Auftragsverarbeitungsvertrag (AVV)

Stand: 26. Oktober 2025

zwischen

visuax UG (haftungsbeschränkt), Backhausstraße 2, 64395 Brensbach, Deutschland

(nachfolgend „**Auftragsverarbeiter**“ oder „**wir**“)

und

dem Kunden (gemäß Registrierung auf der Plattform „{ keep it developed }“)

(nachfolgend „**Verantwortlicher**“ oder „**Kunde**“)

(Auftragsverarbeitungsvertrag und Verantwortlicher gemeinsam „**Parteien**“)

Präambel

Dieser Auftragsverarbeitungsvertrag (AVV) regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Nutzung der Plattform „{ keep it developed }“ gemäß dem zwischen den Parteien geschlossenen Nutzungsvertrag (gem. AGB) (nachfolgend „**Hauptvertrag**“).

Dieser AVV gilt für alle Tätigkeiten, bei denen der Auftragsverarbeiter oder dessen Erfüllungsgehilfen (Mitarbeiter, Subunternehmer) im Rahmen der Erbringung der im Hauptvertrag definierten Leistungen (insb. der Bearbeitung von „Tasks“ an den Shops des Verantwortlichen) personenbezogene Daten (nachfolgend „**Daten**“) verarbeiten, für die der Verantwortliche die datenschutzrechtliche Verantwortung trägt.

Der Verantwortliche kann in diesem Verhältnis (i) der „Verantwortliche“ im Sinne des Art. 4 Nr. 7 DSGVO sein (z.B. als direkter Shop-Inhaber) oder (ii) selbst „Auftragsverarbeiter“ für dessen eigene Endkunden sein (z.B. als Agentur). In Fall (ii) handelt der Auftragsverarbeiter (visuax) als Unterauftragsverarbeiter (gem. Art. 28 Abs. 4 DSGVO) für den Verantwortlichen. Die in diesem AVV festgelegten Pflichten gelten entsprechend.

1 Gegenstand, Dauer und Spezifikation der Auftragsverarbeitung

1.1 Gegenstand & Zweck

Gegenstand und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag (Erbringung von Software-Engineering-Dienstleistungen). Die Spezifika sind in **Anlage A** zu diesem AVV detailliert.

1.2 Dauer

Die Dauer dieser Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrags.

1.3 Art der Daten & Betroffene

Die Art der verarbeiteten personenbezogenen Daten und der Kreis der Betroffenen sind in **Anlage A** spezifiziert.

2 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich, Daten nur im Einklang mit diesem AVV und den geltenden Datenschutzgesetzen zu verarbeiten.

2.1 Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf Grundlage dieses Vertrags und der dokumentierten Weisungen des Verantwortlichen (insb. durch die Erstellung eines „Tasks“). Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen unverzüglich zu informieren, wenn eine Weisung seiner Ansicht nach gegen die DSGVO oder andere Datenschutzvorschriften verstößt (Art. 28 Abs. 3 S. 3 DSGVO).

2.2 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle Personen, die zur Verarbeitung der Daten des Verantwortlichen befugt sind (z.B. Mitarbeiter, Freelancer), zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen wurden (Art. 28 Abs. 3 lit. b DSGVO).

2.3 Technische und Organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter ergreift und unterhält alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten. Diese Maßnahmen sind in **Anlage C** beschrieben. Der Auftragsverarbeiter behält sich das Recht vor, die TOMs an den technischen und organisatorischen Fortschritt anzupassen, solange das Schutzniveau nicht unterschritten wird.

2.4 Unterauftragsverhältnisse

Der Auftragsverarbeiter darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur gemäß den Regelungen in § 4 dieses AVV hinzuzuziehen.

2.5 Unterstützung des Verantwortlichen (Betroffenenrechte)

Soweit dies möglich ist, unterstützt der Auftragsverarbeiter den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten, auf Anträge auf Ausübung der Rechte der Betroffenen (Kapitel III DSGVO) zu reagieren (Art. 28 Abs. 3 lit. e DSGVO). Wendet sich ein Betroffener direkt an den Auftragsverarbeiter, wird dieser das Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

2.6 Unterstützung (Pflichten nach Art. 32-36 DSGVO)

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Datenschutz-Folgenabschätzung, Meldung von Datenschutzverstößen) (Art. 28 Abs. 3 lit. f DSGVO).

2.7 Meldung von Datenschutzverstößen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten, die die Daten des Verantwortlichen betreffen, unverzüglich (ohne schuldhaftes Zögern), nachdem ihm diese bekannt wurden.

2.8 Löschung oder Rückgabe

Nach Beendigung des Hauptvertrags (Kündigung) wird der Auftragsverarbeiter alle im Auftrag verarbeiteten Daten (insb. aus den Shops) nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern keine gesetzliche Speicherpflicht (z.B. handels- oder steuerrechtlich) besteht. Der Auftragsverarbeiter ist berechtigt, die Daten 30 Tage nach Vertragsende unwiederbringlich zu löschen.

2.9 Kontroll- und Auditrechte

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung. Überprüfungen und Inspektionen (Audits) durch den Verantwortlichen oder einen von ihm beauftragten Prüfer sind nach rechtzeitiger Ankündigung (mind. 30 Tage) während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs zu ermöglichen. Der Auftragsverarbeiter kann die Durchführung eines Audits verweigern, wenn der beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Auftragsverarbeiter ist berechtigt, die Erfüllung der Pflichten alternativ durch Vorlage geeigneter, aktueller Zertifikate (z.B. ISO 27001) oder Berichte unabhängiger Prüfer (z.B. Datenschutzaudit) nachzuweisen. Der Aufwand für Audits ist vom Verantwortlichen zu tragen.

3 Pflichten des Verantwortlichen

3.1 Rechtmäßigkeit

Der Verantwortliche ist für die Beurteilung der Rechtmäßigkeit der Verarbeitung (gem. Art. 6 Abs. 1 DSGVO) sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich.

3.2 Weisungen

Der Verantwortliche erteilt alle Weisungen dokumentiert (z.B. über die Plattform). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform (z.B. E-Mail) zu bestätigen.

3.3 Informationspflicht

Der Verantwortliche hat den Auftragsverarbeiter unverzüglich zu informieren, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder im Zusammenhang mit den Datenschutzpflichten feststellt.

4 Unterauftragsverarbeiter

4.1 Genehmigung

Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung (gem. Art. 28 Abs. 2 DSGVO), weitere Unterauftragsverarbeiter hinzuzuziehen.

4.2 Aktuelle Liste

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage B** aufgeführt. Der Verantwortliche erteilt mit Abschluss dieses AVV seine Genehmigung für die Beauftragung dieser Unterauftragsverarbeiter.

4.3 Vertragliche Bindung

Der Auftragsverarbeiter stellt sicher, dass er den Unterauftragsverarbeitern vertraglich dieselben Datenschutzpflichten auferlegt, die in diesem AVV festgelegt sind (gem. Art. 28 Abs. 4 DSGVO), insbesondere hinsichtlich der TOMs und der Vertraulichkeit.

4.4 Drittlandtransfer

Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter in Drittländern (außerhalb der EU/des EWR) einzusetzen. Der Auftragsverarbeiter stellt sicher, dass hierfür ein angemessenes Datenschutzniveau gewährleistet ist, in der Regel durch den Abschluss von Standardvertragsklauseln (SCCs) der EU-Kommission (gem. Art. 46 DSGVO) und die Durchführung von Transfer Impact Assessments (TIAs). Die eingesetzten Sicherungsmaßnahmen sind in Anlage B aufgeführt.

4.5 Information und Widerspruchsrecht

Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung (Hinzufügung oder Ersetzung) von Unterauftragsverarbeitern (z.B. per E-Mail oder über die Plattform). Der Verantwortliche kann gegen eine solche Änderung aus wichtigem, datenschutzrechtlichem Grund schriftlich oder in Textform binnen 14 Tagen widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Bei einem berechtigten Widerspruch steht dem Auftragsverarbeiter ein Sonderkündigungsrecht für den Hauptvertrag zu.

4.6 Einsatz von KI-Systemen

Der Auftragsverarbeiter sichert zu, dass bei der Nutzung von KI-Systemen (z.B. zur Code-Generierung) durch seine Mitarbeiter oder Freelancer keine personenbezogenen Daten des Verantwortlichen (insb. aus dessen Shops) an die KI-Systeme übermittelt werden. Die KI-Anbieter werden auf Basis dieser Zusicherung nicht als Unterauftragsverarbeiter im Sinne dieses AVV behandelt. Der Auftragsverarbeiter trifft die erforderlichen organisatorischen Maßnahmen, um die Einhaltung dieser Vorgabe sicherzustellen.

5 Technische und Organisatorische Maßnahmen (TOMs)

1. Der Auftragsverarbeiter trifft die in **Anlage C** dargelegten technischen und organisatorischen Maßnahmen (TOMs) zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO.

2. Die TOMs unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter ist berechtigt, die TOMs anzupassen, sofern das Schutzniveau der festgelegten Maßnahmen nicht unterschritten wird.

6 Haftung

Die Haftung der Parteien für Datenschutzverstöße richtet sich nach den zwingenden gesetzlichen Bestimmungen der DSGVO, insbesondere Art. 82 DSGVO. Jede Partei haftet im Innenverhältnis für die Schäden, die sie im Rahmen ihrer jeweiligen Verantwortung (gemäß DSGVO) zu vertreten hat.

7 Schlussbestimmungen

7.1 Textform

Änderungen und Ergänzungen dieses AVV bedürfen der Textform (z.B. E-Mail). Mündliche Nebenabreden bestehen nicht.

7.2 Anwendbares Recht & Gerichtsstand

Dieser AVV unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Brensbach, Deutschland.

7.3 Vorrang

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag (AGB) gehen die Bestimmungen dieses AVV vor, soweit sie den Datenschutz betreffen.

7.4 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt. Entsprechendes gilt für eventuelle Vertragslücken.

Anlagen

A Anlage: Beschreibung der Auftragsverarbeitung

(gem. Art. 28 Abs. 3 DSGVO)

A.1 Gegenstand und Zweck der Verarbeitung

- **Gegenstand:** Erbringung von IT-Dienstleistungen (Software-Engineering, technische Unterstützung, Fehlerbehebung) im Rahmen der Nutzung der Plattform „{ keep it developed }“ gemäß Hauptvertrag.
- **Zweck:** Durchführung der vom Verantwortlichen beauftragten „Tasks“ an dessen Online-Shops (insb. Shopify-Instanzen). Dies umfasst die technische Möglichkeit des Zugriffs, der Speicherung, Änderung und Löschung von Daten zur Erfüllung der Werkleistungen.

A.2 Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer der Laufzeit des Hauptvertrags zwischen den Parteien.

A.3 Art der personenbezogenen Daten

Da der Auftragsverarbeiter (visuax) zur Erfüllung der Tasks technischen Zugriff (z.B. Gastzugang) auf die Systeme (Shops) des Verantwortlichen erhält, ist eine Verarbeitung (mindestens einsehbar) folgender Datenkategorien der Endkunden der Shops möglich:

- **Personen-Stammdaten:** Name, Vorname, Anrede
- **Kontaktdaten:** Anschrift (Liefer- und Rechnungsanschrift), E-Mail-Adresse, Telefonnummer
- **Vertrags- & Bestelldaten:** Bestellhistorie, Warenkorb-Informationen, Rechnungs- und Transaktionsnummern, Kunden-IDs
- **Zahlungsdaten:** Zahlungsinformationen (z.B. Zahlungsstatus, genutzter Zahlungsdienstleister, ggf. maskierte Kreditkarteninformationen oder Bankverbindungsdaten)
- **Technische Daten (soweit im Shop gespeichert):** Ggf. IP-Adressen, technische Protokolldaten der Shop-Nutzer.

A.4 Kreis der Betroffenen

- Kunden und Nutzer (Endkunden) der Online-Shops des Verantwortlichen.
- Ggf. Mitarbeiter des Verantwortlichen (sofern deren Daten im Shop-System verarbeitet werden).

B Anlage: Genehmigte Unterauftragsverarbeiter

(Stand: 23. Oktober 2025)

Der Verantwortliche erteilt die allgemeine Genehmigung für folgende Kategorien von Unterauftragsverarbeitern:

Nr.	Unternehmen / Kategorie	Standort (Verarbeitung)	Zweck der Verarbeitung	Angemessenheitsmechanismus (bei Drittland)
1.	**Amazon Web Services (AWS) EMEA SARL**	Frankfurt am Main (Deutschland / EU)	Hosting der Plattform-Infrastruktur, Datenbanken, Speicher	N/A (Verarbeitung in EU)
2.	**Cloudflare, Inc.**	Weltweit (CDN) / USA	CDN, Sicherheit der Plattform-Infrastruktur	Standardvertragsklauseln (SCCs)
3.	**Sorgfältig ausgewählte Freelance-Entwickler** (als Subunternehmer gem. AGB § 2.1)	Weltweit (innerhalb und außerhalb der EU/EWR)	Erbringung der Werkleistung (Durchführung von „Tasks“)	Standardvertragsklauseln (SCCs) (bei Einsatz in Drittländern)

C Anlage: Technische und Organisatorische Maßnahmen (TOMs)

(gem. Art. 32 DSGVO)

Der Auftragsverarbeiter (visuax) trifft folgende Maßnahmen, um die Sicherheit der im Auftrag verarbeiteten Daten zu gewährleisten:

C.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Zutrittskontrolle:** Maßnahmen, die Unbefugten den physischen Zutritt zu den Datenverarbeitungsanlagen verwehren.
    - Die Verarbeitung findet in den Hochsicherheits-Rechenzentren von AWS (Frankfurt) statt. Der Auftragsverarbeiter verlässt sich auf die von AWS implementierten und zertifizierten physischen Zutrittskontrollmaßnahmen (z.B. Sicherheitspersonal, mehrstufige Authentifizierung, Videoüberwachung).
- **Zugangskontrolle:** Maßnahmen, die Unbefugten die Nutzung der Datenverarbeitungssysteme verwehren.
    - Einsatz von branchenüblichen, sicheren Authentifizierungsmechanismen (z.B. Multi-Faktor-Authentifizierung, SAML-basiertes Single Sign-On) für Mitarbeiter und Freelancer.
    - Erzwungene Passwortrichtlinien (Mindestlänge, Komplexität, 2-Faktor-Authentifizierung (2FA) wo möglich).
- **Zugriffskontrolle:** Maßnahmen, die sicherstellen, dass die zur Nutzung eines Systems Befugten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.
    - Einsatz von Rollen- und Berechtigungskonzepten.
    - Zugriff auf Kundensysteme (Shops) erfolgt nur bei Vorliegen eines aktiven Auftrags (Task).
    - Nutzung von branchenüblichen Sicherheitstechnologien zur Absicherung der Endpunkte.
- **Trennungskontrolle:** Maßnahmen, die sicherstellen, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden.
    - Strikte logische Mandantentrennung der Kundendaten auf Datenbank- und Applikationsebene.

C.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle:** Maßnahmen, die sicherstellen, dass Daten bei der elektronischen Übertragung oder beim Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
    - Ausschließliche Nutzung von verschlüsselten Verbindungen (SSL/TLS) für alle externen Datenübertragungen (Data in Transit).
    - Verschlüsselung von Datenbanken im Ruhezustand (Data at Rest).

- **Eingabekontrolle:** Maßnahmen, die sicherstellen, dass nachträglich überprüft werden kann, wer Daten in die Systeme eingegeben, verändert oder entfernt hat.
    - Protokollierung (Logging) von systemrelevanten Ereignissen und administrativen Zugriffen.

C.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b & c DSGVO)

- **Verfügbarkeitskontrolle:** Maßnahmen, die sicherstellen, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
    - Betrieb der Infrastruktur in einer Hochverfügbarkeitsumgebung (AWS Frankfurt).
    - Erstellung von regelmäßigen, automatisierten Backups der Plattform-Datenbanken.
- **Belastbarkeit:** Einsatz von skalierbaren Systemen und Schutz vor DDoS-Angriffen, um die Belastbarkeit der Systeme zu gewährleisten.

C.4 Verfahren zur regelmäßigen Überprüfung und Bewertung (Art. 32 Abs. 1 lit. d DSGVO)

- Regelmäßige Überprüfung der Sicherheitseinstellungen und Anpassung an neue Bedrohungslagen (Data Protection Management).
- Prozesse zur Meldung und Bearbeitung von Datenschutzvorfällen (Incident Response).
- Sorgfältige Auswahl und vertragliche Verpflichtung von Mitarbeitern und Freelancern (Vertraulichkeit, Einhaltung der Weisungen).