

Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 DSGVO · Atlaron GmbH · Stand: 26.06.2026

zwischen

dem Kunden (nachfolgend „**Verantwortlicher**“)

und

Atlaron GmbH, Bonhoefferstr. 26, 73760 Ostfildern, Deutschland (nachfolgend „**Auftragsverarbeiter**“)

vertreten durch den Geschäftsführer Dr. Jochen Kokemüller, Amtsgericht Stuttgart HRB 806002

– gemeinsam die „**Parteien**“ –

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen über die Atlaron-Plattform (KI-Agenten und Plattformfunktionen). Im Rahmen dieser Leistungserbringung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Dieser AVV konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO.

(2) Die Dauer dieses AVV entspricht der Laufzeit des zugrundeliegenden Hauptvertrags (Nutzungs- bzw. Leistungsvertrag über die Plattform). Eine Kündigung des Hauptvertrags gilt zugleich als Kündigung dieses AVV.

(3) Im Verhältnis der Parteien ist der Verantwortliche für die Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich (Art. 28 Abs. 3 lit. a, Art. 4 Nr. 7 DSGVO).

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) **Art der Verarbeitung:** Erheben, Erfassen, Speichern, Auslesen, Verarbeiten durch KI-Agenten, Organisieren, Verändern, Übermitteln innerhalb der Plattform, Löschen.

(2) **Zweck:** Bereitstellung und Ausführung der vom Verantwortlichen beauftragten KI-Agenten und Plattformfunktionen. Der konkrete Umfang der Verarbeitung wird durch den Verantwortlichen bestimmt, indem er die jeweiligen Agenten und Plattformfunktionen auswählt, aktiviert und nutzt sowie Daten in diese eingibt. Die Hinzunahme, Änderung oder Abwahl einzelner Agenten oder Funktionen im Rahmen der Plattform bedarf keiner Änderung dieses Vertrags.

(3) **Kategorien betroffener Personen** (vom Verantwortlichen je nach Einsatz zu konkretisieren): z. B. Beschäftigte, ehemalige Beschäftigte, Kunden, Mandanten, Interessenten, Ansprechpartner des Verantwortlichen.

(4) **Kategorien personenbezogener Daten** (vom Verantwortlichen je nach Einsatz zu konkretisieren): z. B. Stammdaten, Kontaktdaten, Vertragsdaten, Kommunikationsinhalte sowie alle weiteren Daten, die der Verantwortliche in die Agenten eingibt. Gibt der Verantwortliche besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) ein, ist er für deren Zulässigkeit allein verantwortlich.

§ 3 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf die Übermittlung in Drittländer, sofern er nicht durch Unionsrecht oder das Recht eines Mitgliedstaats verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO).

(2) Die Konfiguration und Nutzung der Plattform durch den Verantwortlichen gilt als Weisung. Darüber hinausgehende Einzelweisungen sind in Textform zu erteilen.

(3) Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, informiert er den Verantwortlichen unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO).

§ 4 Keine Nutzung zu eigenen Zwecken, kein Modelltraining

- (1) Der Auftragsverarbeiter nutzt die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und nicht für eigene Zwecke.
- (2) Insbesondere findet kein Training von KI-Modellen mit den Inhaltsdaten des Verantwortlichen statt. Diese Verpflichtung gilt auch für die eingesetzten Unterauftragsverarbeiter (siehe Anlage 2) und ist in den jeweiligen Unterauftragsverhältnissen abgesichert.

§ 5 Vertraulichkeit

Der Auftragsverarbeiter setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO). Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Auftrags fort.

§ 6 Technische und organisatorische Maßnahmen (TOM)

- (1) Der Auftragsverarbeiter trifft die zur Gewährleistung eines angemessenen Schutzniveaus erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Diese sind in Anlage 1 beschrieben.
- (2) Die TOM unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

§ 7 Unterauftragsverarbeiter

- (1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Einschaltung von Unterauftragsverarbeitern (Art. 28 Abs. 2 DSGVO). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt.
- (2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzuziehung oder Austausch) rechtzeitig vorab. Der Verantwortliche kann einer Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen widersprechen (Art. 28 Abs. 2 Satz 2 DSGVO).
- (3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter auf dieselben Datenschutzpflichten, die in diesem AVV festgelegt sind (Art. 28 Abs. 4 DSGVO).

§ 8 Unterstützung des Verantwortlichen

- (1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung von Betroffenenanfragen (Art. 12–22 DSGVO). Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter (Art. 28 Abs. 3 lit. e DSGVO).
- (2) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Datensicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung), Art. 28 Abs. 3 lit. f DSGVO.

§ 9 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden (Art. 33 Abs. 2 DSGVO), spätestens innerhalb von 48 Stunden, und stellt die zur Erfüllung der Meldepflichten des Verantwortlichen erforderlichen Informationen bereit.

§ 10 Löschung und Rückgabe

Nach Abschluss der Leistungserbringung löscht der Auftragsverarbeiter alle personenbezogenen Daten oder gibt sie nach Wahl des Verantwortlichen zurück und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g DSGVO). Die Löschung oder Rückgabe wird auf Verlangen bestätigt.

§ 11 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen (Art. 28 Abs. 3 lit. h DSGVO).

(2) Nachweise können insbesondere durch Vorlage geeigneter Dokumentationen, Zertifizierungen oder Prüfberichte erbracht werden. Vor-Ort-Prüfungen sind nach angemessener Vorankündigung und während der üblichen Geschäftszeiten möglich.

§ 12 Ort der Verarbeitung / Drittland

Die Verarbeitung erfolgt ausschließlich in der Europäischen Union bzw. dem Europäischen Wirtschaftsraum. Eine Übermittlung in ein Drittland erfolgt nur auf Weisung des Verantwortlichen oder bei Vorliegen geeigneter Garantien nach Kapitel V DSGVO. Die eingesetzten Unterauftragsverarbeiter (Anlage 2) verarbeiten innerhalb der EU bzw. des EWR.

§ 13 Haftung und Schlussbestimmungen

(1) Für die Haftung gelten die Regelungen des Hauptvertrags sowie Art. 82 DSGVO.

(2) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV in datenschutzrechtlichen Fragen vor.

(3) Es gilt deutsches Recht. Änderungen bedürfen der Textform.

Ort, Datum

Ort, Datum

Für den Verantwortlichen

Für die Atlaron GmbH

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

nach Art. 32 DSGVO · Stand: 26.06.2026

1. Vertraulichkeit

Zutrittskontrolle: Betrieb der Infrastruktur in Rechenzentren des europäischen Anbieters IONOS (Deutschland/EU) mit etablierten physischen Zugangssicherungen. Der Auftragsverarbeiter betreibt keine eigenen Serverräume mit Kundendaten.

Zugangskontrolle: Zugriff nur über persönliche, authentifizierte Konten; zentrales Identitäts- und Zugriffsmanagement (Keycloak); Mehr-Faktor-Authentifizierung für administrative Zugänge; Passwortrichtlinien.

Zugriffskontrolle: Rollen- und Berechtigungskonzept (Least-Privilege); Mandantentrennung; Protokollierung sicherheitsrelevanter Zugriffe; lückenlose Audit-Trails über Agentenentscheidungen.

Trennungskontrolle: Logische Trennung der Daten verschiedener Kunden bzw. Mandanten; getrennte Verarbeitungskontexte.

Pseudonymisierung/Maskierung: Automatisierte Erkennung und Maskierung personenbezogener Daten (PII-Erkennung) in den Verarbeitungspfaden der Agenten.

2. Integrität

Weitergabekontrolle: Verschlüsselte Datenübertragung (TLS); Verarbeitung der Inhalte durch LLM (Mistral) auf EU-Infrastruktur; keine Übermittlung an außereuropäische Cloud-Anbieter.

Eingabekontrolle: Protokollierung von Eingaben, Änderungen und Agentenaktionen; Nachvollziehbarkeit über exportierbare Audit-Trails.

3. Verfügbarkeit und Belastbarkeit

Backup- und Wiederherstellungskonzept; Monitoring der Systeme; Schutzmaßnahmen gegen Verlust durch technische Störungen; Betrieb auf resilienter europäischer Cloud-Infrastruktur.

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

Auftragskontrolle: Verpflichtung der Unterauftragsverarbeiter nach Art. 28 DSGVO; Weisungsbindung.

Incident-Management: Definierte Prozesse zur Erkennung, Meldung und Behandlung von Datenschutzverletzungen; Eskalationspfade zu menschlichen Entscheidern (Approval Gates).

Datenschutz durch Technikgestaltung und Voreinstellungen (Art. 25 DSGVO): Compliance als Designprinzip der Plattform; Local-First-Verarbeitung sensibler Dokumente; europäische Souveränität by Design.

Anlage 2 – Unterauftragsverarbeiter

Stand: 26.06.2026

Unterauftragsverarbeiter	Sitz	Zweck / Leistung	Ort der Verarbeitung
IONOS SE	Montabaur, Deutschland	Hosting / Cloud-Infrastruktur (ohne inhaltlichen Datenzugriff)	EU (Deutschland)
Mistral AI SAS	Paris, Frankreich	LLM-Verarbeitung von Inhalten der Agenten; kein Modelltraining mit Kundendaten	EU (Frankreich)

Die Zahlungsabwicklung über Stripe Payments Europe, Ltd. (Dublin, Irland) erfolgt nicht im Rahmen dieser Auftragsverarbeitung. Stripe handelt für Zahlungsdaten als eigenständig Verantwortlicher; Einzelheiten hierzu finden sich in der Datenschutzerklärung der Atlaron GmbH.