Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)
Version 2.4 · Stand: Juli 2026

zwischen

der Einrichtung (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO)

Name der Einrichtung: _____

Straße, Hausnummer: _____

PLZ, Ort: _____

Vertreten durch: _____

— nachfolgend „Einrichtung“ —

und

Hendrik Berkensträter, BescheidRecht
Antoniusstraße 47, 49377 Vechta, Deutschland
E-Mail: kontakt@bescheidrecht.de

— nachfolgend „BescheidRecht“ oder „Auftragsverarbeiter“ —

Präambel

Diese Vereinbarung zur Auftragsverarbeitung (im Folgenden „AVV“) regelt die Verarbeitung personenbezogener Daten durch BescheidRecht im Auftrag der Einrichtung, die den Dienst BescheidRecht im Rahmen eines B2B-Abonnements nutzt. Sie ist Bestandteil des zwischen den Parteien geschlossenen Nutzungsvertrags und gilt für alle Tätigkeiten, bei denen Mitarbeitende der Einrichtung personenbezogene Daten von Klienten in die BescheidRecht-Plattform eingeben oder hochladen.

§ 1 — Vertragsgegenstand und Laufzeit

1.1 BescheidRecht verarbeitet im Auftrag der Einrichtung personenbezogene Daten im Rahmen der Bereitstellung der KI-gestützten Bescheidanalyse-Plattform.

1.2 Die Laufzeit dieser AVV entspricht der Laufzeit des zugrunde liegenden B2B-Nutzungsvertrags. Sie endet automatisch mit dessen Beendigung.

1.3 Pflichten, die über das Vertragsende hinausgehen (insbesondere Löschung oder Rückgabe von Daten), bleiben bis zu ihrer vollständigen Erfüllung bestehen.

§ 2 — Art, Zweck und Umfang der Verarbeitung

2.1 Art der Verarbeitung: Erheben, Speichern, Strukturieren, Auslesen, Abfragen, Pseudonymisieren, Analysieren, Löschen.

2.2 Zweck: Prüfung von Behördenbescheiden auf formale und inhaltliche Fehler mittels KI-gestützter Analyse; Generierung von Musterschreiben-Vorlagen; Verwaltung von Fristen; Bereitstellung einer Einrichtungs-Übersicht über Analysevorgänge.

2.3 Kategorien personenbezogener Daten: Name, Anschrift, Geburtsdatum, Aktenzeichen, Bescheiddaten, IBAN, Steuer-ID sowie sonstige im Bescheid enthaltene personenbezogene Angaben der Klienten; Mitarbeiterdaten der Einrichtung (E-Mail, Nutzungsstatistiken). Bescheide können besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO enthalten (insbesondere Gesundheitsdaten, z. B. bei Pflegegrad- oder Erwerbsminderungsbescheiden).

2.4 Kategorien betroffener Personen: Klienten der Einrichtung (Bescheidinhaber und ggf. Mitglieder ihrer Bedarfsgemeinschaft); Mitarbeitende der Einrichtung (Berater, Administratoren).

§ 3 — Weisungsgebundenheit

3.1 BescheidRecht verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung der Einrichtung, sofern nicht eine gesetzliche Pflicht eine andere Verarbeitung erfordert; in einem solchen Fall teilt BescheidRecht der Einrichtung diese Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

3.2 Die Nutzung der Plattform gemäß Nutzungsvertrag und Produktdokumentation gilt als dokumentierte Weisung.

3.3 BescheidRecht informiert die Einrichtung unverzüglich, wenn eine Weisung nach Einschätzung von BescheidRecht gegen die DSGVO oder andere Datenschutzvorschriften verstößt.

§ 4 — Pflichten von BescheidRecht (Auftragsverarbeiter)

BescheidRecht verpflichtet sich:

- personenbezogene Daten ausschließlich zum vereinbarten Zweck zu verarbeiten;
- geeignete technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DSGVO zu treffen und aufrechtzuerhalten (§ 6);
- sicherzustellen, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- die Einrichtung unverzüglich über Verletzungen des Schutzes personenbezogener Daten zu informieren (§ 9);
- die Einrichtung mit geeigneten Mitteln bei der Erfüllung von Betroffenenrechten (Art. 15–22 DSGVO) zu unterstützen;
- die Einrichtung bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldepflichten, Datenschutz-Folgenabschätzung) zu unterstützen;
- alle erforderlichen Informationen zum Nachweis der Einhaltung dieser AVV zur Verfügung zu stellen und Überprüfungen nach § 11 zu ermöglichen.

§ 5 — Pflichten der Einrichtung (Verantwortlicher)

Die Einrichtung verpflichtet sich:

- Klienten über die Datenverarbeitung durch BescheidRecht gemäß Art. 13/14 DSGVO zu informieren;
- nur Daten einzureichen, für deren Verarbeitung eine Rechtsgrundlage besteht;
- Zugangsdaten (Passwörter, Sitzungen) sicher zu verwahren und Zugänge ausscheidender Mitarbeitender zeitnah zu entfernen;
- Datenpannen im eigenen Einflussbereich unverzüglich zu melden;
- BescheidRecht über datenschutzrelevante Änderungen im Nutzungsumfang zu informieren.

§ 6 — Technische und organisatorische Maßnahmen (TOMs)

Pseudonymisierung: Vor der KI-Analyse werden personenbezogene Daten (Name, IBAN, Geburtsdatum, Adresse, Steuer-ID u. a.) automatisch durch Platzhalter ersetzt. KI-Anbieter erhalten keine Klardaten.

Verschlüsselung: Alle Datenübertragungen erfolgen TLS-verschlüsselt (TLS 1.2/1.3). Datenbankzugriffe erfolgen ausschließlich verschlüsselt.

Zugriffskontrolle: Authentifizierung mit gehashten Passwörtern (bcrypt). Row Level Security (RLS) auf Datenbankebene stellt sicher, dass Nutzer nur eigene Daten sehen; Mitglieder einer Einrichtung sehen nur Daten ihrer Einrichtung.

Schutz besonderer Kategorien (Art. 9 DSGVO): Gesundheits- und Sozialdaten aus Bescheiden (z. B. Diagnosen, Grad der Behinderung, Pflegegrad) werden ausschließlich nach ausdrücklicher, serverseitig erzwungener Einwilligung verarbeitet (Art. 9 Abs. 2 lit. a DSGVO) — ohne dokumentierten Einwilligungs-Nachweis lehnt das System die Analyse technisch ab. Zugriff auf Analyseergebnisse nur nach dem Need-to-know-Prinzip über Row Level Security; sicherheitsrelevante Aktionen (Datenexport, Löschung, Einwilligung) werden in einem manipulationsgeschützten Audit-Trail protokolliert. Eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) liegt vor und wird regelmäßig überprüft.

Datensparsamkeit: Hochgeladene Bescheid-Dokumente werden nach der Analyse nicht dauerhaft gespeichert. Die eingesetzten KI-Anbieter verwenden API-Daten nicht zum Training ihrer Modelle; eine technische Zwischenspeicherung erfolgt zeitlich begrenzt (max. 30 Tage) und ausschließlich pseudonymisiert.

Audit-Protokollierung: Analysevorgänge werden mit Zeitstempel und Nutzer-ID protokolliert. Kein Zugriff Unbefugter auf Protokolle.

Verfügbarkeit & Serverstandort Deutschland: Anwendung und Datenbank laufen auf dedizierten Servern der Hetzner Online GmbH in Deutschland. Die Datenbank ist selbst gehostet — kein ausländischer Datenbank-Dienstleister hat Zugriff auf die Daten.

Backups: Tägliche automatisierte Datenbank-Backups, verschlüsselt gespeichert (Verschlüsselung at rest), regelmäßig auf Wiederherstellbarkeit geprüft.

Incident-Response: Verletzungen des Datenschutzes werden gemäß § 9 unverzüglich an die Einrichtung gemeldet und dokumentiert.

§ 7 — Unterauftragnehmer

7.1 Die Einrichtung erteilt die allgemeine Genehmigung (Art. 28 Abs. 2 DSGVO) zur Beauftragung der folgenden Unterauftragnehmer:

Anbieter	Zweck	Sitz / Garantien
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server-Hosting (Anwendung und Datenbank, selbst gehostet)	Deutschland — AVV nach Art. 28 DSGVO
Anthropic Ireland, Limited 6th Floor, South Bank House, Barrow Street, Dublin 4, Irland	KI-Analyse (ausschließlich pseudonymisierte Daten)	Irland (EU); Verarbeitung in den USA — DPA + SCCs, kein Training mit API-Daten
OpenAI Ireland Ltd 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	Embeddings und technischer Analyse-Fallback (ausschließlich pseudonymisierte Daten)	Irland (EU); Verarbeitung in den USA — DPA + SCCs, kein Training mit API-Daten
Plus Five Five, Inc. (Resend) 2261 Market Street #5039, San Francisco, CA 94114, USA	E-Mail-Versand (Konto-Bestätigungen, Fristen-Erinnerungen)	USA — DPA + SCCs
Functional Software, Inc. (Sentry) 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Fehlerüberwachung und Stabilitätsmonitoring	USA — DPA + SCCs
Upstash, Inc. USA (Daten-Region EU/Frankfurt)	Rate-Limiting / Missbrauchsschutz (nur gehashte IP-Adressen, keine Klientendaten)	USA (Daten-Region EU/Frankfurt) — DPA + SCC
Qonto SA (vormals Olinda SAS) 18 rue de Navarin, 75009 Paris, Frankreich	Rechnungsstellung (Kontaktdaten der Einrichtung, keine Klientendaten)	Frankreich (EU) — DSGVO
AlphaAI Technologies Inc. (Tavily) 1350 Broadway, 24th Floor, New York, NY 10018, USA	Web-Recherche zu Rechtsfragen (nur Sach-Suchbegriffe, keine personenbezogenen Daten)	USA — DPA + SCCs

7.2 Drittlandübermittlung (Art. 44 ff. DSGVO): Soweit Unterauftragnehmer ihren Sitz außerhalb der EU/des EWR haben, erfolgt die Übermittlung auf Grundlage von EU-Standardvertragsklauseln (SCCs) bzw. eines Angemessenheitsbeschlusses (EU-US Data Privacy Framework, soweit zertifiziert). Bescheid-Inhalte werden an KI-Anbieter ausschließlich pseudonymisiert übermittelt — Klardaten der Klienten verlassen den Serverstandort Deutschland nicht.

7.3 BescheidRecht legt jedem Unterauftragnehmer per Vertrag dieselben Datenschutzpflichten auf, wie sie in dieser AVV festgelegt sind (Art. 28 Abs. 4 DSGVO), und haftet gegenüber der Einrichtung dafür, dass der Unterauftragnehmer diese Pflichten erfüllt. BescheidRecht informiert die Einrichtung über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragnehmers mit einer Frist von 30 Tagen vorab. Die Einrichtung kann aus datenschutzbezogenen Gründen Einspruch erheben; kann einem berechtigten Einspruch nicht abgeholfen werden, steht der Einrichtung ein Sonderkündigungsrecht hinsichtlich der betroffenen Leistung zu.

§ 8 — Betroffenenrechte

8.1 BescheidRecht unterstützt die Einrichtung mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch gem. Art. 15–22 DSGVO).

8.2 Anfragen betroffener Personen, die direkt an BescheidRecht gerichtet werden, leitet BescheidRecht unverzüglich an die zuständige Einrichtung weiter.

8.3 Die Einrichtung bleibt Verantwortlicher im Sinne der DSGVO und ist für die Beantwortung von Betroffenenanfragen zuständig.

§ 9 — Meldung von Datenschutzverletzungen

9.1 BescheidRecht benachrichtigt die Einrichtung unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, damit die Einrichtung ihre Meldepflicht nach Art. 33 DSGVO (72-Stunden-Frist gegenüber der Aufsichtsbehörde) erfüllen kann.

9.2 Die Benachrichtigung enthält mindestens: Art der Verletzung, betroffene Datenkategorien und ungefähre Zahl der Betroffenen, voraussichtliche Folgen und ergriffene bzw. vorgeschlagene Abhilfemaßnahmen.

9.3 Meldepflichten gegenüber Aufsichtsbehörden und betroffenen Personen verbleiben bei der Einrichtung als Verantwortlichem.

§ 10 — Löschung und Rückgabe von Daten

10.1 Nach Beendigung des Nutzungsvertrags löscht BescheidRecht — nach Wahl der Einrichtung — alle personenbezogenen Daten der Einrichtung und ihrer Klienten innerhalb von 30 Tagen oder gibt sie zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

10.2 Auf Wunsch werden Daten vor der Löschung in einem maschinenlesbaren Format (JSON/CSV) exportiert. Der Exportantrag ist vor Vertragsende zu stellen.

10.3 Hochgeladene Bescheid-Dokumente werden unmittelbar nach der Analyse gelöscht und nicht dauerhaft gespeichert.

§ 11 — Kontrollrechte der Einrichtung

11.1 Die Einrichtung ist berechtigt, die Einhaltung dieser AVV zu überprüfen. Dazu kann sie Auskünfte und Nachweise in Textform anfordern, anerkannte Prüfberichte oder Zertifikate anfordern sowie mit angemessener Vorankündigung (14 Tage) Inspektionen durchführen oder durch beauftragte Dritte durchführen lassen.

11.2 Die Einrichtung trägt die Kosten derartiger Kontrollen, es sei denn, die Kontrolle deckt erhebliche Verstöße von BescheidRecht auf.

§ 12 — Haftung

12.1 Die Haftung der Parteien für Datenschutzverstöße richtet sich nach Art. 82 DSGVO.

12.2 Im Innenverhältnis haftet jede Partei für den Teil des Schadens, der durch ihren Verantwortungsbeitrag entstanden ist (Art. 82 Abs. 5 DSGVO). Eine Partei ist von der Haftung befreit, wenn sie nachweist, dass sie für den schadensauslösenden Umstand in keinerlei Hinsicht verantwortlich ist.

12.3 Im Übrigen gelten die Haftungsregelungen des zugrunde liegenden Nutzungsvertrags.

§ 13 — Schlussbestimmungen

13.1 Diese AVV unterliegt deutschem Recht.

13.2 Gerichtsstand ist Vechta (Niedersachsen), soweit gesetzlich zulässig.

13.3 Änderungen dieser AVV bedürfen der Textform (E-Mail genügt). BescheidRecht informiert über wesentliche Änderungen mit 30 Tagen Vorlauf.

13.4 Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Bei Widersprüchen zwischen dieser AVV und dem Nutzungsvertrag gehen die Regelungen dieser AVV in Datenschutzfragen vor.

Unterschriften

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Für die Einrichtung (Verantwortlicher) Name in Druckbuchstaben, Unterschrift	Hendrik Berkensträter, BescheidRecht (Auftragsverarbeiter)