltung dieser Vereinbarung überprüfen. Ohne besonderen Anlass ist eine Prüfung **höchstens einmal im Kalenderjahr** und nur nach **vorheriger Ankündigung** möglich. Der Nachweis erfolgt **vorrangig durch Vorlage von Unterlagen**. Eine Prüfung vor Ort findet nur bei einem **konkreten Anlass** statt. Der Aufwand des Dienstleisters wird nach Zeit vergütet.

- (3) **Kostentragung bei bestätigtem Verdacht.** Bestätigt sich bei einer anlassbezogenen Prüfung der Verdacht eines erheblichen Verstoßes, so trägt der Dienstleister die Kosten der Prüfung.
- (4) Das gesetzliche Kontrollrecht nach Art. 28 Abs. 3 lit. h DSGVO bleibt von den Beschränkungen dieses Paragraphen unberührt.
-

§ 8 Textform, Anlagen, Fassung

- (1) Diese Vereinbarung und ihre Anlagen sind in **Textform** nach § 126b BGB errichtet. Eine handschriftliche oder qualifizierte elektronische Signatur ist nicht erforderlich.
- (2) **Anlagen.** Bestandteil dieser Vereinbarung sind:

Anlage	Inhalt
Anlage 1	Leistungsbeschreibung
Anlage 2	Weitere mitwirkende Personen / Unterauftragnehmer
Anlage 3	Technische und organisatorische Schutzmaßnahmen
Anlage 4	Auftragsverarbeitungsvertrag nach Art. 28 DSGVO (bestehend)
Anlage 5	Wortlaute der maßgeblichen Vorschriften

- (3) **Fassung und Nachweis.** Diese Vereinbarung wird dem Auftraggeber als **ein PDF-Dokument** (Vereinbarung mit ihren Anlagen) ausgehändigt und mit seiner Zustimmung im Konto festgehalten. Festgehalten werden die **Fassungskennung** dieses Dokuments und eine **Prüfsumme** des ausgehändigten Textes; damit ist der genaue Inhalt unabhängig von der Kennung nachweisbar.
-

§ 9 Schluss- und Auslegungsbestimmungen

- (1) **Vorrang.** Diese Vereinbarung geht den Allgemeinen Geschäftsbedingungen des Dienstes vor. Sie kann **nicht** über die Änderungsklausel der Allgemeinen Geschäftsbedingungen geändert werden; eine Änderung bedarf einer erneuten Zustimmung des Auftraggebers in Textform.
- (2) **Auslegung im Zweifel gesetzesnah.** Die Klauseln dieser Vereinbarung sind so zu verstehen, wie es dem Wortlaut der in Anlage 5 abgedruckten Vorschriften am nächsten kommt.
- (3) **Fortgeltung des Gesetzes.** Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein, so bleibt die Vereinbarung im Übrigen wirksam. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung; die Verschwiegenheitspflicht nach § 203 StGB und den berufsrechtlichen Vorschriften bleibt in jedem Fall bestehen.
- (4) **Laufzeit.** Diese Vereinbarung gilt für die Dauer der Nutzung des Dienstes. Die Verschwiegenheitspflicht nach § 2 besteht über ihr Ende hinaus fort. Die Einzelheiten der Beendigung und des Fassungswechsels regelt § 10.
-

§ 10 Beendigung durch den Auftraggeber und Fassungswechsel

- (1) **Beendigung durch den Auftraggeber.** Der Auftraggeber kann diese Vereinbarung jederzeit in Textform beenden; eine E-Mail genügt. Ein Grund ist nicht erforderlich, eine Frist nicht einzuhalten.
- (2) **Was die Beendigung NICHT beendet.** Die Verschwiegenheitspflicht des Dienstleisters und der von ihm eingesetzten Personen nach § 2 gilt **zeitlich unbegrenzt fort** — auch nach dem Ende dieser Vereinbarung, auch nach dem Ende des Nutzungsverhältnisses und auch für alle Inhalte, die dem Dienstleister vorher zugänglich waren. Sie ist weder befristet noch kündbar. § 203 StGB und die berufsrechtlichen Vorschriften der Anlage 5 gelten unabhängig von dieser Vereinbarung; sie können durch ihre Beendigung nicht entfallen.
- (3) **Laufende Aufträge.** Bereits gestartete Aufträge werden abgewickelt und **nicht angehalten**. Für sie gilt die Verschwiegenheitspflicht nach Absatz 2 ohnehin fort; ein Abbruch würde dem Auftraggeber Ergebnisse und bereits abgebuchtes Guthaben entziehen, ohne irgendjemanden zu schützen. Die Abbruch- und Freigabemöglichkeiten des Auftraggebers aus dem Nutzungsverhältnis bleiben unberührt.
- (4) **Bereits gespeicherte Dateien.** Die Aufbewahrungs- und Löschrufen **ändern sich nicht**. Es bleibt bei der Aufbewahrung: fest 7 Tage ab Auftragsende (nicht wählbar) und bei den gesetzlichen Aufbewahrungspflichten. Die

Beendigung dieser Vereinbarung ist **keine** Kündigung des Nutzungsvertrags; wer auch das Konto beenden will, kündigt nach § 13 der Allgemeinen Geschäftsbedingungen — dann gelten der Übergangs- und der Abrufzeitraum nach § 14 jener Bedingungen.

(5) **Zugang.** Der Zugang zum Dienst **bleibt bestehen**. Die Beendigung führt weder zur Sperre des Kontos noch zum Ausschluss von Leistungen. Diese Vereinbarung ist ein Angebot des Dienstleisters, keine Voraussetzung der Nutzung.

(6) **Was der Auftraggeber verliert.** Für Aufträge nach der Beendigung kann er sich nicht mehr auf eine bestehende Verpflichtung in Textform im Sinne des § 203 Abs. 4 Satz 1 StGB berufen. Ob er den Dienst danach berufsrechtlich weiter einsetzen darf, beurteilt er selbst; der Dienstleister trifft dazu keine Aussage (§ 9 Absatz 2 gilt entsprechend).

(7) **Fassungswechsel.** Ändert der Dienstleister diese Vereinbarung, legt er dem Auftraggeber die neue Fassung vor und bittet um Zustimmung. **Bis zur Zustimmung gilt die zuletzt zugestimmte Fassung unverändert weiter** (§ 9 Absatz 1). Eine Zustimmungsfiktion findet nicht statt; Schweigen ist keine Zustimmung.

(8) **Wenn der Auftraggeber nicht zustimmt.** Dann bleibt es bei Absatz 7: Der Zugang bleibt bestehen, laufende Aufträge laufen weiter, Fristen ändern sich nicht, es entsteht kein Nachteil. Der Dienstleister hält im Konto fest, **welche Fassung vorgelegt und wie entschieden wurde** — die Vorlage und die Entscheidung sind belegbar, die frühere Zustimmung bleibt unverändert nachweisbar.

(9) **Wiederannahme.** Der Auftraggeber kann die Vereinbarung jederzeit erneut annehmen — auch Jahre später. Er erhält dann die dann geltende Fassung als Dokument. Frühere Zustimmungen bleiben im Konto einsehbar; sie werden nicht überschrieben.

Kein Rechtsrat. Dieses Dokument beschreibt Verpflichtungen des Dienstleisters und die maßgeblichen Vorschriften; die berufsrechtliche Bewertung des eigenen Vorgehens obliegt dem Auftraggeber.

Anlage 1 — Leistungsbeschreibung

zur **Verschwiegenheitsvereinbarung** (Fassung
schweigepflicht-hb-2026-11) **Stand:** 18. Oktober 2026

schweigepflicht-rb-2026-11 /

Warum die Leistungsbeschreibung eine Anlage ist. Sie ist bewusst als Anlage geführt, nicht in den Vertragstext gezogen. So wird ein späterer neuer Leistungsbestandteil — etwa eine zusätzliche KI-gestützte Aufgabe — zu einem **Anlagenwechsel** mit erneuter Zustimmung, und nicht zu einem neuen Vertrag mit allen Bestandskunden.

1. Gegenstand

Diese Anlage beschreibt, **welche Arten der Verarbeitung** unter die Verschwiegenheitsvereinbarung fallen. Sie beschreibt nicht die Preise und nicht die Bedienung; maßgeblich ist, welche Verarbeitung an Inhalten des Auftraggebers stattfindet.

2. Verarbeitungsarten

Der Dienstleister verarbeitet die vom Auftraggeber eingelieferten Dateien ausschließlich zur Erbringung der jeweils **gebuchten** Aufgabe. In Betracht kommen:

Verarbeitungsart	Was daran geschieht
Entgegennahme und Speicherung	Hochladen, verschlüsselte Speicherung, Bereitstellung des Ergebnisses, fristgebundene Löschung
Texterkennung aus Bild und PDF	Auslesen von Text, Tabellen und Formularfeldern, insbesondere Beträge, Steuersätze und Angaben auf Belegen
Erkennung personenbezogener Angaben	Auffinden von Namen, Anschriften, Bankverbindungen u. Ä. sowie Erkennung von Sprache und Währung
Bildererkennung zur Unkenntlichmachung	Auffinden von Gesichtern, Kennzeichen und Text in Bildern, damit sie geschwärzt werden können
Schwärzung / Pseudonymisierung	Unkenntlichmachung der gefundenen Stellen
Sprache-zu-Text (Transkription)	Umwandlung gesprochener Sprache in Text
Format- und Dokumentumwandlung	Umwandlung zwischen Datei- und Rechnungsformaten
Optionalen Abgleich mit einer öffentlichen Musikdatenbank	nur bei ausdrücklicher Buchung; siehe Anlage 2, gesonderter Hinweis

3. KI-gestützte Verdichtung (vorausgedacht, gebuchte Ausnahme)

Für eine gesondert zu buchende, KI-gestützte **Verdichtung** von Inhalten (Zusammenfassen, strukturiertes Aufbereiten) kommt ein Sprachmodell des Cloud-Betreibers zum Einsatz. Diese Aufgabe ist nur auf ausdrückliche Auswahl aktiv. Für sie gilt die Ortsregelung nach § 5 Absatz 2 der Vereinbarung (Berechnung innerhalb der EU, Nachweis der Region je Aufruf); die eingesetzten Modelle und der Regionenkreis sind in Anlage 2 benannt.

4. Was nicht stattfindet

- **Keine Zweckentfremdung:** keine Auswertung zu eigenen Zwecken, keine Zusammenführung mit anderen Beständen, keine Weitergabe zu Werbe- oder Analysezwecken.
- **Kein Training:** keine Nutzung der Inhalte zum Training oder zur Weiterentwicklung von KI-Modellen (§ 3 der Vereinbarung).
- **Keine Wiedererkennung von Personen:** Beim Schwärzen von Bildern wird ein Gesicht

gefunden, damit es unkenntlich gemacht werden kann; es wird **kein biometrisches Muster** gebildet, gespeichert oder mit anderen Personen verglichen.

5. Maschinell erzeugte Ergebnisse

Ergebnisse einer maschinellen Erkennung können falsch oder unvollständig sein. Bei den betroffenen Aufgaben nennt der Dienstleister zu ausgelesenen Werten einen Sicherheitswert (Hinweis nach Art. 50 der Verordnung (EU) 2024/1689). Der Auftraggeber prüft Ergebnisse vor der Weiterverwendung.

Anlage 2 — Weitere mitwirkende Personen (Unterauftragnehmer)

zur **Verschwiegenheitsvereinbarung** (Fassung schweigepflicht-rb-2026-11 / schweigepflicht-hb-2026-11) **Stand:** 18. Oktober 2026

Eine Liste, nicht drei. Der Kreis der mitwirkenden Personen ist identisch mit § 7 des Auftragsverarbeitungsvertrags (Anlage 4) und mit Abschnitt 9 der Datenschutzerklärung. Weicht künftig eine der drei Stellen ab, ist das ein Fehler, der zu schließen ist — nicht ein zweiter, eigenständiger Stand.

1. Direkte Auftragsverarbeiter (sehen Inhalte des Auftraggebers)

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage
Amazon Web Services EMEA SARL , 38 avenue John F. Kennedy, L-1855 Luxemburg	Betrieb und Speicherung: Rechen- und Speicherdienste, Datenbanken, Schlüsselverwaltung, Auslieferung der Seiten, Versand der System-E-Mails, Anmeldung und Verwaltung der Benutzerkonten (Amazon Cognito)	Region Frankfurt (eu-central-1), Deutschland	AWS Data Processing Addendum (Bestandteil des AWS-Kundenvertrags) nach Art. 28 DSGVO; für etwaige Drittlandübermittlungen Standardvertragsklauseln der EU-Kommission
Amazon Web Services EMEA SARL (dieselbe Gesellschaft, gesondert ausgewiesen)	KI-gestützte Erkennung, nur bei den dafür gebuchten Aufgaben: Amazon Textract (Belege/Formulare), Amazon Comprehend (Personenangaben, Sprache, Währung), Amazon Rekognition (Gesichter, Kennzeichen, Text in Bildern zur Unkenntlichmachung), Amazon Transcribe (Sprache zu Text)	Region Frankfurt (eu-central-1), Deutschland; Nutzung von Inhalten zur Weiterentwicklung dieser Dienste ist abbestellt („AI services opt-out“)	wie vorstehend, zusätzlich die besonderen Bedingungen des Anbieters für Dienste des maschinellen Lernens

Zur Verpflichtung in Textform. Für diese Ebene liefert der Betreiber eine Vertraulichkeitsverpflichtung in Textform durch eine benannte Partei (Amazon Web Services EMEA SARL) und deckt zugleich die Regionsbindung ab. § 43e Abs. 3 Satz 2 Nr. 3 BRAO verlangt für die Unterauftragnehmer-Ebene **keine Belehrung**, sondern eine Verschwiegenheitsbindung in Textform; diese liegt damit vor.

2. KI-gestützte Verarbeitung mit Sprachmodellen (nur bei den dafür gebuchten Aufgaben und Zusatzoptionen)

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage
Amazon Web Services EMEA SARL (Dienst „Amazon Bedrock“)	KI-gestützte Verdichtung (Zusammenfassen und strukturiertes Aufbereiten) sowie die Zusatzoptionen Nachprüfung und Volltext mittels Sprachmodellen, nur bei ausdrücklicher Buchung	Innerhalb der Europäischen Union , begrenzt auf die EU-Regionen des verwendeten Inferenzprofils — zum Stand dieser Fassung: Frankfurt, Stockholm, Mailand, Spanien (Aragón), Irland, Paris (sechs). Für jeden Aufruf wird die tatsächlich verwendete Region protokolliert. Eine Erweiterung dieses Kreises wird nach § 4 der Vereinbarung angezeigt.	wie Abschnitt 1; die Modelle werden innerhalb der AWS-Infrastruktur ausgeführt — der Modellanbieter erhält die Inhalte nicht

Eingesetzte Modellfamilien (innerhalb Amazon Bedrock): Anthropic Claude (u. a. Claude Sonnet und Claude Opus der jeweils aktuellen, in der EU verfügbaren Generation). Ein Wechsel **zwischen bereits hier benannten Modellen innerhalb desselben Dienstes** ist ein Wechsel zwischen benannten Beteiligten und keine anzeigepflichtige Hinzuziehung.

Rechtlicher Kernpunkt. Bei der Nutzung über Amazon Bedrock bleibt **Amazon Web Services EMEA SARL der Auftragsverarbeiter**. Das Modell wird in der AWS-Infrastruktur betrieben; der Modellhersteller ist auf diesem Weg **nicht** Empfänger der Inhalte. Es kommt daher **kein neuer Rechtsträger** als Unterauftragnehmer hinzu — es erweitern sich nur die Art der Verarbeitung (Sprachmodell statt reiner Erkennung) und der Verarbeitungsraum (Frankfurt -> benannte EU-Regionen). Beide sind hier benannt.

Zum Regionskreis. Der Kreis der sechs Regionen ergibt sich aus dem verwendeten EU-Inferenzprofil, das AWS bestimmt und erweitern kann. Die sechs Regionen sind deshalb der **heutige Stand**, nicht eine für die Vertragsdauer erzwungene Grenze. **Nimmt AWS eine weitere EU-Region in das verwendete Inferenzprofil auf, wird dies wie ein Wechsel eines Unterauftragnehmers behandelt und dem Auftraggeber nach § 4 der Vereinbarung mindestens 30 Tage vorher in Textform angezeigt**; dem Auftraggeber stehen das Widerspruchs- und Kündigungsrecht nach § 4 Absatz 4 zu. Zusätzlich weist das Protokoll je Aufruf die tatsächlich verwendete Region aus, sodass eine Änderung nicht verborgen bleibt.

Warum Anzeige statt harter Begrenzung. Eine erzwungene Begrenzung auf genau diese sechs Regionen ließe Aufrufe scheitern, sobald AWS das Profil erweitert. Die Anzeige nach § 4 hält die Zusage ehrlich. Der laufende Abgleich „sind es noch genau diese sechs?“ ist als Betriebsablauf geführt.

3. Zahlungsabwicklung (verarbeitet keine Dateiinhalte)

Unternehmen	Leistung	Ort	Grundlage
Stripe Payments Europe, Limited , 1 Grand Canal Street Lower, Dublin 2, Irland (mit Stripe, Inc., USA)	Zahlungsabwicklung beim Aufladen von Guthaben — ausschließlich Zahlungs- und Kontaktdaten des Auftraggebers, keine Inhalte hochgeladener Dateien	Irland; Verarbeitung auch in den USA möglich	Je nach Zweck eigene Verantwortlichkeit oder Auftragsverarbeitung nach der jeweils einschlägigen Stripe-Dokumentation; EU-US Data Privacy Framework sowie ergänzend Standardvertragsklauseln der EU-Kommission, soweit anwendbar

Der Eintrag dient der Vollständigkeit; Stripe berührt keine Mandats- oder Patientendaten.

4. Empfänger einer optionalen Abfrage (kein Auftragsverarbeiter)

Empfänger	Anlass	Ort	Grundlage
MetaBrainz Foundation Inc. , San Luis Obispo, Kalifornien, USA	Abgleich von Titel-, Interpreten- und Albumangaben gegen die öffentlichen Datenbanken MusicBrainz und Cover Art Archive — nur bei der ausdrücklich gebuchten Aufgabe „Audio-Metadaten abgleichen“. Übermittelt werden Suchbegriffe aus Dateiname und Metadaten, nicht die Datei selbst.	USA	Kein für diese Abfrage belegter Angemessenheitsmechanismus und keine Standardvertragsklauseln. Art. 49 DSGVO ist keine Grundlage für planmäßige oder wiederkehrende Übermittlungen. Bis zur dokumentierten Einzelfallprüfung dürfen keine personenbezogenen, Mandats- oder Patientendaten verwendet werden.

5. E-Mail-Postfächer für Anfragen an uns (verarbeitet keine hochgeladenen Dateien)

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Betrieb unserer E-Mail-Postfächer: Eingang und Ausgang der persönlich beantworteten E-Mails — keine Verarbeitung hochgeladener Dateien. Bitte senden Sie uns Mandats-, Patienten- und andere Berufsgeheimnisse nicht per E-Mail, sondern nur über die Plattform. Geschieht es dennoch, ist die IONOS SE insoweit weitere mitwirkende Person; sie hat sich in Ziffer 5.4 ihres Auftragsverarbeitungsvertrags (Version 1.4) zur Vertraulichkeit verpflichtet, ausdrücklich auch — in Kenntnis der Strafbarkeit — für Geheimnisse nach § 203 StGB.	Mitgliedstaat der EU bzw. des EWR (§ 4.3 des IONOS-AVV, Version 1.4); eine Übermittlung in Drittstaaten nur, soweit sie zur Erbringung der Leistung erforderlich ist	Auftragsverarbeitungsvertrag nach Art. 28 DSGVO, abgeschlossen am 26.09.2026

6. Öffentliche Unterauftragnehmerliste des Betreibers (Kette unterhalb von AWS)

Die von Amazon Web Services selbst eingesetzten Unterauftragnehmer veröffentlicht der Betreiber unter:

<https://aws.amazon.com/compliance/sub-processors/>

Der Betreiber aktualisiert diese Liste nach seinen Angaben **mindestens 30 Tage, bevor er einen neuen Unterauftragnehmer einsetzt** — dieselbe Frist, die der Dienstleister für seine eigenen direkten Dienstleister zusagt (§ 4 der Vereinbarung). Die Ketten greifen ineinander, ohne dass der Dienstleister eine Frist verspricht, die er nicht steuert.

Anlage 3 — Technische und organisatorische Schutzmaßnahmen

zur **Verschwiegenheitsvereinbarung** (Fassung schweigepflicht-rb-2026-11 / schweigepflicht-hb-2026-11) **Stand:** 18. Oktober 2026

1. Gegenstand und Zweck dieser Anlage

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, mit denen der Dienstleister die ihm anvertrauten Inhalte schützt. Sie ist so gefasst, dass ein Auftraggeber sie seiner **eigenen Auswahl- und Überwachungsprüfung** zugrunde legen kann (für Rechtsanwälte: § 43e Absatz 2 BRAO).

Maßgeblich ist der **tatsächliche** Zustand. Wo eine Maßnahme heute anders oder schwächer ausgeprägt ist als sie klingen könnte, steht das ausdrücklich dabei. Zugesichert wird nur, was unter „Prüfweg“ mit einem Beleg hinterlegt ist.

2. Verarbeitungsort

Die Verarbeitung der Inhalte findet in der Region **Frankfurt am Main (eu-central-1)** statt. Speicher, Datenbanken, Rechenfunktionen und Container der laufenden Bearbeitung liegen in dieser Region. Die Ausnahmen am Ende dieses Abschnitts sind abschließend. Es besteht **keine Spiegelung oder Replikation von Inhaltsdaten in eine andere Region**; eine früher im Leerlauf eingeschaltete Cross-Region-Replikation zweier Altbestände nach Irland (eu-west-1) wurde abgeschaltet und vollständig entfernt.

Für alle Funktionen, die Inhalte verarbeiten, ist diese Ortsbindung **technisch begrenzt**, nicht nur organisatorisch zugesagt: Eine Berechtigungssperre verweigert ihnen jeden Aufruf eines regionsgebundenen Dienstes, dessen Zielregion nicht eu-central-1 ist. Sie wirkt als Verbot und geht damit jeder gegenteiligen Berechtigung vor; aufheben kann sie nur, wer die Berechtigungen des Kontos verwaltet. Dienste ohne Regionsbindung und die KI-gestützte Verdichtung (Ausnahmen unten) erfasst sie nicht. Für die KI-gestützte Verdichtung begrenzt eine eigene Berechtigungssperre die Aufrufe auf die EU-Inferenzprofile in Mitgliedstaaten der Europäischen Union. Der Auftraggeber kann sich die wirksame Konfiguration vorlegen lassen.

Ausgenommen und offen benannt:

- **Auslieferungsnetz und Zertifikate** (CDN, DNS, Zertifikatsverwaltung) arbeiten naturgemäß global. Sie transportieren die Zugriffe, **verarbeiten aber keine Inhalte**.
- **KI-gestützte Verdichtung**, sofern gesondert gebucht: Sie läuft über den EU-Regionenkreis des Cloud-Betreibers, der in Anlage 2 benannt ist. Für sie gilt § 5 Absatz 2 der Vereinbarung, nicht die Frankfurt-Bindung dieses Abschnitts.
- **Abrechnungs- und Kostenauskünfte** des Cloud-Betreibers werden global bereitgestellt. Sie enthalten Verbrauchszahlen, **keine Inhalte**.

3. Verschlüsselung

Bei der Übertragung. Der Zugang ist ausschließlich über TLS erreichbar; unverschlüsselte Aufrufe werden auf die verschlüsselte Adresse umgeleitet. Mindestversion **TLS 1.2**.

Ehrlich abgegrenzt: Die Erzwingung wirkt am Zugangsweg (Auslieferungsnetz). Eine zusätzliche Bedingung, die auf Ebene der einzelnen Speicher jeden unverschlüsselten Zugriff verweigert, ist derzeit **nicht** gesetzt. Praktisch sind die Speicherzugriffe verschlüsselt, weil sowohl die Dienstschnittstellen als auch die ausgegebenen Einmal-Links ausschließlich über TLS laufen.

Bei der Speicherung. Alle Inhalte liegen verschlüsselt. Verwendet wird ein **eigens für diesen Dienst eingerichteter, verwalteter Schlüssel** (Customer Managed Key) in der Region Frankfurt (eu-central-1) — **nicht** der pauschale, kontoweite Standardschlüssel des Cloud-Betreibers. Der Datenspeicher ist auf diesen Schlüssel voreingestellt, und die verarbeitenden Bausteine (Voreingang, Umbenennung, Schwärzung, KI-Metadaten) geben ihn zusätzlich bei jedem Schreibvorgang ausdrücklich an, sodass keine Ablage still auf den Standardschlüssel zurückfällt.

Ehrlich abgegrenzt: Dieser Schlüssel ist ein Schlüssel **des Dienstleisters**, kein kundeneigener. Die Inhalte sind im Ruhezustand verschlüsselt und der Zugriff auf den Klartext hängt an diesem einen Schlüssel; der Auftraggeber hat jedoch **keine eigene Schlüsselhoheit** und kann den Zugriff nicht durch Entzug eines eigenen Schlüssels unterbinden. Vereinzelt Inhalte, die vor der Umstellung auf diesen Schlüssel abgelegt wurden, können noch mit dem früheren Standardschlüssel verschlüsselt sein.

4. Mandantentrennung

Die Inhalte verschiedener Auftraggeber werden getrennt gehalten. Jede Datei wird nach der festen Konvention

{bereich}/{auftraggeber}/{auftrag}/{dateiname}

abgelegt. Der Auftraggeber-Anteil des Schlüssels stammt aus dem geprüften Anmeldemerkmal des angemeldeten Kontos und wird **nicht** aus der Anfrage übernommen. Einmal-Links für Hochladen und Herunterladen werden auf **je einen konkreten Schlüssel** signiert und sind nicht auf fremde Schlüssel übertragbar.

In der Datenbank erfolgen kundenbezogene Abfragen über einen **Index auf die Kennung des Auftraggebers**. Bei den Rechnungsdatensätzen ist diese Kennung zugleich der Partitionsschlüssel der Tabelle.

Diese Trennung ist im **Rechtesystem der Infrastruktur technisch erzwungen**, nicht nur in der Anwendung angelegt. Jede Anfrage wird unter einer **auftraggebergebundenen Sitzung** ausgeführt: Die ausführende Funktion nimmt für die Dauer der Anfrage eine enge Rolle an, die das Auftraggebermerkmal aus dem geprüften Anmeldemerkmal trägt. Die Rechte dieser Rolle binden **jeden** Datenpfad an genau dieses Merkmal. Ein Zugriff auf die Daten eines **fremden** Auftraggebers endet dadurch in einem **ausdrücklichen Verbot** (explicit deny) — auch dann, wenn ein Fehler in der Anwendungslogik ihn versuchen würde. Die Trennung hat damit eine **zweite, von der Anwendung unabhängige Sperre** unter sich.

Ehrlich abgegrenzt: In der Datenbank bleibt die Zuordnung zum Auftraggeber Sache der Anwendung (Abfrage über den kundenbezogenen Index); die infrastrukturseitige Sperre wirkt auf der **Dateiablage**, dem Ort der eigentlichen Inhalte. Der Schlüssel der Speicherung lässt sich nicht auftraggeberweise fassen; die Trennung wirkt dort über den Objektzugriff: Wer das Objekt nicht lesen darf, kommt an den Klartext nicht heran.

5. Zugriffsprotokollierung

Verwaltende Zugriffe auf die Infrastruktur werden lückenlos aufgezeichnet. Die Aufzeichnung umfasst, **wer wann welche** Handlung vorgenommen hat, einschließlich der Zugriffe auf Rechte- und Anmeldeverwaltung.

Die Protokolle werden mit einer **Protokollvalidierung** abgelegt: Jede nachträgliche Veränderung an einer abgelegten Protokolldatei ist erkennbar. Die Ablage ist ein **eigener, vom Datenbereich getrennter Speicher**, öffentlich nicht erreichbar und versioniert. Für den Protokolldienst ist der Schreibzugriff ausdrücklich geöffnet; darüber hinaus werden Schreibrechte auf diesen Speicher nicht vergeben.

Ehrlich abgegrenzt: Die Öffnung für den Protokolldienst ist eine Erlaubnis, kein Verbot für alle anderen. Ein **zusätzliches** Verbot, das jeden anderen Schreibzugriff auf diese Ablage ausschließt, ist derzeit nicht gesetzt. Der Schutz gegen unbemerkte Veränderung ruht deshalb auf der Protokollvalidierung und der Versionierung, nicht auf einer Schreibsperre.

Damit ist die Frage „Wer bei Ihnen hat wann auf meine Daten zugegriffen?“ beantwortbar.

Umfang offen benannt: Aufgezeichnet werden **verwaltende** Ereignisse. Die einzelne Leseoperation auf ein einzelnes Dokument wird nicht gesondert protokolliert; für die Bearbeitung selbst tritt an ihre Stelle das Protokoll je Datei (Abschnitt 8).

6. Unveränderbare Beweisablage

Die dem Auftraggeber ausgehändigten Urkunden und die zugehörigen Zustimmungsprotokolle werden in einer gesonderten, **unveränderbaren** Ablage geführt. Sie ist im Modus **COMPLIANCE** für **zehn Jahre** schreibgeschützt. In diesem Modus kann ein abgelegter Nachweis vor Fristablauf **von niemandem** gelöscht oder überschrieben werden — auch nicht vom Betreiber selbst und auch nicht vom höchstberechtigten Konto.

Diese Ablage ist vom Bereich der Auftragsdaten **bewusst getrennt**: Für die Auftragsdaten gilt das Löschversprechen aus Abschnitt 7, für die Nachweise die Zehnjahresfrist. Zwei verschiedene Versprechen erfordern zwei verschiedene Speicher.

Ein zweiter schreibgeschützter Speicher besteht bereits. Für langlebige, steuerlich aufbewahrungspflichtige Belege ist ein Archiv mit derselben Zehnjahressperre eingerichtet und **in Betrieb**: Dort werden die **Rechnungen** über die erbrachten Leistungen abgelegt, die gesetzlich zehn Jahre aufzubewahren sind (§ 147 Abgabenordnung, § 14b Umsatzsteuergesetz). Jeder dort abgelegte Beleg ist für zehn Jahre **unveränderbar und nicht löschtbar** — auch nicht durch den Betreiber. **Mandatsinhalte des Auftraggebers werden in diesem Archiv nicht abgelegt**; für sie gilt das Löschversprechen aus Abschnitt 7. Würde ein Mandatsdokument dort abgelegt, wäre es zehn Jahre lang nicht löschtbar — auch nicht auf Verlangen des Auftraggebers; das setzt daher eine gesonderte Vereinbarung voraus und findet ohne sie nicht statt.

7. Löschkonzept

Auftragsdaten. Die Dateien eines Auftrags werden nach dessen Abschluss gelöscht. Aufbewahrung: **fest 7 Tage ab Auftragsende (nicht wählbar)**. Eine andere Frist ist nicht einstellbar. Gelöscht wird **vollständig einschließlich aller Vorgängerefassungen**.

Die Löschung nimmt bei entgeltlichen Aufträgen ein dafür bestimmtes **Alterungs-Modul** vor — bewusst nicht die pauschale Ablauf-Automatik des Speicherdienstes. Grund: Die Löschung soll kontrolliert, nachvollziehbar und protokolliert erfolgen und den Auftragsbezug prüfen, statt nur ein Alter zu messen. Für die Eingangszone gilt zusätzlich: Solange kein Auftragsende vermerkt ist, wird dort **nicht** gelöscht — ein nie abgeschlossener Auftrag darf nicht stillschweigend verschwinden.

Ausnahme kostenloser Test. Für Dateien aus dem unentgeltlichen Test gilt abweichend eine pauschale Automatik des Speicherdienstes: Sie werden in allen sechs Bereichen bereits nach **24 Stunden** entfernt, ohne Rücksicht auf ein Auftragsende. Das ist kürzer als die feste Frist von 7 Tagen und für den Nutzer günstiger; es ist hier genannt, weil die Aussage „nur das Alterungs-Modul löscht“ sonst zu weit ginge.

Diesem Löschversprechen unterliegen die Bereiche **Eingang, Erfolgreich, Viren, Defekt, Falsch geliefert und Systemfehler** sowie die Zwischenzone der Verarbeitungsketten.

Ehrlich abgegrenzt — dauerhaft gehaltene Bereiche. Nicht jeder Bereich unterliegt der Frist. Dauerhaft gehalten werden, bis der Auftraggeber sie selbst entfernt:

Bereich	Inhalt
Postfach	dauerhaft eingerichtete Eingänge des Auftraggebers
Konfiguration	Eigentum des Auftraggebers: Firmenlogo, Unterschriftsbild, Referenztabellen
Berichte	erzeugte Auswertungen

Diese Bereiche sind bewusst dauerhaft, weil ihr Inhalt nicht zu einem einzelnen Auftrag gehört. Sie sind hier genannt, damit das Löschversprechen nicht weiter verstanden wird als es reicht.

Daneben bestehen zwei rein betriebsinterne Zwischenbereiche ohne festgelegte Frist. Sie nehmen keine Kundendateien auf.

Vorschau-Trefferlisten. Wird eine Schwärzung als Vorschau angefordert, entsteht je Datei eine Liste der gefundenen personenbezogenen Fundstellen. Diese **Vorschau endet mit dem Abschluss des Auftrags** — positiv wie negativ; die Trefferliste wird dann entfernt und bleibt nicht liegen. Für Vorschauen, die weder abgeschlossen noch abgebrochen werden, greift ein zeitlicher Notausgang.

Nachweise. Zustimmungsurkunden und Zustimmungprotokolle werden **zehn Jahre** aufbewahrt (Abschnitt 6). Das ist **kein Widerspruch** zum Löschversprechen: Gelöscht werden die *Inhalte* des Auftraggebers; aufbewahrt wird der *Nachweis darüber, was vereinbart und zugestimmt wurde*. Der Nachweis enthält keine Mandatsinhalte.

Arbeitsbereiche. Interne Zwischenbereiche werden zusätzlich durch eine Ablauf-Automatik nach 7 bzw. 14 Tagen geräumt. Sie enthalten Zwischenstände, keine Endergebnisse.

8. Protokoll je Datei

Jede eingelieferte Datei durchläuft einen protokollierten Weg und endet in genau einem von **sechs benannten Zuständen**:

Zustand	Bedeutung
Eingang	eingeliefert, noch nicht abschließend bearbeitet
Erfolgreich	bearbeitet, Ergebnis bereitgestellt
Viren	Schadsoftware festgestellt, abgewiesen
Defekt	technisch nicht verwertbar
Falsch geliefert	nicht zur gebuchten Aufgabe passend
Systemfehler	Störung auf Seiten des Dienstleisters

Der Zustand ist je Datei nachvollziehbar; der Auftraggeber sieht ihn im Ergebnisbericht. Zur Wiedererkennung und zum Ausschluss doppelter Verarbeitung werden **Prüfsummen (SHA-256)** über den Dateiinhalt gebildet.

Gesondertes Schwärzungsprotokoll. Bei der Schwärzung entsteht neben der geschwärzten Datei ein **eigenes Protokoll**, das je Fundstelle Art und Behandlung festhält. Es ist durch eine **Hash-Kette** gesichert — jeder Eintrag trägt den Hashwert seines Vorgängers, sodass nachträgliches Entfernen oder Umstellen einzelner Einträge erkennbar wird — und enthält die Prüfsumme der erzeugten Ausgabedatei. Das Protokoll liegt neben dem Ergebnis unter derselben Auftraggeber- und Auftragskennung.

9. Zertifikate und Eigenschaften der Infrastruktur

Die genutzte Infrastruktur des Cloud-Betreibers ist nach den einschlägigen Normen zertifiziert und geprüft (unter anderem ISO/IEC 27001, SOC-Berichte, C5).

Ausdrücklich klargestellt: Dies sind die Zertifikate **des Cloud-Betreibers**, nicht des Dienstleisters. Sie sind hier als **Eigenschaft der eingesetzten Infrastruktur** genannt. Der Dienstleister führt sie **nicht** als eigene Zertifizierung und leitet aus ihnen keine eigene Zertifizierung ab. Eine eigene Zertifizierung des Dienstleisters besteht derzeit nicht.

10. Änderungen dieser Anlage

Diese Anlage beschreibt einen Zustand, keinen Plan. Ändert sich eine hier beschriebene Maßnahme wesentlich zum Nachteil des Auftraggebers, wird die Änderung nach den Regeln der Vereinbarung angezeigt. Verbesserungen werden erst aufgenommen, **wenn sie wirksam sind**.

Anlage 4 — Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO · Stand: 18. Oktober 2026 · Fassung av-vertrag-2026-11

In einfachen Worten

Wenn Sie Dateien hochladen, in denen Angaben zu Personen stehen, bleiben Sie derjenige, der über diese Daten bestimmt — wir arbeiten nur nach Ihrer Anweisung. Genau das muss nach europäischem Datenschutzrecht schriftlich vereinbart werden, und das leistet dieses Dokument. Es legt fest, was wir mit Ihren Daten tun dürfen und was nicht, wie wir sie schützen, wen wir dabei einsetzen und wann wir sie löschen. Sie brauchen dieses Dokument, wenn eine Aufsichtsbehörde, ein Prüfer oder ein Kunde von Ihnen nachweisen möchte, dass Ihre Dienstleister ordentlich eingebunden sind. Sie können es hier lesen, ausdrucken und zu Ihren Unterlagen nehmen.

§ 1 Parteien und Gegenstand

1. Dieser Vertrag wird geschlossen zwischen dem Kunden von TitanCore24 als **Verantwortlichem** (nachfolgend „Verantwortlicher“) und **Robin Knecht, Einzelunternehmen, handelnd unter dem Geschäftsnamen TitanCore24**, Ringstraße 25a, 61118 Bad Vilbel, Deutschland, als **Auftragsverarbeiter** (nachfolgend „Auftragsverarbeiter“).
2. Verantwortlicher ist, wer über Zwecke und Mittel der Verarbeitung entscheidet. Auftragsverarbeiter ist, wer personenbezogene Daten ausschließlich nach Weisung des Verantwortlichen verarbeitet, ohne selbst über die Zwecke zu bestimmen.
3. Der Vertrag konkretisiert die Pflichten aus Art. 28 DSGVO für die Verarbeitung, die der Auftragsverarbeiter im Rahmen des zwischen den Parteien bestehenden Nutzungsvertrags (Hauptvertrag, siehe Allgemeine Geschäftsbedingungen) durchführt.
4. Er gilt für alle personenbezogenen Daten, die der Verantwortliche im Rahmen der Nutzung des Dienstes hochlädt oder eingibt, sowie für die daraus erzeugten Ergebnisse.
5. Er gilt **nicht** für die Bestandsdaten des Kundenkontos, für Abrechnungs- und Zahlungsdaten und für die Server-Protokolldaten. Insoweit ist TitanCore24 selbst Verantwortlicher; Einzelheiten stehen in der Datenschutzerklärung.
6. Dieser Vertrag kommt mit der Nutzung des Dienstes zustande und bedarf keiner gesonderten Unterschrift. Der Vertragstext ist jederzeit auf dieser Seite abrufbar und erfüllt damit die Anforderung der Textform nach Art. 28 Abs. 9 DSGVO.

§ 2 Art, Zweck und Dauer der Verarbeitung

1. **Art der Verarbeitung.** Erheben durch Entgegennahme hochgeladener Dateien, Speichern, Auslesen, Umwandeln, Verändern, Schwärzen, Maskieren oder Pseudonymisieren, Ordnen, Zusammenführen, Bereitstellen zum Abruf, Löschen. Eine Anonymisierung wird nur dann so bezeichnet, wenn die Voraussetzungen der Anonymität für den konkreten Datenbestand geprüft und dokumentiert sind. Bei einzelnen vom Verantwortlichen ausgewählten Aufgaben tritt hinzu: **maschinelle Text-, Sprach-, Bild- und Entitätenerkennung sowie Sprachmodelle mit KI-gestützten Diensten** (Auslesen von Belegangaben, Umwandlung von Sprache in Text, Erkennen von Personenangaben und Gesichtern zum Zweck der Unkenntlichmachung, Zusammenfassen, Nachprüfen und Volltext) — die eingesetzten Dienste sind in § 7 einzeln benannt. Die Verarbeitung erfolgt ausschließlich automatisiert; eine inhaltliche Sichtung durch Menschen findet nicht statt.
2. **Zweck.** Durchführung genau derjenigen Aufgabe, die der Verantwortliche für den jeweiligen Auftrag im Dienst ausgewählt hat — zum Beispiel Umbenennen, Umwandeln in PDF- oder PDF/A-Dateien, Auslesen von Rechnungsangaben, Unkenntlichmachen personenbezogener Daten, Prüfen und Sortieren von Tabellen. Ein darüber hinausgehender eigener Zweck des Auftragsverarbeiters besteht nicht.
3. **Keine Zweckentfremdung.** Der Auftragsverarbeiter nutzt die Daten des Verantwortlichen insbesondere **nicht** für eigene Auswertungen, nicht für Werbung, nicht zur Erstellung von Profilen und nicht zum Training von Verfahren des maschinellen Lernens.

4. **Auch nicht durch den Unterauftragnehmer.** Für die in § 7 genannten KI-Dienste hat der Auftragsverarbeiter der Nutzung von KundInnenhalten zur Verbesserung und Weiterentwicklung dieser Dienste gegenüber dem Anbieter **ausdrücklich widersprochen** (Abbestellung auf Kontoebene, „AI services opt-out“). Damit werden Inhalte des Verantwortlichen weder zum Training verwendet noch zu diesem Zweck außerhalb der Verarbeitungsregion gespeichert.
5. **Ort der Verarbeitung.** Die Kernverarbeitung ist für Amazon Web Services, Region Frankfurt (eu-central-1), konfiguriert. Optionale KI-Dienste können nach ausgewiesener Freigabe innerhalb der EU verarbeitet werden. Drittlandbezüge und kundenseitig bestimmte Ziele oder Quellen sind in diesem Vertrag einzeln benannt; eine pauschale Zusage „ausschließlich Deutschland“ wird nicht abgegeben.
6. **Die erste planmäßige Ausnahme.** Wählt der Verantwortliche die Aufgabe *Audio-Metadaten abgleichen*, werden zum Abgleich Titel-, Interpreten- und Albumangaben sowie Angaben aus dem Dateinamen an die öffentliche Musikdatenbank **MusicBrainz** und das **Cover Art Archive** übermittelt (Betreiber: MetaBrainz Foundation Inc., Kalifornien, USA). Die Anfrage geht von unseren Servern aus; Ihre IP-Adresse wird dabei nicht übermittelt. Für die USA besteht insoweit kein für diese Abfrage dokumentierter Angemessenheitsmechanismus und keine Standardvertragsklauseln. Art. 49 DSGVO ist keine allgemeine Grundlage für planmäßige oder wiederkehrende Übermittlungen. Die Funktion ist deshalb für Suchbegriffe mit Personenbezug nicht freigegeben; eine ausdrückliche Auswahl allein beseitigt diesen Vorbehalt nicht.
7. **Die zweite planmäßige Ausnahme.** Bucht der Verantwortliche eine Aufgabe, die fertige Ergebnisse an ein von ihm angegebenes Ziel ausliefert, eine Fertigmeldung an ein von ihm angegebenes System sendet oder Dateien von einer von ihm angegebenen Quelle abholt, so bestimmt **der Verantwortliche** dieses Ziel oder diese Quelle und damit deren Ort. Liegt ein solches Ziel außerhalb der Europäischen Union, so verlassen die dorthin ausgelieferten Inhalte auf seine Veranlassung die Europäische Union; für den Ort eines vom Verantwortlichen bestimmten Ziels kann der Auftragsverarbeiter nicht eintreten. Diese Übermittlung ist eine **Weisung des Verantwortlichen** (Art. 28 Abs. 3 lit. a DSGVO); für ihre Zulässigkeit nach Art. 44 ff. DSGVO hat der Verantwortliche einzustehen. Anders als bei der ersten Ausnahme findet sie nicht bei einer einzelnen Aufgabe statt, sondern überall dort, wo ein Ziel oder eine Quelle angegeben werden kann.
8. **Dauer.** Der Vertrag beginnt mit dem Hauptvertrag und endet mit ihm. Für die einzelnen Datenbestände gilt:
- **Eingangsordner (1, 2 und 3):** hochgeladene, noch nicht in einen Auftrag übernommene Dateien werden **7 Tage nach dem ersten Hochladen** in den leeren Ordner automatisch und unwiderruflich gelöscht, einschließlich aller gespeicherten Fassungen. Der Verantwortliche erteilt diese Löschung als dauerhafte Weisung; er kann Dateien jederzeit vorher selbst löschen. Vorher erinnert der Auftragsverarbeiter per E-Mail an die im Konto hinterlegte Adresse; zwischen dem Versand der Erinnerung und der Löschung liegen mindestens etwa 23 Stunden. Die Löschung kann sich deshalb im Regelfall um bis zu rund 23 Stunden verschieben; verzögert sich der Versand der Erinnerung, verschiebt sie sich entsprechend. Ein Anspruch auf die Erinnerung besteht nicht; für die Löschung maßgeblich ist ihr Versand, nicht ihr Zugang. Dateien, deren Frist bei der Inbetriebnahme der automatischen Löschung bereits abgelaufen war, werden ohne vorherige Erinnerung gelöscht, auch wenn im Konto keine Adresse hinterlegt ist. Für alle übrigen Dateien gilt: Ist im Konto keine Adresse hinterlegt, wird nicht erinnert und werden die Dateien dann nicht automatisch gelöscht. Mit dem Start eines Auftrags werden die Dateien dem Eingangsordner entnommen und in den Auftrag übernommen (Entnahme).
 - **Ergebnisse und aussortierte Dateien (Ordner 02, 02b, 03, 04, 04b, 05) sowie in einen Auftrag übernommene Dateien:** automatische, unwiderrufliche Löschung nach **Auftragsende zuzüglich der festen Aufbewahrungsfrist von 7 Tagen** (nicht wählbar).
 - **Auftragsberichte (Ordner 01):** bleiben von der automatischen Löschung ausgenommen und können vom Verantwortlichen im Kundenbereich selbst gelöscht werden; gelöschte Berichte sind über das Konto des Verantwortlichen nicht wiederherstellbar. Nicht gelöschte Berichte bleiben bis zum Ende des Hauptvertrags erhalten; mit dem Ende des Hauptvertrags gilt § 11. Daten zur Menge und Abrechnung des Auftrags (Mengennachweis, Ereignisprotokoll mit Zeitstempel, Vermerk über die Löschung des Berichts) bewahrt der Auftragsverarbeiter getrennt vom Bericht auf; die Löschung des Berichts berührt sie nicht. Wird die CSV-Fassung eines Berichts abgerufen, legt der Auftragsverarbeiter zusätzlich eine Kopie im Ordner 02 ab. Die Frist beginnt mit der Ablage der Kopie, nicht mit dem Auftragsende; der erste Abruf der CSV-Fassung löst die Ablage aus. Die Kopie ist für eine automatische Entfernung 7 Tage nach ihrer Ablage vorgesehen und bis dahin abrufbar.
 - **Systeminterne Zwischenablagen:** 7 Tage, durchgesetzt über eine eigene automatische Löschregel auf der Speicherebene.
 - **Kundenarchiv:** Eine gesonderte langfristige oder unveränderbare Archivierungsleistung wird derzeit nicht angeboten.

§ 3 Art der Daten und Kategorien betroffener Personen

Welche personenbezogenen Daten verarbeitet werden, bestimmt allein der Verantwortliche durch die Auswahl der Dateien, die er hochlädt. Der Auftragsverarbeiter hat darauf keinen Einfluss. Die folgende Aufstellung ist deshalb bewusst offen formuliert und beschreibt, was typischerweise vorkommt.

Art der Daten	Typische Beispiele	Kategorien betroffener Personen
Stammdaten	Name, Anrede, Geburtsdatum, Kundennummer, Personalnummer	Kunden, Lieferanten und Interessenten des Verantwortlichen
Kontaktdaten	Anschrift, Telefonnummer, E-Mail-Adresse	Beschäftigte und Bewerber des Verantwortlichen
Vertrags- und Abrechnungsdaten	Rechnungen, Belege, Bestellnummern, Beträge, Bankverbindungen	Mandanten und deren Beschäftigte
Inhalte von Dokumenten	Schriftverkehr, Verträge, Formulare, Tabellen, gescannte Unterlagen	Sonstige in den Unterlagen genannte Personen
Bild-, Ton- und Videodaten	Fotos, Scans, Aufnahmen, in denen Personen erkennbar sind	Abgebildete oder aufgenommene Personen
Technische Begleitdaten der Dateien	Dateiname, Zeitstempel, Verfasserangaben in Dateieigenschaften	Ersteller und Bearbeiter der Dateien
Besondere Kategorien nach Art. 9 DSGVO	Nur, soweit der Verantwortliche solche Daten hochlädt — etwa Gesundheitsdaten in Bescheinigungen. Der Verantwortliche entscheidet und verantwortet dies allein.	Die jeweils betroffenen Personen

Der Verantwortliche prüft vor dem Hochladen, ob die Verarbeitung der jeweiligen Daten zulässig ist, und lädt keine Daten hoch, für die er keine Rechtsgrundlage hat.

Zum Erkennen von Gesichtern. Bei der Aufgabe „Personenbezogene Daten schwärzen“ werden in Bildern Gesichter und Kennzeichen *erkannt*, um sie unkenntlich zu machen. Es wird dabei kein biometrisches Muster gebildet, gespeichert oder mit anderen Personen abgeglichen; eine Wiedererkennung oder Identifizierung findet nicht statt. Nach dem gegenwärtigen Verständnis der Aufsichtsbehörden liegt darin keine Verarbeitung biometrischer Daten zum Zweck der eindeutigen Identifizierung im Sinne von Art. 9 Abs. 1 DSGVO. Die Verarbeitung bleibt eine gewöhnliche Verarbeitung personenbezogener Daten nach Art. 6 DSGVO im Auftrag des Verantwortlichen.

§ 4 Weisungsrecht des Verantwortlichen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Das gilt auch für eine Übermittlung in ein Drittland, es sei denn, der Auftragsverarbeiter ist dazu nach dem Recht der Union oder der Mitgliedstaaten verpflichtet; in diesem Fall teilt er dies dem Verantwortlichen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. **Form der Weisungen.** Die Auswahl der Aufgabe, die Konfiguration des Auftrags und die Auswahl der hochgeladenen Dateien im Dienst gelten als Weisung; sie werden im Auftragsprotokoll dokumentiert. Darüber hinausgehende Einzelweisungen erteilt der Verantwortliche in Textform an datenschutz@titancore24.de. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
3. **Weisungsberechtigte.** Weisungsberechtigt ist, wer auf Seiten des Verantwortlichen Zugang zum Kundenkonto hat oder von diesem in Textform benannt wurde. Der Verantwortliche hält diese Angaben aktuell.
4. **Hinweispflicht.** Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt, weist er den Verantwortlichen unverzüglich darauf hin. Er ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis der Verantwortliche sie bestätigt oder ändert.
5. Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, muss der Auftragsverarbeiter nur ausführen, wenn sich die Parteien über den Mehraufwand verständigt haben.

§ 5 Vertraulichkeit und Verpflichtung der eingesetzten Personen

1. Der Auftragsverarbeiter stellt sicher, dass sich alle Personen, die zur Verarbeitung der Daten befugt sind, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus.
2. TitanCore24 wird als Einzelunternehmen ohne Beschäftigte geführt. Zugriff hat derzeit ausschließlich der Inhaber Robin Knecht. Werden künftig Beschäftigte, freie Mitarbeiter oder Dienstleister eingesetzt, werden diese vor der

Aufnahme ihrer Tätigkeit in Textform auf die Vertraulichkeit verpflichtet und in den Grundzügen des Datenschutzrechts unterwiesen.

3. Der Auftragsverarbeiter sieht die Inhalte hochgeladener Dateien nicht ein. Ein Einblick erfolgt ausnahmsweise nur zur Behebung einer konkreten Störung und nur, wenn der Verantwortliche dies ausdrücklich verlangt; ein solcher Zugriff wird protokolliert.
4. Der Auftragsverarbeiter macht die Personen, die Zugriff haben, mit den für sie geltenden Bestimmungen dieses Vertrags vertraut.
5. **Was dieser Paragraph leistet — und was nicht.** Die Absätze 1 bis 4 erfüllen **Art. 28 Abs. 3 lit. b DSGVO**, also das Datenschutzrecht. Sie erfüllen **nicht** die Verschwiegenheitspflicht nach **§ 203 StGB** und den berufsrechtlichen Vorschriften (§ 43e BRAO, § 62a StBerG, § 26a BNotO, § 50a WPO). Unterliegt der Verantwortliche einer solchen Pflicht, ist dafür die gesonderte **Vereinbarung über die Verschwiegenheit mitwirkender Personen** zu schließen (Verweis im Hinweis unter diesem Paragraphen); dieser Vertrag ist ihre Anlage 4 und gilt neben ihr, nicht statt ihrer. Die Verpflichtung in Textform nach Absatz 2 bleibt davon unberührt — sie ist ein Baustein, nicht der Nachweis des Berufsrechts.

Diese Klausel erfüllt Art. 28 Abs. 3 lit. b DSGVO. Unterliegen Sie der Schweigepflicht nach § 203 StGB — als Rechtsanwältin, Steuerberater, Notarin, Wirtschaftsprüfer oder im Heilberuf —, verlangt Ihr Berufsrecht darüber hinaus eine eigene Verpflichtung in Textform samt Belehrung über die Strafbarkeit. Die stellen wir gesondert bereit: Der AVV allein genügt Berufsgeheimnisträgern nicht — warum.

§ 6 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die nachfolgenden Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragslaufzeit aufrecht. Aufgeführt sind ausschließlich Maßnahmen, die tatsächlich umgesetzt sind. Maßnahmen dürfen weiterentwickelt werden, solange das Schutzniveau nicht unterschritten wird.

Bereich	Umgesetzte Maßnahmen
Zutrittskontrolle Wer kommt räumlich an die Technik heran?	Es werden keine eigenen Server betrieben. Die Verarbeitung findet in den Rechenzentren von Amazon Web Services in Frankfurt statt; die gesondert gebuchte KI-gestützte Verdichtung kann innerhalb der Europäischen Union in einem benannten Kreis von EU-Regionen rechnen. Für den physischen Zutritt gelten die dortigen Maßnahmen des Unterauftragnehmers (unter anderem Vereinzelungsanlagen, Videoüberwachung, Berechtigungsnachweise); sie sind über dessen öffentlich zugängliche Prüfberichte belegt.
Zugangskontrolle Wer darf sich am System anmelden?	Zugang ausschließlich über persönliche Anmeldung mit individuellem Konto und Kennwort; Kennwörter werden nur verschlüsselt gespeichert. Verwaltungszugänge sind auf den Inhaber beschränkt und zusätzlich abgesichert. Alle Verbindungen laufen verschlüsselt über TLS. Zugangsdaten für kundenseitig bestimmte Gegenstellen dürfen nur als mandantenbezogene Secret-Referenz verarbeitet werden, nicht als Klartext in Browserzustand, Auftrag oder Protokoll. Erstellung, Rotation und Löschung dieses Secret-Lebenszyklus sind vor Freischaltung serverseitig zu verifizieren.
Zugriffskontrolle Wer darf welche Daten sehen und bearbeiten?	Berechtigungen nach dem Grundsatz der geringstmöglichen Rechte. Anwendungsseitig ist jedem Konto ausschließlich der eigene Datenbereich zugänglich. Gespeicherte Dateien und Datenbestände sind verschlüsselt abgelegt.
Weitergabekontrolle Wie sind Daten unterwegs geschützt?	Verschlüsselung bei jeder Übertragung (TLS). Download-Verweise auf Ergebnisse sind zeitlich befristet und an das jeweilige Konto gebunden. Eine Weitergabe an Dritte außerhalb der in § 7 genannten Unterauftragnehmer findet nicht statt — ausgenommen die Auslieferung an ein vom Verantwortlichen selbst angegebenes Ziel, die Fertigmeldung an ein von ihm angegebenes System und die Abholung von einer von ihm angegebenen Quelle. Ziel, System und Quelle bestimmt der Verantwortliche und damit auch deren Ort; für diesen Ort kann der Auftragsverarbeiter nicht eintreten. Eine Zustellung per E-Mail ist nicht Ende-zu-Ende verschlüsselt und darf für Berufsgeheimnisse oder besonders schutzbedürftige Daten erst nach einer dokumentierten serverseitigen Freigabe angeboten werden. Liegt ein solches Ziel außerhalb der Europäischen Union, so verlassen die dorthin ausgelieferten Inhalte auf Veranlassung des Verantwortlichen die Europäische Union. Datenträger werden nicht versandt.

Bereich	Umgesetzte Maßnahmen
Eingabekontrolle Lässt sich nachvollziehen, was geschehen ist?	Jede Verarbeitung wird je Datei protokolliert : Zeitpunkt, ausgewählte Aufgabe, Ergebnis und gegebenenfalls Fehlergrund. Der Verantwortliche kann die Protokolle zu seinen Aufträgen jederzeit im Kundenbereich einsehen. Anmeldungen und Verwaltungszugriffe werden ebenfalls protokolliert.
Auftragskontrolle Wird wirklich nur nach Weisung gearbeitet?	Verarbeitung ausschließlich nach der im Auftrag gewählten Aufgabe (§ 4). Unterauftragnehmer werden nur nach Maßgabe von § 7 und auf vertraglicher Grundlage nach Art. 28 DSGVO eingesetzt. Keine Nutzung der Daten für eigene Zwecke, keine Auswertung, kein Training von Verfahren des maschinellen Lernens.
Verfügbarkeitskontrolle Was schützt vor Verlust und Ausfall?	Betrieb auf einer mehrfach ausgelegten Infrastruktur des Unterauftragnehmers. Fehlerhaft verarbeitete Dateien werden getrennt abgelegt, damit sie nicht in Ergebnisbestände geraten. Arbeitsdaten werden nach Auftragsende zuzüglich der festen Aufbewahrungsfrist von 7 Tagen (nicht wählbar) zur Löschung vorgesehen (§ 11). Eine gesonderte langfristige oder unveränderbare Kundenarchivierung wird nicht angeboten. Der Dienst ist ausdrücklich kein Sicherungsdienst ; der Verantwortliche behält seine Originaldateien. Eine Wiederherstellung gelöschter Dateien ist nach Ablauf der Frist auch dem Auftragsverarbeiter nicht möglich.
Trennungskontrolle Bleiben Kunden voneinander getrennt?	Für jeden Kunden besteht ein eigener, logisch getrennter Datenbereich. Aufträge, Dateien, Ergebnisse und Protokolle sind diesem Bereich fest zugeordnet. Ein Zugriff über die Anwendung auf Bereiche anderer Kunden ist nicht vorgesehen. Test- und Produktivbetrieb sind getrennt; für Tests werden keine Echtdaten verwendet.

Hinweis zur Verschlüsselung: Sie schützt gegen unbefugten Zugriff auf Datenträger und Übertragungswege. Sie schließt technisch nicht aus, dass der Betreiber der Rechenzentren im Rahmen seiner Systeme auf Daten zugreifen könnte, da die Schlüsselverwaltung dort betrieben wird. Ein solcher Zugriff ist vertraglich untersagt.

§ 7 Unterauftragnehmer

1. Der Verantwortliche erteilt dem Auftragsverarbeiter die **allgemeine Genehmigung** zur Beauftragung weiterer Auftragsverarbeiter (Art. 28 Abs. 2 Satz 2 DSGVO) nach Maßgabe der folgenden Absätze.
2. Bei Vertragsschluss sind für die Verarbeitung nach diesem AVV folgende Unterauftragnehmer eingesetzt und genehmigt. Die Zahlungsabwicklung ist hiervon getrennt und in der Tabelle ausdrücklich als nicht Teil dieses AVV gekennzeichnet:

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage
1. Direkte Auftragsverarbeiter (sehen Inhalte des Auftraggebers)			
Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxemburg	Betrieb und Speicherung: Rechen- und Speicherdienste, Datenbanken, Schlüsselverwaltung, Auslieferung der Seiten, Versand der System-E-Mails, Anmeldung und Verwaltung der Benutzerkonten (Amazon Cognito)	Region Frankfurt (eu-central-1), Deutschland	AWS Data Processing Addendum (Bestandteil des AWS-Kundenvertrags) nach Art. 28 DSGVO; für etwaige Drittlandübermittlungen Standardvertragsklauseln der EU-Kommission
Amazon Web Services EMEA SARL (dieselbe Gesellschaft, gesondert ausgewiesen)	KI-gestützte Erkennung, nur bei den dafür gebuchten Aufgaben: Amazon Textract (Belege/Formulare), Amazon Comprehend (Personenangaben, Sprache, Währung), Amazon Rekognition (Gesichter, Kennzeichen, Text in Bildern zur Unkenntlichmachung), Amazon Transcribe (Sprache zu Text)	Region Frankfurt (eu-central-1), Deutschland; Nutzung von Inhalten zur Weiterentwicklung dieser Dienste ist abbestellt („AI services opt-out“)	wie vorstehend, zusätzlich die besonderen Bedingungen des Anbieters für Dienste des maschinellen Lernens
2. KI-gestützte Verarbeitung mit Sprachmodellen (nur bei den dafür gebuchten Aufgaben und Zusatzoptionen)			

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage
Amazon Web Services EMEA SARL (Dienst „Amazon Bedrock“)	KI-gestützte Verdichtung (Zusammenfassen und strukturiertes Aufbereiten) sowie die Zusatzoptionen Nachprüfung und Volltext mittels Sprachmodellen, nur bei ausdrücklicher Buchung	Innerhalb der Europäischen Union, begrenzt auf die EU-Regionen des verwendeten Inferenzprofils — zum Stand dieser Fassung: Frankfurt, Stockholm, Mailand, Spanien (Aragón), Irland, Paris (sechs). Für jeden Aufruf wird die tatsächlich verwendete Region protokolliert. Eine Erweiterung dieses Kreises wird nach § 4 der Vereinbarung angezeigt.	wie Abschnitt 1; die Modelle werden innerhalb der AWS-Infrastruktur ausgeführt — der Modellanbieter erhält die Inhalte nicht
3. Zahlungsabwicklung (nicht Teil dieses AVV; verarbeitet keine Dateiinhalte)			
Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Dublin 2, Irland (mit Stripe, Inc., USA)	Zahlungsabwicklung beim Aufladen von Guthaben — ausschließlich Zahlungs- und Kontaktdaten des Auftraggebers, keine Inhalte hochgeladener Dateien	Irland; Verarbeitung auch in den USA möglich	Zahlungsdienstleister mit zweckabhängiger eigener Verantwortlichkeit oder Auftragsverarbeitung nach der jeweils einschlägigen Stripe-Dokumentation; diese Zahlungsabwicklung ist nicht Teil der Verarbeitung nach diesem AVV. EU-US Data Privacy Framework sowie ergänzend Standardvertragsklauseln der EU-Kommission, soweit anwendbar
4. Empfänger einer optionalen Abfrage (kein Auftragsverarbeiter)			
MetaBrainz Foundation Inc., San Luis Obispo, Kalifornien, USA	Abgleich von Titel-, Interpreten- und Albumangaben gegen die öffentlichen Datenbanken MusicBrainz und Cover Art Archive — nur bei der ausdrücklich gebuchten Aufgabe „Audio-Metadaten abgleichen“. Übermittelt werden Suchbegriffe aus Dateiname und Metadaten, nicht die Datei selbst.	USA	Kein für diese Abfrage dokumentierter Angemessenheitsmechanismus und keine Standardvertragsklauseln. Art. 49 DSGVO trägt keine planmäßige oder wiederkehrende Übermittlung; bis zur dokumentierten Einzelfallprüfung nicht für personenbezogene, Mandats- oder Patientendaten freigegeben.
5. E-Mail-Postfächer für Anfragen an uns (verarbeitet keine hochgeladenen Dateien; bitte senden Sie uns personenbezogene Daten Dritter und Berufsgeheimnisse nicht per E-Mail — Datenschutzerklärung Abschnitt 13)			
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Betrieb unserer E-Mail-Postfächer: Eingang und Ausgang der persönlich beantworteten E-Mails — keine Verarbeitung hochgeladener Dateien	Mitgliedstaat der EU bzw. des EWR (§ 4.3 des IONOS-AVV, Version 1.4); eine Übermittlung in Drittstaaten nur, soweit sie zur Erbringung der Leistung erforderlich ist	Auftragsverarbeitungsvertrag nach Art. 28 DSGVO, abgeschlossen am 26.09.2026

Diese Liste ist mit **Anlage 2** der Vereinbarung über die Verschwiegenheit mitwirkender Personen und mit den Abschnitten 8 bis 11 der Datenschutzerklärung deckungsgleich. Weicht eine der drei Stellen ab, ist das ein Fehler, der zu schließen ist — und kein zweiter, eigenständiger Stand.

1. **Ergänzende Verweise zur Tabelle.** Die Abbestellung der Nutzung von Inhalten zur Weiterentwicklung der KI-Dienste (Gruppe 1, zweite Zeile) ist in § 2 Absatz 4 geregelt; Inhalte verlassen die Region auch zu diesem Zweck nicht. Die Abfrage der öffentlichen Musikdatenbanken (Gruppe 4) findet nur auf ausdrückliche Auswahl des Verantwortlichen statt (§ 2 Absatz 6). Die von der Amazon Web Services EMEA SARL ihrerseits eingesetzten Unterauftragnehmer veröffentlicht der Anbieter unter aws.amazon.com/compliance/sub-processors; er aktualisiert

diese Liste nach seinen Angaben mindestens 30 Tage, bevor er einen neuen Unterauftragnehmer einsetzt.

2. **Die zweite Gruppe wirkt nur bei Buchung.** Die KI-gestützte Verarbeitung mit Sprachmodellen wird nur wirksam, wenn Sie eine Aufgabe oder Zusatzoption buchen, die sie ausdrücklich verwendet. Ohne eine solche Buchung werden die Dienste dieser Gruppe nicht angesprochen.
3. Stripe verarbeitet keine Inhalte hochgeladener Dateien, sondern ausschließlich Zahlungs- und Kontaktdaten des Verantwortlichen selbst. Der Eintrag dient der Vollständigkeit.
4. Der Auftragsverarbeiter wählt Unterauftragnehmer sorgfältig aus und verpflichtet sie vertraglich auf Datenschutzpflichten, die den hier vereinbarten mindestens gleichwertig sind. Kommt ein Unterauftragnehmer seinen Pflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für dessen Verhalten wie für eigenes.
5. **Ankündigung von Änderungen.** Beabsichtigte Änderungen — die Hinzuziehung eines neuen oder der Austausch eines bestehenden Unterauftragnehmers — teilt der Auftragsverarbeiter dem Verantwortlichen **mindestens vier Wochen vorher** in Textform an die im Konto hinterlegte E-Mail-Adresse mit. Für Verantwortliche, die der Vereinbarung über die Verschwiegenheit mitwirkender Personen zugestimmt haben, gilt die dort zugesagte längere Frist von **mindestens 30 Tagen** (§ 4 Absatz 2 der Vereinbarung); dasselbe gilt, wenn der Anbieter den Kreis der EU-Regionen für die KI-gestützte Verdichtung erweitert (§ 4 Absatz 5 der Vereinbarung).
6. **Widerspruchsrecht.** Der Verantwortliche kann einer angekündigten Änderung binnen **vier Wochen** ab Zugang der Mitteilung aus einem datenschutzrechtlichen Grund in Textform widersprechen. Der Widerspruch ist zu begründen. Lässt sich die Leistung ohne den betreffenden Unterauftragnehmer nicht mit vertretbarem Aufwand erbringen, kann jede Partei den Hauptvertrag zum Zeitpunkt der geplanten Umstellung kündigen; ein etwaiges Restguthaben wird dabei wie bei jeder anderen Vertragsbeendigung nach § 13 der Allgemeinen Geschäftsbedingungen behandelt.
7. Nicht als Unterauftragsverhältnis gelten reine Nebenleistungen ohne Zugriff auf personenbezogene Daten des Verantwortlichen, etwa Telekommunikations- oder Reinigungsleistungen.

Für Berufsgeheimnisträger sind diese Unterauftragnehmer zugleich „weitere Personen“ im Sinne des Berufsrechts (etwa § 43e Abs. 3 Nr. 3 BRAO): Sie sind namentlich zu benennen und in Textform zu verpflichten — die allgemeine Genehmigung nach Absatz 1 genügt dafür nicht. Der AVV allein genügt Berufsgeheimnisträgern nicht — warum.

§ 8 Unterstützung bei Betroffenenrechten

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu erfüllen (Art. 28 Abs. 3 lit. e DSGVO).
2. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, beantwortet dieser den Antrag nicht selbst, sondern leitet ihn unverzüglich an den Verantwortlichen weiter und teilt der betroffenen Person mit, dass er dies getan hat.
3. Der Auftragsverarbeiter unterstützt den Verantwortlichen ferner bei der Einhaltung der Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei der Meldung von Datenschutzverletzungen und bei einer Datenschutz-Folgenabschätzung, jeweils unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.
4. Die Unterstützung erfolgt unentgeltlich, soweit sie sich auf die im Dienst ohnehin vorhandenen Funktionen und Auskünfte beschränkt. Für darüber hinausgehenden Aufwand, der nicht auf einem Fehlverhalten des Auftragsverarbeiters beruht, kann eine angemessene Vergütung verlangt werden; sie ist vorher abzustimmen.

§ 9 Meldung von Datenschutzverletzungen

1. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten **unverzüglich** nach Bekanntwerden (Art. 33 Abs. 2 DSGVO), in der Regel innerhalb von 24 Stunden. Eine Verletzung ist jeder Vorfall, der zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu Daten führt.
2. Die Meldung erfolgt in Textform an die im Konto hinterlegte E-Mail-Adresse und enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien, ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Gegenmaßnahmen sowie eine Kontaktstelle für Rückfragen.

3. Sind noch nicht alle Angaben verfügbar, meldet der Auftragsverarbeiter zunächst den bekannten Sachverhalt und liefert die weiteren Angaben unverzüglich nach.
4. Der Auftragsverarbeiter ergreift unverzüglich Maßnahmen zur Sicherung der Daten und zur Begrenzung nachteiliger Folgen und dokumentiert den Vorfall.
5. Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen obliegen dem Verantwortlichen. Der Auftragsverarbeiter nimmt solche Meldungen nicht ohne vorherige Abstimmung selbst vor.

§ 10 Nachweise und Kontrollrechte

1. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen (Art. 28 Abs. 3 lit. h DSGVO).
2. **Nachweis ohne Vor-Ort-Prüfung.** Der Nachweis kann geführt werden durch Selbstauskunft in Textform, durch Vorlage dieser Maßnahmenübersicht in der jeweils aktuellen Fassung, durch Beantwortung eines Fragebogens des Verantwortlichen sowie durch Vorlage der öffentlich zugänglichen Prüfberichte und Zertifikate der eingesetzten Unterauftragnehmer. Der Auftragsverarbeiter beantwortet solche Anfragen innerhalb von **30 Tagen**.
3. Eine Prüfung vor Ort ist nur erforderlich, wenn ein konkreter Anlass besteht und die Auskünfte nach Absatz 2 nicht ausreichen. Sie ist mit angemessener Vorlaufzeit von mindestens zwei Wochen anzukündigen, auf die üblichen Geschäftszeiten zu beschränken und so durchzuführen, dass der Betrieb nicht unangemessen gestört wird. Da keine eigenen Serverräume betrieben werden, bezieht sich eine solche Prüfung auf Organisation, Dokumentation und Konfiguration.
4. Prüfer dürfen keine Wettbewerber des Auftragsverarbeiters sein und sind zur Vertraulichkeit zu verpflichten.
5. Für Prüfungen, die über Absatz 2 hinausgehen und nicht durch ein Fehlverhalten des Auftragsverarbeiters veranlasst sind, kann eine angemessene Aufwandsentschädigung verlangt werden.
6. Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungen, die er im Auftrag durchführt (Art. 30 Abs. 2 DSGVO), und legt es dem Verantwortlichen und der Aufsichtsbehörde auf Verlangen vor.

§ 11 Löschung und Rückgabe nach Vertragsende

1. Bereits während der Vertragslaufzeit sind Ergebnisse, aussortierte Dateien und in einen Auftrag übernommene Dateien für eine Löschung **nach Auftragsende zuzüglich der festen Aufbewahrungsfrist von 7 Tagen** vorgesehen; die Frist ist nicht wählbar. Der Verantwortliche ist verpflichtet, Ergebnisse innerhalb dieser Frist abzurufen. Für die Eingangsordner gilt § 2 Absatz 8 (Löschung 7 Tage nach dem ersten Hochladen). Auftragsberichte sind von der automatischen Löschung ausgenommen (§ 2 Absatz 8).
2. Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter alle noch vorhandenen personenbezogenen Daten des Verantwortlichen, spätestens innerhalb von **30 Tagen**. Der Verantwortliche kann stattdessen die Rückgabe verlangen; das Verlangen ist vor Vertragsende in Textform zu stellen.
3. Von der Löschung ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht des Auftragsverarbeiters besteht. Diese Daten werden bis zum Ablauf der jeweiligen Frist aufbewahrt und in ihrer Verwendung auf den Aufbewahrungszweck beschränkt. Eine Kundenarchivierung wird nicht angeboten.
4. Der Auftragsverarbeiter bestätigt die Löschung auf Verlangen in Textform.
5. Die Löschung erstreckt sich auch auf Kopien bei Unterauftragnehmern nach Maßgabe der dort vereinbarten Fristen.

§ 12 Haftung und Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO. Im Verhältnis der Parteien untereinander gelten ergänzend die Haftungsregelungen des Hauptvertrags (§ 10 der Allgemeinen Geschäftsbedingungen). Zwingende gesetzliche Haftung bleibt unberührt.
2. Der Verantwortliche ist für die Zulässigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich. Er stellt sicher, dass er über eine Rechtsgrundlage verfügt und seine Informationspflichten erfüllt.
3. Änderungen dieses Vertrags bedürfen der Textform. Der Auftragsverarbeiter darf diesen Vertrag anpassen, wenn dies zur Anpassung an geänderte Rechtsvorschriften, an eine geänderte Aufsichtspraxis oder an eine Weiterentwicklung des Dienstes erforderlich ist und das Schutzniveau nicht sinkt; er kündigt solche Änderungen mindestens vier Wochen vorher in Textform an. § 7 Absatz 6 gilt für das Widerspruchsrecht entsprechend.

4. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags in datenschutzrechtlicher Hinsicht vor.
5. Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.
6. Es gilt deutsches Recht. Gegenüber Kaufleuten ist Gerichtsstand der Sitz des Auftragsverarbeiters; gegenüber Verbrauchern gelten die gesetzlichen Gerichtsstände.

§ 13 Dieses Dokument sichern

Dieser Vertrag gilt mit der Nutzung des Dienstes; eine gesonderte Unterschrift ist nach Art. 28 Abs. 9 DSGVO nicht erforderlich, weil Textform genügt. Für Ihre Unterlagen können Sie ihn hier sichern:

Wenn Sie ein von uns unterzeichnetes Exemplar benötigen — etwa für eine Prüfung oder für Ihre eigenen Kunden —, schreiben Sie an datenschutz@titancore24.de. Nennen Sie dabei bitte Ihren vollständigen Firmen- oder Namenseintrag und die Anschrift. Sie erhalten das gegengezeichnete Exemplar per E-Mail zurück.

Anlage 5 — Wortlaute der maßgeblichen Vorschriften

zur Verschwiegenheitsvereinbarung · Stand: 18. Oktober 2026

Warum diese Anlage besteht. Die Belehrung nach § 2 Absatz 3 der Vereinbarung ist erst vollständig, wenn der Wortlaut der Vorschriften beiliegt, auf die sie sich stützt. Diese Anlage druckt sie ab. (Anlage 4 ist der bestehende Auftragsverarbeitungsvertrag.)

Hinweis. Gesetzestexte sind amtliche Werke (§ 5 UrhG) und frei wiedergebbar, **ändern sich aber**. Die folgenden Fassungen wurden am **28.08.2026** Wort für Wort gegen die amtliche Quelle abgeglichen (www.gesetze-im-internet.de; für § 9 MBO-Ä gegen die (Muster-)Berufsordnung der Bundesärztekammer, Stand 18.06.2026). **Für die Heilberufe ist die jeweilige Landesberufsordnung maßgeblich**, nicht die Musterberufsordnung unmittelbar.

§ 203 StGB — Verletzung von Privatgeheimnissen (maßgebliche Absätze)

Absatz 1 stellt unter Strafe, dass die dort genannten Berufsgeheimnisträger — darunter Rechtsanwälte, Steuerberater, Notare, Wirtschaftsprüfer sowie Ärzte, Zahnärzte, Apotheker und Angehörige anderer Heilberufe — ein fremdes Geheimnis unbefugt offenbaren, das ihnen in dieser Eigenschaft anvertraut oder bekannt geworden ist.

Absatz 3 Satz 2 (Erlaubnis für mitwirkende Personen):

„Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.“

Absatz 4 (Strafbarkeit rund um die Verpflichtung mitwirkender Personen):

Satz 1: Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person bekannt geworden ist. — Strafraum wie Absatz 1: **Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.**

Satz 2: Ebenso wird bestraft, wer **Nr. 1** — als in Absatz 1 oder 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, deren er sich bedient, zur Geheimhaltung verpflichtet wurde; **Nr. 2** — als mitwirkende Person sich einer weiteren mitwirkenden Person bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

Zur Zuordnung (nicht Gesetzestext, sondern Lesehilfe): **Nr. 1** trifft den Auftraggeber (Kunde) hinsichtlich des Dienstleisters. **Nr. 2** trifft den Dienstleister hinsichtlich der weiteren mitwirkenden Person (AWS). Die Strafe droht **auch dann, wenn nie ein Geheimnis offenbart wurde** — schon das Unterlassen der Verpflichtung genügt.

§ 43e BRAO — Inanspruchnahme von Dienstleistungen (Rechtsanwälte)

Absatz 3 (die Checkliste für den Dienstleistervertrag):

„Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist

1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,
2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und
3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.“

Absatz 2 verpflichtet den Rechtsanwalt, den Dienstleister sorgfältig auszuwählen (Grundlage des Prüfrechts nach § 7 der Vereinbarung).

Absatz 4 (Auslandsschranke): Für Dienstleistungen, die im Ausland erbracht werden, gelten zusätzliche Anforderungen. Bei Verarbeitung in Frankfurt ist der Tatbestand nicht eröffnet; er kann eingreifen, sobald ein Fernzugriff aus Drittstaaten möglich wäre.

Absatz 5 (Einwilligung des Mandanten): Bei Dienstleistungen, die **unmittelbar einem einzelnen Mandat dienen**, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen nur eröffnen, wenn der Mandant eingewilligt hat. — Hierfür stellt der Dienstleister die **Muster-Einwilligung** bereit; ob sie im Einzelfall nötig ist, entscheidet der Auftraggeber.

§ 62a StBerG — Inanspruchnahme von Dienstleistungen (Steuerberater)

Parallel zu § 43e BRAO aufgebaut: **Textform, Belehrung über die strafrechtlichen Folgen, Beschränkung auf das Erforderliche, Verpflichtung weiterer Personen in Textform**. Ebenso eine Einwilligungsregelung für Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen.

Wortlaut (§ 62a StBerG — amtliche Fassung):

- (1) Steuerberater und Steuerbevollmächtigte dürfen Dienstleistern den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung zur Verschwiegenheit gemäß § 57 Absatz 1 bezieht, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Dienstleister ist eine andere Person oder Stelle, die vom Steuerberater oder vom Steuerbevollmächtigten im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird.
- (2) Steuerberater und Steuerbevollmächtigte sind verpflichtet, den Dienstleister sorgfältig auszuwählen. Die Zusammenarbeit muss unverzüglich beendet werden, wenn die Einhaltung der dem Dienstleister gemäß Absatz 3 zu machenden Vorgaben nicht gewährleistet ist.
- (3) Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist
1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,
 2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und
 3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.
- (4) Bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, darf der Steuerberater und der Steuerbevollmächtigte dem Dienstleister den Zugang zu fremden Geheimnissen unbeschadet der übrigen Voraussetzungen dieser Vorschrift nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet.
- (5) Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, darf der Steuerberater und der Steuerbevollmächtigte dem Dienstleister den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der Mandant darin eingewilligt hat.
- (6) Die Absätze 2 und 3 gelten auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung der in den Absätzen 2 und 3 genannten Anforderungen verzichtet hat.
- (7) Die Absätze 1 bis 6 gelten nicht, soweit Dienstleistungen auf Grund besonderer gesetzlicher Vorschriften in Anspruch genommen werden. Absatz 3 Satz 2 gilt nicht, soweit der Dienstleister hinsichtlich der zu erbringenden Dienstleistung gesetzlich zur Verschwiegenheit verpflichtet ist.
- (8) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

Quelle: www.gesetze-im-internet.de/stberg/_62a.html · abgerufen 28.08.2026.

§ 26a BNotO — Inanspruchnahme von Dienstleistungen (Notare)

Parallel aufgebaut. **Besonderheit: Absatz 1** erlaubt den Zugang „ohne Einwilligung der Beteiligten“; **Absatz 4** verlangt die Einwilligung jedoch wieder für Dienstleistungen, die unmittelbar einem einzelnen Amtsgeschäft dienen. Wer nur Absatz 1 liest, hält Notariate irrig für den leichtesten Fall.

Zusätzlich zu beachten (keine Norm, aber Maßstab): BNotK-Rundschreiben 1/2026 vom 02.02.2026 zur Cloud-Nutzung und Aktenführung.

Wortlaut (§ 26a BNotO — amtliche Fassung):

(1) Der Notar darf Dienstleistern ohne Einwilligung der Beteiligten den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung zur Verschwiegenheit gemäß § 18 bezieht, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Dienstleister ist eine andere Person oder Stelle, die vom Notar im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird.

(2) Der Notar ist verpflichtet, den Dienstleister sorgfältig auszuwählen. Die Zusammenarbeit muss unverzüglich beendet werden, wenn die Einhaltung der dem Dienstleister gemäß Absatz 3 zu machenden Vorgaben nicht gewährleistet ist.

(3) Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist

1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,
2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und
3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.

(4) Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Amtsgeschäft dienen, darf der Notar dem Dienstleister den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der Beteiligte darin eingewilligt hat.

(5) Die Absätze 2 und 3 gelten auch für den Fall der Inanspruchnahme von Dienstleistungen, in die die Beteiligten eingewilligt haben, sofern die Beteiligten nicht ausdrücklich auf die Einhaltung der in den Absätzen 2 und 3 genannten Anforderungen verzichtet haben.

(6) Absatz 3 gilt nicht in den Fällen, in denen der Dienstleister nach § 1 des Verpflichtungsgesetzes förmlich verpflichtet wurde. Absatz 3 Satz 2 gilt nicht, soweit der Dienstleister hinsichtlich der zu erbringenden Dienstleistung gesetzlich zur Verschwiegenheit verpflichtet ist.

(7) Andere Vorschriften, die für Notare die Inanspruchnahme von Dienstleistungen einschränken, sowie die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

Quelle: www.gesetze-im-internet.de/bnoto/_26a.html · abgerufen 28.08.2026.

§ 50a WPO — Inanspruchnahme von Dienstleistungen (Wirtschaftsprüfer)

Parallel zu § 43e BRAO aufgebaut: Textform, Belehrung, Beschränkung auf das Erforderliche, Verpflichtung weiterer Personen in Textform.

Wortlaut (§ 50a WPO — amtliche Fassung):

- (1) Der Wirtschaftsprüfer darf Dienstleistern den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung zur Verschwiegenheit gemäß § 43 bezieht, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Dienstleister ist eine andere Person oder Stelle, die vom Wirtschaftsprüfer im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird.
- (2) Der Wirtschaftsprüfer ist verpflichtet, den Dienstleister sorgfältig auszuwählen. Die Zusammenarbeit muss unverzüglich beendet werden, wenn die Einhaltung der dem Dienstleister gemäß Absatz 3 zu machenden Vorgaben nicht gewährleistet ist.
- (3) Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist
1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,
 2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und
 3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.
- (4) Bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, darf der Wirtschaftsprüfer dem Dienstleister den Zugang zu fremden Geheimnissen unbeschadet der übrigen Voraussetzungen dieser Vorschrift nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet.
- (5) Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, darf der Wirtschaftsprüfer dem Dienstleister den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der Mandant darin eingewilligt hat.
- (6) Die Absätze 2 und 3 gelten auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung der in den Absätzen 2 und 3 genannten Anforderungen verzichtet hat.
- (7) Die Absätze 1 bis 6 gelten nicht, soweit Dienstleistungen aufgrund besonderer gesetzlicher Vorschriften in Anspruch genommen werden. Absatz 3 Satz 2 gilt nicht, soweit der Dienstleister hinsichtlich der zu erbringenden Dienstleistung gesetzlich zur Verschwiegenheit verpflichtet ist.
- (8) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

Quelle: www.gesetze-im-internet.de/wipro/_50a.html · abgerufen 28.08.2026.

§ 9 MBO-Ä — Schweigepflicht (Heilberufe)

Maßgeblich ist die **Landesberufsordnung des jeweiligen Landes** (Satzung der zuständigen Ärztekammer); die **(Muster-)Berufsordnung (MBO-Ä)** gilt **nicht unmittelbar**, sondern als Vorlage. Ihr Wortlaut wird hier als Vorlage abgedruckt — der einschlägige Landestext **kann abweichen** (mehrere Landesberufsordnungen fassen etwa Absatz 2 und Absatz 4 anders als das Muster).

Wortlaut (§ 9 MBO-Ä — Vorlage, amtliche Fassung der Bundesärztekammer):

(1) Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist – auch über den Tod der Patientin oder des Patienten hinaus – zu schweigen. Dazu gehören auch schriftliche Mitteilungen der Patientin oder des Patienten, Aufzeichnungen über Patientinnen und Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

(2) Ärztinnen und Ärzte sind zur Offenbarung befugt, soweit sie von der Schweigepflicht entbunden worden sind oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. Soweit gesetzliche Vorschriften die Schweigepflicht der Ärztin oder des Arztes einschränken, soll die Ärztin oder der Arzt die Patientin oder den Patienten darüber unterrichten.

(3) Ärztinnen und Ärzte dürfen ihren Mitarbeiterinnen und Mitarbeitern sowie Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, Informationen über Patientinnen und Patienten zugänglich zu machen. Über die gesetzliche Pflicht zur Verschwiegenheit haben sie diese zu belehren und dies schriftlich festzuhalten.

(4) Gegenüber den Mitarbeiterinnen und Mitarbeitern von Dienstleistungsunternehmen sowie sonstigen Personen, die an der beruflichen Tätigkeit mitwirken, sind Ärztinnen und Ärzte zur Offenbarung befugt, soweit dies für die Inanspruchnahme der Tätigkeit der mitwirkenden Personen erforderlich ist. Ärztinnen und Ärzte haben dafür zu sorgen, dass die mitwirkenden Personen schriftlich zur Geheimhaltung verpflichtet werden. Diese Verpflichtung zur Geheimhaltung haben Ärztinnen und Ärzte vorzunehmen oder auf das von ihnen beauftragte Dienstleistungsunternehmen zu übertragen.

(5) Wenn mehrere Ärztinnen und Ärzte gleichzeitig oder nacheinander dieselbe Patientin oder denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis der Patientin oder des Patienten vorliegt oder anzunehmen ist.

Quelle: (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte — MBO-Ä 1997 i. d. F. der Bekanntmachung der Bundesärztekammer (Stand 18.06.2026), www.bundesaerztekammer.de · abgerufen 28.08.2026. **Maßgeblich bleibt die jeweilige Landesberufsordnung.**

Wichtig — Form. § 9 Abs. 4 verlangt, dass die mitwirkenden Personen **schriftlich** zur Geheimhaltung verpflichtet werden; diese Verpflichtung darf der Arzt auf das beauftragte Dienstleistungsunternehmen **übertragen** (Abs. 4 Satz 3). Dieses Dokument stellt sie — parallel zu § 43e BRAO — in **Textform** samt Belehrung bereit. § 9 kennt darüber hinaus keinen Belehrungs- oder Einwilligungskatalog wie § 43e Abs. 3/5 BRAO; beides übernimmt der Dienstleister freiwillig. **Maßgeblich bleibt die Landesberufsordnung:** verlangt diese für die Verpflichtung ausdrücklich **Schriftform**, sorgt der Arzt hierfür ergänzend selbst — die Textform-Verpflichtung ist dann die Grundlage, nicht der Ersatz.

§ 126b BGB — Textform

„Ist durch Gesetz Textform vorgeschrieben, so muss eine lesbare Erklärung, in der die Person des Erklärenden genannt ist, auf einem dauerhaften Datenträger abgegeben werden. Ein dauerhafter Datenträger ist jedes Medium, das

1. es dem Empfänger ermöglicht, eine auf dem Datenträger befindliche, an ihn persönlich gerichtete Erklärung so aufzubewahren oder zu speichern, dass sie ihm während eines für ihren Zweck angemessenen Zeitraums zugänglich ist, und
2. geeignet ist, die Erklärung unverändert wiederzugeben.“

Folge für dieses Dokument: Keine handschriftliche Unterschrift und keine qualifizierte elektronische Signatur nötig. Ein Häkchen (dokumentierte Zustimmung) plus das ausgehändigte PDF genügt der Textform.

Kein Rechtsrat. Diese Anlage gibt Vorschriften wieder; die verbindliche Fassung ergibt sich aus der jeweils gültigen amtlichen Quelle zum Zeitpunkt der Aushändigung.