

Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO

Stand: Oktober 2026 · ersetzt das Data Processor Agreement vom 10.01.2023

zwischen dem Kunden als Verantwortlichem (der „Auftraggeber“)
und der Founders1 GmbH, Sitz Berlin (Amtsgericht Charlottenburg, HRB 234373 B), Geschäftsanschrift
Berger Straße 224, 60385 Frankfurt am Main, als Auftragsverarbeiter (der „Auftragnehmer“).

Präambel

- A.** Dieser Auftragsverarbeitungsvertrag („AVV“) ist Bestandteil des Vertrags über die Nutzung der BetterCo-Plattform, bestehend aus Bestellformular und Nutzungsbedingungen (der „Hauptvertrag“). Er wird zusammen mit dem Hauptvertrag in Textform abgeschlossen und endet mit ihm.
- B.** Die Begriffe „personenbezogene Daten“, „Verarbeitung“, „betroffene Person“ und „Verletzung des Schutzes personenbezogener Daten“ haben die Bedeutung der Verordnung (EU) 2016/679 („DSGVO“).
- C.** „Mandatsdaten“ sind die personenbezogenen Daten, die der Auftraggeber bei der Nutzung der Plattform zu seinen Mandanten, Klienten oder Kunden und den mit ihnen verbundenen Personen verarbeitet, einschließlich Identifikationsdaten, Ausweisdokumenten, Beteiligungsstrukturen, Screening-Ergebnissen und Risikobewertungen. „Berufsgeheimnis“ bezeichnet die Pflichten nach § 203 StGB und den berufsrechtlichen Vorschriften, insbesondere § 43e BRAO, § 26a BNotO, § 62a StBerG und § 50a WPO.
- D.** Für die Verarbeitung von Konto- und Abrechnungsdaten, Support-Korrespondenz und technischen Betriebsprotokollen ist der Auftragnehmer selbst Verantwortlicher; sie ist nicht Gegenstand dieses AVV.

1 Gegenstand, Dauer, Art und Zweck

- 1.1** Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich, um die im Hauptvertrag beschriebenen Leistungen zu erbringen. Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 3.
- 1.2** Ist der Auftragnehmer nach Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2 Weisungen

- 2.1** Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf die Übermittlung in ein Drittland. Als Weisung gilt der Hauptvertrag einschließlich der Nutzung der Plattform durch den Auftraggeber und seine Nutzer. Einzelweisungen erfolgen in Textform.
- 2.2** Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung bis zur Klärung aussetzen.
- 2.3** Der Auftragnehmer verarbeitet die Daten nicht für eigene Zwecke und verwendet sie insbesondere nicht zum Training von Modellen der künstlichen Intelligenz.
- 2.4** Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

3 Vertraulichkeit

- 3.1** Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind; die Verpflichtung gilt über das Ende ihrer Tätigkeit hinaus. Für Mandatsdaten gilt zusätzlich Ziffer 13.

- 3.2** Verlangt eine Behörde oder ein Gericht die Herausgabe von Daten des Auftraggebers, unterrichtet der Auftragnehmer den Auftraggeber vorab, soweit dies rechtlich zulässig ist. Stammt die Anordnung von einer Stelle außerhalb der Europäischen Union, weist er auf Art. 48 DSGVO hin und gibt Daten nur heraus, soweit eine Rechtsgrundlage nach Unionsrecht besteht.

4 Technische und organisatorische Maßnahmen

- 4.1** Der Auftragnehmer trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Anlage 1 ist Bestandteil dieses AVV.
- 4.2** Der Auftragnehmer darf die Maßnahmen fortentwickeln. Das Schutzniveau der Anlage 1 darf dabei nicht unterschritten werden. Wesentliche Änderungen zeigt er dem Auftraggeber vorab in Textform an.
- 4.3** Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen mindestens jährlich und dokumentiert das Ergebnis.

5 Verletzungen des Schutzes personenbezogener Daten

- 5.1** Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten, die dessen Daten betrifft, unverzüglich, spätestens innerhalb von 48 Stunden, nachdem der Auftragnehmer Kenntnis erlangt hat.
- 5.2** Die Meldung enthält, soweit bekannt, die Art der Verletzung mit Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, eine Kontaktstelle, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Betrifft die Verletzung Mandatsdaten, weist die Meldung ausdrücklich darauf hin. Nicht sofort verfügbare Angaben werden ohne unangemessene Verzögerung nachgereicht.
- 5.3** Der Auftragnehmer dokumentiert jede Verletzung und unterstützt den Auftraggeber bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

6 Orte der Verarbeitung

- 6.1** Der Auftragnehmer speichert und verarbeitet die Daten des Auftraggebers einschließlich der Sicherungskopien ausschließlich im Europäischen Wirtschaftsraum; dies gilt auch für den Wiederanlauf im Notfall. Ausgenommen sind allein Supportzugriffe nach Ziffer 6.2. Die Orte je Dienst nennt Anlage 2.
- 6.2** Microsoft und MongoDB haben keinen ständigen Zugriff auf die Daten. Zugriffe ihres Personals sind technisch gesperrt (Customer Lockbox für Microsoft Azure, Sperre des Supportzugriffs in MongoDB Atlas) und nur in kritischen Störungs- oder Sicherheitsfällen, nach vorheriger Freigabe durch den Auftragnehmer im Einzelfall und zeitlich befristet möglich. Erfolgt ein solcher Zugriff aus einem Drittland, beruht er auf dem EU-US Data Privacy Framework (Art. 45 DSGVO) oder den Standardvertragsklauseln (Art. 46 DSGVO) in den Verträgen mit den Anbietern. Der Auftragnehmer protokolliert jede Freigabe und stellt dem Auftraggeber die Bewertung dieser Zugriffe (Transfer Impact Assessment) auf Anfrage zur Verfügung.
- 6.3** Jede darüber hinausgehende Übermittlung in ein Drittland bedarf einer Weisung des Auftraggebers in Textform und der Einhaltung des Kapitels V DSGVO.

7 Unterauftragsverarbeiter

- 7.1** Der Auftraggeber genehmigt die Beauftragung der in Anlage 2 genannten Unterauftragsverarbeiter. Anlage 2 ist zugleich unter betterco.ai/subprocessors veröffentlicht.
- 7.2** Der Auftragnehmer informiert den Auftraggeber über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens 30 Tage vorher in Textform. Der Auftraggeber kann innerhalb von 30 Tagen nach Zugang aus sachlichem Grund, insbesondere aus Gründen des Datenschutzes oder des Berufsgeheimnisses, in Textform widersprechen. Bis zu einer Einigung setzt der Auftragnehmer den neuen Unterauftragsverarbeiter für Daten des widersprechenden Auftraggebers nicht ein. Ist dies nicht möglich oder kommt innerhalb von 30 Tagen nach dem Widerspruch keine Einigung zustande, kann der Auftraggeber diesen AVV und den Hauptvertrag zum Zeitpunkt des Einsatzes kündigen; im Voraus gezahlte Entgelte für die Zeit danach werden anteilig erstattet.

- 7.3** Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die ihn nach diesem AVV treffen, und bleibt dem Auftraggeber für dessen Einhaltung voll verantwortlich. Erhält ein Unterauftragsverarbeiter Mandatsdaten, verpflichtet er ihn zusätzlich nach Ziffer 13.
- 7.4** Nicht als Unterauftragsverarbeitung gelten Nebenleistungen, bei denen der Dienstleister keinen Zugriff auf die Daten des Auftraggebers erhält, etwa Telekommunikationsleistungen.

8 Rechte betroffener Personen

- 8.1** Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO, insbesondere bei Auskunft, Berichtigung, Einschränkung, Löschung und Datenübertragbarkeit.
- 8.2** Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er das Anliegen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst.

9 Unterstützung, Nachweise und Prüfungen

- 9.1** Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, einschließlich Datenschutz-Folgenabschätzungen und vorheriger Konsultationen.
- 9.2** Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung dieses AVV zur Verfügung. Da er derzeit keine eigene Zertifizierung führt, legt er dazu insbesondere Anlage 1, das Ergebnis der jährlichen Wirksamkeitsprüfung und die Zertifizierungen seiner Unterauftragsverarbeiter vor.
- 9.3** Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann Überprüfungen einschließlich Inspektionen durchführen. Regelprüfungen sind mindestens 30 Tage vorher anzukündigen, finden zu üblichen Geschäftszeiten statt und höchstens einmal je Vertragsjahr. Für Microsoft und MongoDB erfolgt der Nachweis über deren Zertifizierungen und Prüfberichte nach Ziffer 9.2; Inspektionen in deren Rechenzentren sind ausgeschlossen.
- 9.4** Ohne Vorlaufzeit und ohne Anrechnung auf Ziffer 9.3 kann der Auftraggeber prüfen, wenn eine Verletzung des Schutzes personenbezogener Daten gemeldet wurde, eine Aufsichtsbehörde oder berufsrechtliche Stelle es verlangt, ein Unterauftragsverarbeiter für Mandatsdaten gewechselt wird oder konkrete Anhaltspunkte für einen Verstoß gegen diesen AVV bestehen.
- 9.5** Prüfungen erfolgen unter Rücksicht auf den Geschäftsbetrieb des Auftragnehmers und die Vertraulichkeit der Daten anderer Kunden.

10 Pflichten des Auftraggebers

- 10.1** Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlagen einschließlich derjenigen nach Art. 9 und 10 DSGVO und für die Information der betroffenen Personen. Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

11 Löschung und Rückgabe

- 11.1** Nach Ende des Hauptvertrags löscht der Auftragnehmer die Daten des Auftraggebers oder gibt sie nach dessen Wahl heraus. Der Auftraggeber teilt seine Wahl innerhalb von 30 Tagen nach Vertragsende mit; trifft er keine Wahl, wird gelöscht. Vor der Löschung weist der Auftragnehmer auf die Möglichkeit des Exports hin.
- 11.2** Löschung oder Herausgabe erfolgen innerhalb von 30 Tagen nach Zugang der Wahl oder Ablauf der Wahlfrist. Der Auftragnehmer bestätigt die Löschung in Textform mit einem Löschprotokoll, das Datum, Umfang und betroffene Systeme ausweist.
- 11.3** Daten in Sicherungskopien werden mit dem regelmäßigen Sicherungsumlauf entfernt, spätestens nach 12 Monaten, und bis dahin nicht in den Produktivbetrieb zurückgespielt.
- 11.4** Eine längere Aufbewahrung erfolgt nur, soweit Unionsrecht oder das Recht eines Mitgliedstaats sie vorschreibt; der Auftragnehmer teilt Rechtsgrundlage und Dauer mit.

12 Verarbeitung mit künstlicher Intelligenz

- 12.1 Der Auftragnehmer setzt ein Sprachmodell ein, um hochgeladene Dokumente auszulesen und Angaben vorzubefüllen. Die Verarbeitung erfolgt ausschließlich über den in Anlage 2 genannten Azure OpenAI Service in einer auf die EU-Datenzone beschränkten Bereitstellung.
- 12.2 Ein- und Ausgabedaten werden nicht zum Training oder zur Verbesserung von Modellen verwendet.
- 12.3 Ausgaben sind gekennzeichnete Vorschläge, die erst nach Bestätigung oder Korrektur durch einen Menschen übernommen werden. Entscheidungen, insbesondere nach dem Geldwäschegesetz, trifft der Auftraggeber.
- 12.4 Der Einsatz eines weiteren KI-Dienstes ist eine Änderung der Unterauftragsverarbeiter nach Ziffer 7.

13 Berufsgeheimnis

- 13.1 Soweit der Auftraggeber Berufsgeheimnisträger ist oder Daten verarbeitet, die einem Berufsgeheimnis unterliegen, ist der Auftragnehmer mitwirkende Person im Sinne des § 203 Abs. 3 StGB. Es gilt ergänzend die Vereinbarung zur beruflichen Verschwiegenheit.
- 13.2 Der Auftragnehmer ist verpflichtet, alle Personen, die Zugang zu Mandatsdaten erhalten, vor Aufnahme ihrer Tätigkeit in Textform zur Verschwiegenheit zu verpflichten und über die Strafbarkeit nach §§ 203, 204 StGB zu belehren. Unterauftragsverarbeiter, die Mandatsdaten erhalten, hat er in gleicher Weise zu verpflichten, einschließlich der Verpflichtung ihrer eigenen Unterauftragnehmer. Alle Unterauftragsverarbeiter, die Mandatsdaten erhalten, sind entsprechend verpflichtet. Ausgenommen sind Microsoft und MongoDB, die eine gesonderte Verpflichtung nach § 203 StGB nicht anbieten; sie stellen Infrastruktur bereit, sind nach ihren Auftragsverarbeitungsbedingungen zur Vertraulichkeit verpflichtet und erhalten Zugriff nur nach Ziffer 6.2.
- 13.3 Der Auftragnehmer beschränkt den Zugang zu Mandatsdaten auf das für die Leistung Erforderliche, protokolliert Zugriffe und führt ein Verzeichnis der Verpflichtungen, dessen Stand er dem Auftraggeber auf Verlangen offenlegt.

14 Haftung

- 14.1 Für die Haftung der Parteien untereinander gelten die Bestimmungen des Hauptvertrags. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

15 Schlussbestimmungen

- 15.1 Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag geht für Fragen des Datenschutzes dieser AVV vor.
- 15.2 Änderungen dieses AVV bedürfen der Textform. Der Auftragnehmer kann den AVV mit Wirkung für die Zukunft anpassen, soweit dies wegen einer Änderung der Rechtslage erforderlich ist und das Schutzniveau nicht gesenkt wird; für das Verfahren gilt die Änderungsregelung der Nutzungsbedingungen entsprechend. Änderungen der Unterauftragsverarbeiter richten sich ausschließlich nach Ziffer 7.
- 15.3 Werden die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet, unterrichtet der Auftragnehmer den Auftraggeber unverzüglich.
- 15.4 Es gilt deutsches Recht. Gerichtsstand ist Berlin, soweit der Hauptvertrag nichts anderes bestimmt. Maßgeblich ist die deutsche Fassung.
- 15.5 Die Unwirksamkeit einzelner Bestimmungen berührt die Wirksamkeit der übrigen nicht.

Anlagen

Anlage	Inhalt	Fundstelle
Anlage 1	Technische und organisatorische Maßnahmen	betterco.ai/technische-und-organisatorische-massnahmen
Anlage 2	Unterauftragsverarbeiter und Orte der Verarbeitung	betterco.ai/subprocessors

Anlage	Inhalt	Fundstelle
Anlage 3	Gegenstand und Umfang der Verarbeitung	in diesem Dokument

Anlage 3 – Gegenstand und Umfang der Verarbeitung

1 Gegenstand und Dauer

Gegenstand ist die Bereitstellung und der Betrieb der Plattform BetterCo als Dienst über das Internet, einschließlich der Schnittstellen und der vom Auftraggeber gebuchten Datenpakete. Die Plattform unterstützt den Auftraggeber bei der Identifizierung von Vertragspartnern und der Erfüllung seiner Sorgfaltspflichten nach dem Geldwäschegesetz und, soweit anwendbar, nach berufsrechtlichen Vorgaben. Die Verarbeitung dauert so lange wie der Hauptvertrag; Rückgabe und Löschung richten sich nach Ziffer 11 des AVV. Aufbewahrungspflichten des Auftraggebers, insbesondere nach § 8 Abs. 4 GWG, erfüllt dieser in eigener Verantwortung.

2 Art und Zweck der Verarbeitung

Modul	Art der Verarbeitung	Zweck
Onboarding: Selbstauskunft, Konflikt- und Compliance-Prüfung, Anlage von Mandanten, Aktenanlage	Erheben, Strukturieren, Speichern, Anzeigen	Identifizierung des Vertragspartners und der wirtschaftlich Berechtigten; Dokumentation der Mandatsbeziehung
Vollmachten, Zustimmungen, Beschlüsse	Erheben, Speichern, Bereitstellen zur Unterzeichnung	Dokumentation von Vertretungs- und Zustimmungsverhältnissen
Risikomanagement	Auswerten, Bewerten, Zusammenführen	Risikoeinstufung und laufende Überwachung
Identitätsprüfung und Signatur, einschließlich Videoidentifizierung	Erheben, Abgleichen einschließlich biometrischem Gesichtsabgleich, Speichern des Ergebnisses	Feststellung und Nachweis der Identität
Datenpakete Stammdaten und Stammdaten GwG	Abruf aus öffentlichen Registern, Vorbefüllen, Überwachen auf Änderungen; Ermitteln der Beteiligungsstruktur	Richtigkeit der Angaben; Pflichten nach §§ 10 ff. GWG
Datenpaket Compliance	Abgleich gegen Sanktions-, PEP- und Negativpresselisten, einmalig oder fortlaufend	Sanktions- und Reputationsprüfung
Auslesen von Dokumenten mit einem Sprachmodell	Auslesen hochgeladener Dokumente; Vorschläge mit Quellenangabe; ärztliche Unterlagen werden nur als solche erkannt und nicht inhaltlich ausgewertet	Vorbefüllung; Übernahme erst nach Prüfung durch einen Menschen
Betrieb, Sicherheit, Support	Protokollieren, Sichern, Fehlerbehebung	Verfügbarkeit, Nachvollziehbarkeit, Wiederherstellbarkeit

3 Art der personenbezogenen Daten

Gruppe	Umfasst
Stammdaten	Vorname, Nachname, Geburtsdatum und -ort, Staatsangehörigkeit, Anschrift, Funktion
Kontaktdaten	E-Mail-Adresse, Telefonnummer
Ausweisdaten	Art, Nummer, ausstellende Behörde und Gültigkeit des Ausweisdokuments; Abbild des Dokuments; Ergebnis der Identitätsprüfung
Biometrische Daten	Gesichtsbild aus dem Ausweisdokument und aus der Live-Aufnahme sowie deren automatisierter Abgleich
Kennnummern	Umsatzsteuer-Identifikationsnummer, Registernummern; Steuer-Identifikationsnummer nur, soweit der Auftraggeber sie nach § 139b Abs. 2 AO verarbeiten darf
Beteiligungs- und Strukturdaten	Gesellschafterstellung, Anteilshöhe, Stellung als wirtschaftlich Berechtigter, Vertretungsverhältnisse

Gruppe	Umfasst
Screening-Ergebnisse	Treffer und Nicht-Treffer gegen Sanktions- und Beobachtungslisten, PEP-Eigenschaft, Negativpresse mit Fundstellen
Mandats- und Vertragsdaten	Gegenstand der Mandatsbeziehung, soweit für die Risikoeinstufung erforderlich; hochgeladene Unterlagen und deren Inhalte
Vermögens- und Wirtschaftsdaten	Bankverbindung, Einkommens- und Schuldenangaben, Immobilien- und Fahrzeugeigentum, Grundbuchdaten, Sozialversicherungsnummer – nur, soweit der vom Auftraggeber eingesetzte Fragebogen sie erhebt
Bearbeitungsprotokolle	Bearbeiter, Zeitpunkt und Art von Eingaben, Änderungen und Bestätigungen an Mandatsdaten
Zugangsdaten der Auskunftspersonen	E-Mail-Adresse, technischer Zugangsschlüssel mit Ablaufzeitpunkt, Einmalcode, Zugriffszeitpunkte, IP-Adresse

Besondere Kategorien (Art. 9 DSGVO). Biometrische Daten werden bei der Identitätsprüfung verarbeitet, soweit der Auftraggeber dieses Verfahren nutzt. Gesundheitsdaten können in hochgeladenen ärztlichen Unterlagen enthalten sein; diese werden gespeichert, aber nicht inhaltlich ausgewertet. Weitere besondere Kategorien können in Screening-Treffern aus der Negativpresse enthalten sein; sie werden nicht gesondert ausgewertet.

Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) können in Treffern aus dem Negativpresse-Screening und in hochgeladenen behördlichen Unterlagen, etwa Führungszeugnissen, enthalten sein. Ein Treffer auf einer Sanktionsliste ist für sich genommen keine Angabe über eine Straftat. Die Verarbeitung erfolgt auf Weisung des Auftraggebers zur Erfüllung seiner Pflichten nach dem Geldwäschegesetz.

4 Kategorien betroffener Personen

Kategorie	Beschreibung
Interessenten	natürliche Personen, zu denen der Auftraggeber eine Mandatsbeziehung prüft
Mandanten und Klienten	natürliche Personen, die der Auftraggeber identifiziert
Auskunftspersonen	Personen, die über einen befristeten Link Angaben für einen Interessenten oder Mandanten eintragen, auch wenn sie selbst weder Vertragspartner noch wirtschaftlich Berechtigter sind
Gesetzliche Vertreter und Bevollmächtigte	Geschäftsführer, Vorstände, Prokuristen und Bevollmächtigte der Mandanten
Wirtschaftlich Berechtigte	natürliche Personen hinter juristischen Personen und Rechtsgestaltungen
Gesellschafter und Beteiligte	soweit sie in der Beteiligungsstruktur erscheinen
Beschäftigte des Auftraggebers	als Bearbeiter von Mandatsdaten
Dritte aus Unterlagen	Personen, die in hochgeladenen Dokumenten genannt sind

5 Orte der Verarbeitung

Die Daten werden im Europäischen Wirtschaftsraum gespeichert und verarbeitet: Anwendung und Dateispeicher auf Microsoft Azure in der Region Germany West Central (Frankfurt am Main), die Datenbank bei MongoDB Atlas in derselben Region, das Sprachmodell in der EU-Datenzone. Die Unterauftragsverarbeiter mit Sitz, Zweck und Ort der Verarbeitung nennt Anlage 2; zu Zugriffen aus Drittländern gilt Ziffer 6.2 des AVV.