Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO · Anlage zum «Hauptvertrag» Nr. «Vertragsnummer»

VERANTWORTLICHER	AUFTRAGSVERARBEITER
«Firma» **«Straße»** **«PLZ Ort»** **«Registergericht, HRB»** vertreten durch **«Name, Funktion»** („Verantwortlicher“)	**Outcomet UG (haftungsbeschränkt)** Amalie-Baader-Straße 1 76137 Karlsruhe Amtsgericht Mannheim, HRB 758563 vertreten durch den Geschäftsführer Andy Görnt („Auftragsverarbeiter“)

1 Gegenstand und Dauer

Der Auftragsverarbeiter betreibt für den Verantwortlichen die Software Outcomet als Software-as-a-Service nach dem **«Hauptvertrag»** Nr. **«Vertragsnummer»** („Hauptvertrag"). Dabei verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen.

Dieser Vertrag gilt, solange der Hauptvertrag läuft, und darüber hinaus, bis alle Daten nach Ziffer 10 gelöscht oder zurückgegeben sind.

2 Art, Zweck und Umfang der Verarbeitung

Zweck: Bereitstellung von Outcomet zur Sammlung, Strukturierung und Auswertung von Kundenfeedback, Produktinhalten und Entscheidungen, einschließlich KI-gestützter Auswertung.

Art der Verarbeitung: Erheben, Speichern, Ordnen, Strukturieren, Auswerten, Abfragen, Übermitteln an die Unterauftragsverarbeiter nach Anlage B, Löschen.

Arten personenbezogener Daten

- Kontodaten der Nutzer: Name, E-Mail-Adresse, Rolle, Anmeldedaten
- Inhalte, die der Verantwortliche einbringt: Feedback, Interviewnotizen und -transkripte, Kommentare, Produkt- und Strategieinhalte, soweit sie Personenbezug haben
- Kontaktdaten von Gesprächspartnern und Kunden des Verantwortlichen: Name, E-Mail-Adresse, Rolle, Unternehmen sowie die Einstufungen, die der Verantwortliche oder Outcomet dazu im Workspace speichert
- Daten aus Integrationen, die der Verantwortliche verbindet: Vorgänge, Kommentare, Commits und Pull Requests mit Autorenangaben
- E-Mails, die Outcomet im Auftrag des Verantwortlichen versendet
- Nutzungs- und Protokolldaten: IP-Adresse, Browserdaten, Fehlerprotokolle, Sitzungsaufzeichnungen mit maskierten Eingaben

Kategorien betroffener Personen

- Beschäftigte und Beauftragte des Verantwortlichen, die er als Nutzer einlädt
- Kunden, Nutzer und Interviewpartner des Verantwortlichen, deren Daten er einbringt
- Personen, die in verbundenen Systemen des Verantwortlichen als Autoren oder Bearbeiter erscheinen

Besondere Kategorien nach Art. 9 DSGVO verarbeitet Outcomet nicht bestimmungsgemäß. Der Verantwortliche bringt solche Daten nicht ein.

3 Weisungen

Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Dieser Vertrag, der Hauptvertrag und die Nutzung der Funktionen von Outcomet durch den Verantwortlichen sind solche Weisungen. Weitere Weisungen erteilt der Verantwortliche in Textform.

Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er das unverzüglich mit.

Eine Verarbeitung für eigene Zwecke findet nicht statt. Insbesondere werden Daten des Verantwortlichen nicht zum Training von KI-Modellen verwendet, weder vom Auftragsverarbeiter noch von seinen

Unterauftragsverarbeitern. Die einzige Ausnahme von der Verarbeitung für eigene Zwecke betrifft TypeSafe: zusammenfassende Statistiken und Erkenntnisse aus den Anfragen, kein Modelltraining (Anlage B). Der Verantwortliche stimmt ihr mit diesem Vertrag zu.

4 Vertraulichkeit

Alle Personen, die beim Auftragsverarbeiter Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet. Zugang zu den Daten in der Lösung hat derzeit ausschließlich der Geschäftsführer. Wer in einem gemeinsamen Kanal mit dem Verantwortlichen mitliest, ist schriftlich zur Vertraulichkeit verpflichtet. Weitere Personen erhalten Zugang erst nach schriftlicher Verpflichtung auf Vertraulichkeit.

5 Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage A beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.

6 Unterauftragsverarbeiter

Der Verantwortliche genehmigt die Unterauftragsverarbeiter in Anlage B.

Über neue oder ersetzte Unterauftragsverarbeiter informiert der Auftragsverarbeiter mindestens 30 Tage vorher in Textform. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Einigen sich die Parteien nicht, kann der Verantwortliche den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Datenschutzniveau. Die Dienstleister der Unterauftragsverarbeiter richten sich nach deren veröffentlichten Listen, die Anlage B nennt.

7 Übermittlung in Drittländer

Die Datenbank mit allen Inhalten des Verantwortlichen liegt in der EU. Einige Unterauftragsverarbeiter verarbeiten Daten in den USA oder im Vereinigten Königreich (Anlage B). Grundlage sind jeweils Angemessenheitsbeschlüsse der EU-Kommission, einschließlich des EU-US Data Privacy Framework, oder die EU-Standardvertragsklauseln.

8 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Anfragen betroffener Personen (Art. 12 bis 23 DSGVO) sowie bei seinen Pflichten nach Art. 32 bis 36 DSGVO. Anfragen, die direkt beim Auftragsverarbeiter eingehen, leitet er unverzüglich weiter.

9 Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung unverzüglich, spätestens 48 Stunden nachdem er davon erfahren hat. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO.

10 Löschung und Rückgabe

Nach Ende des Hauptvertrags kann der Verantwortliche seine Daten 30 Tage lang exportieren. Danach löscht der Auftragsverarbeiter sie, auch in der Entwicklungsumgebung, soweit keine gesetzliche Aufbewahrungspflicht besteht. Kopien in Datensicherungen werden im regulären Sicherungszyklus überschrieben. Bei Unterauftragsverarbeitern richtet sich die Löschung nach Anlage B. Nachrichten in einem gemeinsamen Kanal löscht der Auftragsverarbeiter auf Verlangen.

11 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen die Informationen zur Verfügung, die zum Nachweis der Pflichten aus diesem Vertrag nötig sind. Er ermöglicht Überprüfungen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer nach Ankündigung von mindestens 14 Tagen, zu den üblichen Geschäftszeiten und höchstens einmal im Jahr, außer bei konkretem Anlass.

12 Verhältnis zu anderen Vereinbarungen und Schlussbestimmungen

Die Haftung richtet sich nach Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.

Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag und einer Geheimhaltungsvereinbarung (NDA) der Parteien vor, soweit es um die Verarbeitung personenbezogener Daten geht. Der Einsatz der in Anlage B genannten Unterauftragsverarbeiter verstößt nicht gegen eine solche NDA.

Änderungen bedürfen der Textform. Es gilt deutsches Recht, Gerichtsstand ist Karlsruhe.

VERANTWORTLICHER **«Firma»**	AUFTRAGSVERARBEITER **Outcomet UG (haftungsbeschränkt)**
ORT	ORT Karlsruhe
DATUM	DATUM
NAME, FUNKTION **«Name, Funktion»**	NAME, FUNKTION Andy Görnt, Geschäftsführer
UNTERSCHRIFT	UNTERSCHRIFT

A Anlage A · Technische und organisatorische Maßnahmen nach Art. 32 DSGVO · Stand 31. Oktober 2026

Der Auftragsverarbeiter ist ein Kleinstunternehmen. Die Maßnahmen sind darauf ausgelegt: wenige Personen mit Zugriff, Sicherheit über die Plattformen der Unterauftragsverarbeiter, alles nachvollziehbar.

1 Vertraulichkeit

Zutritt: Outcomet betreibt keine eigenen Server. Die Rechenzentren gehören den Anbietern aus Anlage B, die ihre physische Sicherheit nach SOC 2 Typ II bzw. ISO 27001 nachweisen.

Zugang zu Systemen

- Administrativen Zugang zu Datenbank, Hosting und Anbieterkonten hat ausschließlich der Geschäftsführer.
- Zugangsdaten für Programmschnittstellen liegen als Umgebungsvariablen beim jeweiligen Anbieter, nicht im Quellcode.
- Nutzer melden sich mit E-Mail und Passwort oder über einen Identitätsanbieter an. Die Anmeldung verwaltet Supabase Auth.

Zugriff auf Daten

- Kundendaten sind auf Ebene des Workspace getrennt. Row-Level-Security ist in der Produktivdatenbank auf allen Tabellen aktiv. Ein Nutzer sieht nur Daten der Workspaces, zu denen er eingeladen ist.
- Neue Nutzer lädt ein Administrator des Verantwortlichen ein. Nutzer mit einer E-Mail-Adresse unter der Domain des Verantwortlichen werden seinem Workspace automatisch zugeordnet.
- Integrationen (GitHub, Jira, HubSpot, Granola, LinkedIn, Discord) verbindet der Verantwortliche selbst per OAuth und kann sie einzeln trennen. KI-Clients, die er über den Outcomet-MCP-Server anbindet, richtet er selbst ein und kann ihnen den Zugang jederzeit entziehen.

Trennung

- Produktiv- und Entwicklungsumgebung sind getrennte Datenbankprojekte, beide in der EU.
- Die Entwicklungsumgebung wird mit einer vollständigen Kopie der Produktivdaten befüllt, um Fehler unter realen Bedingungen nachzustellen. Für sie gelten dieselben Zugriffsregeln. Zugriff hat nur der Geschäftsführer.

Pseudonymisierung: Eingaben in Formularfeldern werden in Sitzungsaufzeichnungen maskiert. Eine Pseudonymisierung von Inhalten vor der KI-Verarbeitung findet derzeit nicht statt. Daten, die der Verantwortliche bereits pseudonymisiert einbringt, bleiben pseudonymisiert.

2 Integrität

Weitergabe

- Alle Verbindungen sind per TLS verschlüsselt: Browser, Schnittstellen und Verbindungen zu Unterauftragsverarbeitern.
- Gespeicherte Daten verschlüsselt Supabase mit AES-256.
- Inhalte gehen nur an die Unterauftragsverarbeiter aus Anlage B und dort nur über geschäftliche API-Zugänge, nie über Verbraucherprodukte.

Eingabekontrolle

- Von Nutzern angelegte Inhalte tragen Ersteller und Zeitpunkt der letzten Änderung. Daten aus Integrationen tragen ihre Herkunft. Ein vollständiges Änderungsprotokoll je Feld gibt es nicht.
- KI-Aufrufe werden mit Funktion, Modell, Workspace und Zeitpunkt protokolliert.
- Anmeldungen und Serverzugriffe protokollieren die Hosting-Anbieter.

3 Verfügbarkeit und Belastbarkeit

- Tägliche Datensicherung durch Supabase, sieben Tage vorgehalten.
- Der Verantwortliche kann seine Daten jederzeit exportieren.
- Fehler und Ausfälle meldet die Fehlerüberwachung (Sentry, EU) sofort.
- Schemaänderungen laufen über versionierte Migrationen im Quellcode-Repository.

4 Überprüfung und Bewertung

- Änderungen am Quellcode laufen über Pull Requests mit automatischer Prüfung und Code-Review vor dem Zusammenführen.
- Die Sicherheitshinweise des Datenbankanbieters (Supabase Advisor) werden regelmäßig geprüft.
- Diese Anlage und Anlage B werden bei jeder Änderung an Anbietern oder Datenflüssen aktualisiert, mindestens einmal im Jahr.

5 Auftragskontrolle

- Mit jedem Unterauftragsverarbeiter besteht ein Vertrag nach Art. 28 DSGVO, bei Übermittlung in Drittländer mit Standardvertragsklauseln oder auf Grundlage eines Angemessenheitsbeschlusses.
- Daten des Verantwortlichen werden nicht in private Konten oder in Werkzeuge ohne Auftragsverarbeitungsvertrag übertragen.
- Kein Unterauftragsverarbeiter darf die Daten zum Training von KI-Modellen verwenden.

6 Datenschutzverletzungen

- Verdacht auf eine Verletzung prüft der Geschäftsführer sofort.
- Meldung an den Verantwortlichen unverzüglich, spätestens 48 Stunden nach Kenntnis, nach Ziffer 9 des Vertrags.
- Kontakt: andy@crew.outcomet.app

B Anlage B · Unterauftragsverarbeiter · Stand 31. Oktober 2026

Die Datenbank mit allen Inhalten des Verantwortlichen liegt in der EU.

Kernbetrieb

ANBIETER	ZWECK	DATEN	ORT DER VERARBEITUNG	GRUNDLAGE FÜR DRITTLAND
Supabase Inc., USA	Datenbank, Anmeldung, Dateispeicher, Serverfunktionen	alle Konto- und Inhaltsdaten	EU (Paris); Entwicklungsumgebung EU (Frankfurt)	nicht erforderlich für die Speicherung; für Supportzugriffe aus den USA Standardvertragsklauseln
Netlify Inc., USA	Auslieferung der Anwendung; Weiterleitung der Fehlerberichte an Sentry	IP-Adresse, technische Anfragedaten, Fehlerberichte	weltweites Netz, Auslieferung vom nächstgelegenen Standort; Unternehmen in den USA	Standardvertragsklauseln
API Hero Ltd (Trigger.dev), Vereinigtes Königreich	Hintergrundverarbeitung, KI-Abläufe	Inhalte während der Verarbeitung	Ausführung EU (Frankfurt, AWS eu-central-1); Lauf- und Protokolldaten auf der Plattform des Anbieters, Standort nicht zugesichert	Standardvertragsklauseln
Resend Inc., USA	Versand und Empfang von E-Mails in Outcomet	E-Mail-Adresse, Nachrichteninhalt	Versand und Empfang EU (Irland, AWS eu-west-1); Konto- und Protokolldaten beim Anbieter in den USA möglich	Standardvertragsklauseln, EU-US Data Privacy Framework
Functional Software Inc. (Sentry), USA	Fehlerüberwachung, Sitzungsaufzeichnung mit maskierten Eingaben	technische Daten, Nutzerkennung, Bildschirmaufzeichnung einzelner Sitzungen	EU (Frankfurt)	Standardvertragsklauseln, EU-US Data Privacy Framework
Slack Technologies Ltd., Irland (Salesforce-Gruppe)	Kommunikation mit dem Verantwortlichen, wenn ein gemeinsamer Kanal vereinbart ist	Name, E-Mail-Adresse und Profil der Teilnehmer; Nachrichten und Dateien, die der Verantwortliche im Kanal teilt	USA (Datenhaltung des Anbieters)	Standardvertragsklauseln
Google Cloud EMEA Ltd., Irland (Google Workspace)	E-Mail, Kalender und Videotermine mit dem Verantwortlichen	Name und E-Mail-Adresse der Beteiligten; Inhalte von E-Mails und Terminen	EU und USA (Rechenzentren des Anbieters)	Standardvertragsklauseln
Granola Inc., USA	Notizen und Transkripte der Termine mit dem Verantwortlichen	Gesprächsinhalte; Namen und E-Mail-Adressen der Teilnehmer	USA	Standardvertragsklauseln

KI-Verarbeitung

Inhalte gehen ausschließlich über geschäftliche API-Zugänge. Keiner dieser Anbieter trainiert Modelle mit den Daten des Verantwortlichen.

ANBIETER	ZWECK	DATEN	ORT	SPEICHERUNG BEIM ANBIETER	GRUNDLAGE
Anthropic PBC, USA	Auswertung, Zusammenfassung, Assistent (Claude)	Feedback, Interviewinhalte, Produktinhalte, Chatverläufe	USA	bis zu 30 Tage zur Missbrauchserkennung	Standardvertragsklauseln
OpenAI Ireland Ltd., Irland, mit OpenAI OpCo, LLC, USA	Klassifikation, Metadaten, Embeddings für die Suche	Textinhalte	USA	bis zu 30 Tage zur Missbrauchserkennung	Standardvertragsklauseln
TypeSafe AI, Inc., USA	Klassifikation von Feedback, Content Sources und Änderungen (Modell „Jev“)	Feedbacktext, Name der meldenden Person, Transkript-Abschnitte; Name, E-Mail-Adresse, Rolle und Unternehmen der Gesprächsteilnehmer mit ihren Einstufungen und bis zu fünf früheren Signalen; Titel, Beschreibung und Dateinamen von Änderungen; Quelleninhalte	USA (AWS; Rechenknoten bei Modal, Nebius, CoreWeave)	auf den Rechenknoten keine Speicherung; für die Datenbank keine vertragliche Zusage zur Dauer	Standardvertragsklauseln Modul 2 und 3

Ausnahme nach Ziffer 3 · TypeSafe

TypeSafe darf aus den Anfragen gewonnene zusammenfassende Statistiken, Klassifikationen, Kennzahlen und Erkenntnisse für den eigenen Dienst und eigene Produkte verwenden (TypeSafe Master Customer Agreement § 4.3). Modelltraining mit den Inhalten ist ohne Zustimmung ausgeschlossen (§ 4.1). Die Ergebnisse der Klassifikation gehören dem Auftragsverarbeiter (§ 11) und werden nur im Workspace des Verantwortlichen gespeichert.

TypeSafe ist fester Bestandteil der Klassifikation in Outcomet. Mit Unterzeichnung dieses Vertrags stimmt der Verantwortliche dieser Ausnahme zu.

Dienste zum Lesen öffentlicher Websites

Diese Dienste erhalten nur Adressen öffentlicher Websites, keine Inhalte und keine personenbezogenen Daten des Verantwortlichen. Sie sind deshalb keine Unterauftragsverarbeiter. Die Angabe dient der Vollständigkeit.

ANBIETER	FUNKTION	SITZ
SideGuide Technologies, Inc. (Firecrawl)	Product Context und Competitor Context: Lesen der Website, die der Verantwortliche angibt	USA
Jina AI GmbH (Elastic)	wie Firecrawl, als Ersatzweg	Berlin
Microlink	Link-Vorschau für Content Sources	Spanien

Keine Unterauftragsverarbeiter

GitHub, Atlassian (Jira), HubSpot, Granola (als Integration des Verantwortlichen), LinkedIn und Discord verbindet der Verantwortliche selbst per OAuth. Sie handeln gegenüber dem Verantwortlichen als eigene Anbieter. Die Verbindung lässt sich jederzeit einzeln trennen. Dasselbe gilt für KI-Clients, die der Verantwortliche über den Outcomet-MCP-Server anbindet: Sie erhalten nur die Daten, die der Verantwortliche über sie abfragt.

Dienstleister der Unterauftragsverarbeiter

Jeder Anbieter oben setzt eigene Dienstleister ein und veröffentlicht sie. Maßgeblich sind deren Listen, unter anderem:

- Supabase: https://supabase.com/legal/customer-resources/subprocessor-list
- Sentry: https://sentry.io/legal/subprocessors/
- Resend: https://resend.com/legal/subprocessors
- OpenAI: https://openai.com/policies/sub-processor-list/
- TypeSafe: https://trust.typesafe.ai/subprocessors
- Anthropic, Netlify, Trigger.dev: über die jeweilige Datenschutz- bzw. DPA-Seite des Anbieters