Auftragsverarbeitungsvertrag (AVV)

Stand: 30. November 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.

Dieser Vertrag wird im Wege des elektronischen Vertragsschlusses geschlossen. Er bedarf keiner handschriftlichen Unterzeichnung. Die Parteien verzichten ausdrücklich auf das Erfordernis einer qualifizierten elektronischen Signatur oder Schriftform, soweit gesetzlich zulässig.

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. Die Bestimmungen dieses AVV gelten über das Ende des Hauptvertrags hinaus fort, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen besitzt, speichert oder verarbeitet (z.B. während der Karenzzeit bis zur endgültigen Löschung gemäß § 2.8).

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 Anonymisierung und Aggregation

Der Verantwortliche weist den Auftragsverarbeiter an, personenbezogene Daten zu aggregieren oder zu anonymisieren, um diese für die in den AGB (§ 11) definierten Zwecke (z.B. KI-Training, Benchmarking) zu nutzen. Der Auftragsverarbeiter wendet hierfür marktübliche Verfahren an, die darauf abzielen, den Personenbezug zu entfernen (z.B. Entfernung von Direktdentifikatoren). Sollte trotz dieser Maßnahmen eine Re-Identifizierung technisch möglich sein, gilt dies nicht als weisungswidrige Verarbeitung zu eigenen Zwecken,

sondern die betroffenen Daten unterliegen in diesem Fall weiterhin vollumfänglich den Schutzbestimmungen dieses Vertrags.

2.4 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.

2.5 Unterauftragsverhältnisse

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

2.6 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.

Soweit der Verantwortliche die Rechte der Betroffenen (insb. Auskunft, Berichtigung, Löschung) durch die vorhandenen Funktionalitäten der Plattform selbst erfüllen kann (Self-Service), besteht keine gesonderte Unterstützungspflicht des Auftragsverarbeiters. Der Verantwortliche ist verpflichtet, diese Möglichkeiten vorrangig zu nutzen.

2.7 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). Soweit der Auftragsverarbeiter Unterstützungsleistungen erbringt (z.B. bei Datenschutz-Folgenabschätzungen oder komplexen Auskunftsanfragen), die über die Bereitstellung standardisierter Informationen hinausgehen, ist er berechtigt, diesen Aufwand gesondert zu vergüten, sofern die Ursache für die Unterstützungspflicht nicht in einem Fehlverhalten des Auftragsverarbeiters liegt.

2.8 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. Die Meldung erfolgt in Textform an die im Account des Verantwortlichen hinterlegte E-Mail-Adresse des Administrators. Der Verantwortliche stellt sicher, dass diese Adresse aktuell ist und regelmäßig überwacht wird.

Die Meldepflicht umfasst nicht bloße Störungen oder erfolglose Angriffsversuche (z.B. ‚Ping'-Sweeps, Port-Scans, erfolgreich durch Firewalls abgewehrte Angriffe oder gescheiterte Login-Versuche), solange diese nicht zu einem tatsächlichen unbefugten Zugriff auf Daten oder deren Beeinträchtigung geführt haben.

Sollte der Verantwortliche den Auftragsverarbeiter zur Untersuchung eines Sicherheitsvorfalls oder Verdachtsfalls auffordern, und stellt sich heraus, dass dieser Vorfall nicht im Verantwortungsbereich des Auftragsverarbeiters lag oder sich der Verdacht als unbegründet erweist, ist der Auftragsverarbeiter berechtigt, den für die Analyse und Untersuchung entstandenen Aufwand (Forensik, Logging-Analyse) zu marktüblichen Sätzen in Rechnung zu stellen.

2.9 Löschung oder Rückgabe

Der Auftragsverarbeiter ist berechtigt, Daten, die vom Verantwortlichen offensichtlich irrtümlich oder ohne erkennbaren Bezug zum Auftrag (Task) übermittelt wurden (z.B. vollständige Datenbank-Dumps statt Testdaten), nach eigenem Ermessen sofort zu löschen, um die Datensparsamkeit und Datensicherheit zu gewährleisten. Der Auftragsverarbeiter wird den Verantwortlichen hierüber informieren.

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. Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format (z.B. JSON oder CSV) nach Wahl des Auftragsverarbeiters. Wünscht der Verantwortliche eine Konvertierung in ein anderes Format, so ist diese gesondert zu vergüten. Der Auftragsverarbeiter ist berechtigt, die Daten 30 Tage nach Vertragsende unwiederbringlich zu löschen. Soweit sich Daten in systemseitigen Datensicherungen (Backups) befinden, ist eine sofortige Löschung technisch nicht möglich. Diese Daten werden im Rahmen der regulären Rotationszyklen (spätestens nach 90 Tagen) automatisch überschrieben und bis dahin nicht für andere Zwecke verarbeitet (Sperrung). Als Nachweis der erfolgten Löschung genügt eine Bestätigung des Auftragsverarbeiters in Textform (z.B. E-Mail oder Benachrichtigung auf der Plattform). Die Erstellung formeller Löschprotokolle oder Zertifikate ist nicht geschuldet, kann jedoch als kostenpflichtige Zusatzleistung beauftragt werden.

2.10 Kontroll- und Auditrechte

Der Auftragsverarbeiter stellt die für das Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen (Art. 30 DSGVO) erforderlichen Angaben vollständig in diesem Vertrag und seinen Anlagen bereit. Der Verantwortliche erkennt dies als ausreichend an. Die Bearbeitung darüber hinausgehender, individueller Sicherheitsfragebögen des Verantwortlichen ist eine kostenpflichtige Zusatzleistung.

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 Verantwortliche verpflichtet sich, alle im Rahmen von Kontrollen oder Audits erlangten Kenntnisse über die Sicherheitsarchitektur, TOMs und internen Prozesse des Auftragsverarbeiters als Geschäftsgeheimnisse streng vertraulich zu behandeln. Eine Weitergabe an Dritte (außer an zuständige Aufsichtsbehörden) ist untersagt. 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. Überprüfungen und Inspektionen sind auf einmal pro Kalenderjahr beschränkt, es sei denn, es liegen begründete Verdachtsmomente für erhebliche Datenschutzverstöße vor. Der Aufwand für Audits ist vom Verantwortlichen zu tragen. Der Auftragsverarbeiter ist berechtigt, den durch die Begleitung von Überprüfungen und Inspektionen entstehenden Personalaufwand zu angemessenen, marktüblichen Stundensätzen in Rechnung zu stellen, sofern das Audit nicht durch einen Verstoß des Auftragsverarbeiters veranlasst wurde.

2.11 Wiederherstellung von Daten

Die in Anlage C genannten Backups der Plattform-Datenbanken dienen ausschließlich der Sicherstellung der allgemeinen Systemverfügbarkeit und der Wiederherstellung der Gesamt-Plattform nach systemischen Ausfällen (Disaster Recovery). Der Auftragsverarbeiter stellt keine Funktionalität zur selektiven Wiederherstellung einzelner, vom Verantwortlichen (oder dessen Nutzern) gelöschter oder veränderter Daten (z.B. einzelne Tasks, Projekte oder Inhalte) bereit. Ein Anspruch des Verantwortlichen auf eine solche individuelle Datenwiederherstellung besteht nicht. Sollte der Auftragsverarbeiter auf gesonderten Wunsch des Verantwortlichen dennoch versuchen, Daten aus den System-Backups zu extrahieren, ist dieser Aufwand gesondert zu vergüten; eine Erfolgsgarantie wird hierfür nicht übernommen.

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. Der Verantwortliche benennt die weisungsbefugten Personen durch die Einrichtung von Benutzerkonten auf der Plattform. Jede über ein authentifiziertes Benutzerkonto (Admin oder Employee) übermittelte Weisung (Task) gilt gegenüber dem Auftragsverarbeiter als wirksam erteilt. Der Auftragsverarbeiter ist nicht verpflichtet, interne Berechtigungsstufen des Verantwortlichen zu prüfen.

Der Verantwortliche sichert zu, keine besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO (z.B. Gesundheitsdaten) oder unmaskierte Kreditkartendaten (PCI-DSS)

in die Systeme des Auftragsverarbeiters einzugeben oder zu übermitteln, sofern dies nicht ausdrücklich schriftlich als Vertragszweck vereinbart wurde. Sollten solche Daten dennoch übermittelt werden, haftet der Verantwortliche für alle daraus resultierenden Schäden und Mehraufwände.

3.2 Weisungen

Weisungen sind grundsätzlich über die Eingabemasken der Plattform (‚Tasks') zu erteilen. Mündliche Weisungen sind nur in dringenden Gefahrensituationen zulässig und müssen vom Verantwortlichen unverzüglich in Textform bestätigt werden. Bis zum Eingang der Bestätigung ist der Auftragsverarbeiter berechtigt, die Ausführung der mündlichen Weisung auszusetzen.

Die Weisung zur Bearbeitung eines Tasks umfasst implizit die Ermächtigung und Anweisung, alle technisch notwendigen operativen Zwischenschritte (z.B. temporäre Zwischenspeicherung, Erstellung von Debug-Logs, Caching, Kompilierung) vorzunehmen, die zur ordnungsgemäßen technischen Erfüllung des Tasks erforderlich sind.

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. Dies erfolgt vorrangig auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission (z.B. das „EU-U.S. Data Privacy Framework"), sofern der Unterauftragsverarbeiter entsprechend zertifiziert ist. Andernfalls

erfolgt der Transfer auf Grundlage der Standardvertragsklauseln (SCCs) der EU-Kommission (gem. Art. 46 DSGVO) unter Ergänzung erforderlicher zusätzlicher Schutzmaßnahmen (Transfer Impact Assessments). 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. Erfolgt ein Widerspruch, und ist dem Auftragsverarbeiter die Erbringung der Leistung ohne den neuen Unterauftragsverarbeiter technisch unmöglich oder wirtschaftlich unzumutbar, ist der Auftragsverarbeiter berechtigt, den Hauptvertrag mit einer Frist von zwei Wochen außerordentlich zu kündigen. Ein Anspruch des Verantwortlichen auf Fortführung der Leistung unter Nutzung der alten Unterauftragsverarbeiter-Struktur besteht in diesem Fall nicht.

4.6 Einsatz von KI-Systemen

Der Auftragsverarbeiter setzt KI-gestützte Tools (z.B. zur Code-Generierung oder -Analyse) ein, um die Effizienz der Leistungserbringung zu steigern. Der Auftragsverarbeiter verpflichtet seine Mitarbeiter und Subunternehmer vertraglich, keine Echtdaten (Real Data) aus den Shops des Verantwortlichen in offene KI-Modelle einzugeben, sofern diese Modelle die Eingabedaten zum Training nutzen („No-Training-Policy“). Sollte die Nutzung eines KI-Tools die Verarbeitung personenbezogener Daten des Verantwortlichen erfordern, wird der jeweilige KI-Anbieter (z.B. OpenAI, Microsoft) vorab als Unterauftragsverarbeiter gemäß § 4 Abs. 2 und 5 in die Liste aufgenommen.

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 richtet sich nach den gesetzlichen Bestimmungen. Für Schadensersatzansprüche gegenüber dem Auftragsverarbeiter gelten jedoch die im Hauptvertrag (AGB) vereinbarten Haftungsbeschränkungen und -ausschlüsse auch für Ansprüche aus diesem AVV, soweit dies nicht zwingenden gesetzlichen Vorschriften (insb. Art. 82 DSGVO gegenüber Betroffenen) entgegensteht.

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: 30. November 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	EU-U.S. Data Privacy Framework
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 (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).

C.5 Mobile Arbeit und Homeoffice

Der Verantwortliche gestattet dem Auftragsverarbeiter und dessen Unterauftragsverarbeitern ausdrücklich die Erbringung der Leistung im Wege der mobilen Arbeit (Homeoffice, Remote Work). Der Auftragsverarbeiter stellt sicher, dass in diesen Umgebungen ein angemessenes Schutzniveau gewährleistet wird. Dazu gehören insbesondere:

- Vollständige Verschlüsselung der Festplatten (Full Disk Encryption) auf allen mobilen Endgeräten.
- Einsatz von Sichtschutzfiltern oder Wahl eines Arbeitsplatzes ohne Einsichtnahme durch Dritte.
- Nutzung sicherer VPN-Verbindungen für den Zugriff auf Unternehmensressourcen.
- Automatische Bildschirmsperre bei Abwesenheit vom Arbeitsplatz.