

Auftragsverarbeitungsvertrag (AVV)

zwischen

_____ (Name und Anschrift der Organisation) – nachfolgend „Auftraggeber“ –

und

Nils Walter Heinrich Lappenbusch, Einzelunternehmen (Marke „DokAudit“), Baumackerstrasse 11, 8107 Buchs ZH, Schweiz – nachfolgend „Auftragnehmer“ –

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO, Fassung 2026-09. Der Auftragnehmer hat diesen Vertrag vorab unterzeichnet; er kommt mit der Unterzeichnung durch den Auftraggeber zustande.

§ 1 Gegenstand und Dauer

1. Der Auftragnehmer betreibt die Plattform DokAudit (dokaudit.de) zur Prüfung und Reparatur der Barrierefreiheit von PDF-Dokumenten. Der Auftraggeber nutzt diese Leistung auf Grundlage des Nutzungs- bzw. Testzugangs. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers.
2. Der Vertrag gilt ab Unterzeichnung durch den Auftraggeber und endet mit der Beendigung der Hauptleistung, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten zu Löschung und Vertraulichkeit gelten darüber hinaus.

§ 2 Art, Zweck, Daten und Betroffene

1. **Art der Verarbeitung:** Hochladen, Speichern, automatisierte Analyse und Reparatur von PDF-Dokumenten, Erzeugung von Prüfberichten, Betrieb der Benutzerkonten.
2. **Zweck:** Prüfung und Herstellung der Barrierefreiheit der vom Auftraggeber hochgeladenen Dokumente.
3. **Datenkategorien:** Kontaktdaten der Nutzer (Name, dienstliche E-Mail-Adresse, Organisation), Protokoll- und Nutzungsdaten (Anmeldezeitpunkte, IP-Adressen) sowie personenbezogene Inhalte, die in hochgeladenen Dokumenten enthalten sein können (z. B. Namen, Adressen, Angaben in Bescheiden oder Protokollen).
4. **Betroffene:** Mitarbeitende des Auftraggebers als Nutzer sowie Personen, deren Daten in den Dokumenten vorkommen (Bürgerinnen und Bürger, Ratsmitglieder, Beschäftigte).
5. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sollen nicht hochgeladen werden, es sei denn, dies wurde vorab in Textform vereinbart.

§ 3 Weisungen

1. Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO). Die Weisungen ergeben sich aus diesem Vertrag und der Nutzung der Plattform.
2. Einzelweisungen erteilt der Auftraggeber in Textform. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich und darf die Ausführung bis zur Klärung aussetzen.
3. Eine Verarbeitung zu eigenen Zwecken, insbesondere das Training von KI-Modellen mit Dokumenten des Auftraggebers, findet nicht statt.

§ 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer setzt die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen um und hält sie aufrecht (Art. 32 DSGVO). Er darf sie weiterentwickeln, sofern das Schutzniveau nicht sinkt.
2. Er unterstützt den Auftraggeber bei den Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenpannen, Datenschutz-Folgenabschätzung, Konsultation der Aufsichtsbehörde).
3. Der Auftragnehmer führt ein Verzeichnis aller Verarbeitungstätigkeiten im Auftrag (Art. 30 Abs. 2 DSGVO).
4. Ansprechperson für den Datenschutz beim Auftragnehmer: Nils Lappenbusch, kontakt@dokaudit.de.

§ 5 Vertraulichkeit

Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind und mit den Datenschutzvorschriften vertraut gemacht wurden. Diese Pflicht besteht nach Vertragsende fort.

§ 6 Unterauftragsverarbeiter

1. Der Auftraggeber stimmt dem Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter zu (allgemeine schriftliche Genehmigung, Art. 28 Abs. 2 DSGVO).
2. Änderungen (Hinzuziehung oder Ersetzung) teilt der Auftragnehmer mindestens 30 Tage vorher in Textform mit. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen; kommt keine Einigung zustande, hat jede Seite ein Sonderkündigungsrecht.
3. Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter auf dieselben Datenschutzpflichten wie in diesem Vertrag und haftet für dessen Pflichtverletzungen gegenüber dem Auftraggeber.
4. Der Auftragnehmer hat seinen Sitz in der Schweiz, für die der Angemessenheitsbeschluss der EU-Kommission gilt (Art. 45 DSGVO). Eine über Anlage 2 hinausgehende Verarbeitung außerhalb der EU, der Schweiz und des EWR erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

§ 7 Rechte der Betroffenen

Anfragen Betroffener leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst. Er unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei den Betroffenenrechten nach Kapitel III DSGVO.

§ 8 Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden, mit den Angaben, die der Auftraggeber für seine Meldung nach Art. 33 DSGVO braucht.

§ 9 Kontrollrechte

Der Auftragnehmer stellt alle Informationen zum Nachweis der Einhaltung dieses Vertrags bereit und ermöglicht Überprüfungen einschließlich Inspektionen (Art. 28 Abs. 3 lit. h DSGVO). Vor-Ort-Kontrollen sind mindestens 14 Tage vorher anzumelden und finden während der üblichen Geschäftszeiten statt.

§ 10 Rückgabe und Löschung

1. Nach Beendigung der Leistung löscht der Auftragnehmer alle Dokumente, Analyseergebnisse und Nutzerdaten des Auftraggebers oder gibt sie auf Wunsch zurück, spätestens 30 Tage nach Vertragsende. Die Löschung wird auf Anfrage bestätigt.
2. Dokumente der Einzelprüfung werden nach 7 Tagen automatisch gelöscht. Dokumente im Hub bleiben, bis der Auftraggeber sie löscht oder die von ihm eingestellte Aufbewahrungsfrist endet.
3. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

§ 11 Haftung

Für die Haftung gelten Art. 82 DSGVO und die Regelungen der Hauptleistung.

§ 12 Schlussbestimmungen

1. Änderungen und Ergänzungen bedürfen der Textform.
2. Bei Widersprüchen geht dieser Vertrag den übrigen Vereinbarungen im Hinblick auf den Datenschutz vor.
3. Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, der Sitz des Auftraggebers.
4. Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Bereich	Maßnahme
Zutritt	Betrieb im Rechenzentrum des Hosters (Deutschland); kein physischer Zugang für den Auftragnehmer
Zugang	Persönliches Konto, Passwort-Hashing, zeitlich begrenzte Zugangscodes und Anmeldelinks, Begrenzung von Anmeldeversuchen, Administrationszugang nur für den Auftragnehmer
Zugriff	Mandantentrennung: Nutzer sehen nur Dokumente ihrer Organisation; Rollen (Administrator, Nutzer)
Weitergabe	Verschlüsselte Übertragung (TLS) für Web und E-Mail-Versand
Eingabe	Protokollierung von Anmeldungen und Administrationsaktionen (Audit-Protokoll)
Verfügbarkeit	Regelmäßige Datensicherung
Trennung	Getrennte Datenhaltung je Organisation; keine Nutzung der Dokumente für KI-Training
Datenminimierung	Automatische Löschung der Einzelprüfung nach 7 Tagen; einstellbare Aufbewahrung im Hub; KI-Nutzung im Hub durch Administratoren abschaltbar
Organisation	Verpflichtung auf Vertraulichkeit, Vorgehen bei Vorfällen, regelmäßige Überprüfung dieser Maßnahmen

Anlage 2 – Unterauftragsverarbeiter

Unternehmen	Leistung	Verarbeitungsort
Hetzner Online GmbH, Gunzenhausen	Hosting der Anwendung und Datenspeicherung	Deutschland
Anthropic PBC (Claude-API)	KI-gestützte Analyse einzelner Dokumentinhalte (Alternativtexte, Strukturerkennung), nur soweit die KI-Funktion genutzt wird. Keine Nutzung zum Modelltraining. Auf Wunsch Verarbeitung mit einem KI-Anbieter in der EU.	USA (Drittland, Art. 44 ff. DSGVO)

Systemmails (Anmeldelinks, Zugangscodes) versendet der Auftragnehmer über einen eigenen Mailserver; ein weiterer Unterauftragsverarbeiter wird dafür nicht eingesetzt.

Auftraggeber – Ort, Datum, Name, Funktion,
Unterschrift



Auftragnehmer – Nils Lappenbusch, Buchs ZH,
06.10.2026