

Vertrag zur Auftragsverarbeitung

Version 1.1 · gültig ab 26.08.2026 · [English version](#)

Dieser Vertrag (nachfolgend „AVV“) konkretisiert die Pflichten nach Art. 28 DS-GVO für die Verarbeitung personenbezogener Daten, die die **becom Systemhaus GmbH & Co. KG**, Am Feldkreuz 16a, 35578 Wetzlar (nachfolgend „Auftragnehmer“) im Rahmen des Dienstes **Astreo** für den Kunden (nachfolgend „Auftraggeber“) durchführt.

Der Auftraggeber ist **Verantwortlicher** im Sinne des Art. 4 Nr. 7 DS-GVO, der Auftragnehmer ist **Auftragsverarbeiter** im Sinne des Art. 4 Nr. 8 DS-GVO. Der AVV ist Anlage zu den Allgemeinen Geschäftsbedingungen und kommt bei der Einrichtung des Kontos in elektronischer Form zustande (Art. 28 Abs. 9 Satz 2 DS-GVO); Zeitpunkt, bestätigende Person und Fassung werden protokolliert. Auf Wunsch stellt der Auftragnehmer eine unterschriebene Ausfertigung zur Verfügung.

§ 0 Was dieser Vertrag *nicht* regelt

Damit die Rollen nicht durcheinandergeraten, drei Abgrenzungen vorab:

- **Vertrags- und Rechnungsdaten des Auftraggebers** (Firmenname, Anschrift, Umsatzsteuer-Identifikationsnummer, Zahlungsvorgänge) verarbeitet der Auftragnehmer **als eigener Verantwortlicher**, nicht in dessen Auftrag. Dafür gilt die Datenschutzerklärung, nicht dieser Vertrag. Der dort genannte Zahlungsdienstleister ist deshalb *kein* Unterauftragsverarbeiter im Sinne von § 5.
- **Die vom Auftraggeber angebundenen Postfächer** (z. B. Microsoft 365, Google Workspace, ein IMAP-Server) sind Dienste, die der Auftraggeber selbst beauftragt hat. Deren Anbieter sind **keine** Unterauftragsverarbeiter des Auftragnehmers. Astreo ist ein Client: die Mails bleiben beim Anbieter des Auftraggebers.
- **Beschäftigtendaten des Auftraggebers**, die dieser selbst in Astreo anlegt (Nutzerkonten seines Teams), verarbeitet der Auftragnehmer im Auftrag - sie sind von diesem Vertrag umfasst (Anlage A).

§ 1 Gegenstand, Umfang und Dauer

Gegenstand der Verarbeitung ist die Erbringung des Dienstes Astreo gemäß AGB und gewählter Edition. Art, Zweck und Umfang der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen ergeben sich abschließend aus Anlage A.

Der AVV gilt für die Dauer des Hauptvertrags. Er endet mit diesem, jedoch nicht vor Erfüllung der Pflichten aus § 8 (Löschung und Rückgabe).

§ 2 Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DS-GVO). Die Nutzung des Dienstes im vertraglich vorgesehenen Rahmen - insbesondere jede Handlung, die der Auftraggeber oder seine Nutzer in der Anwendung

vornehmen - gilt als erteilte Weisung. Weisungen darüber hinaus bedürfen der Textform an datenschutz@becom.net.

Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber unverzüglich. Er ist berechtigt, die Ausführung auszusetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

Verarbeitet der Auftragnehmer Daten aufgrund einer **rechtlichen Verpflichtung** (Art. 28 Abs. 3 lit. a Halbsatz 2 DS-GVO), unterrichtet er den Auftraggeber vor der Verarbeitung, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 3 Vertraulichkeit

Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DS-GVO). Die Verpflichtung wirkt über das Ende des jeweiligen Beschäftigungsverhältnisses hinaus.

Ein Zugriff auf Inhalte des Auftraggebers erfolgt **nicht routinemäßig**, sondern nur, soweit es zur Erbringung, Fehlerbehebung oder Sicherheit des Dienstes erforderlich ist - und dann nach dem Grundsatz der Erforderlichkeit. Mail-Inhalte werden nicht protokolliert und nicht zu Werbe- oder Trainingszwecken ausgewertet.

§ 4 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die nach Art. 32 DS-GVO erforderlichen Maßnahmen. Der Stand zum Zeitpunkt dieses Vertrags ist in Anlage B beschrieben. Die Maßnahmen unterliegen dem technischen Fortschritt; der Auftragnehmer darf sie fortentwickeln, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden in Anlage B nachgeführt.

§ 5 Unterauftragsverarbeiter

Der Auftraggeber erteilt eine **allgemeine Genehmigung** zur Hinzuziehung weiterer Auftragsverarbeiter (Art. 28 Abs. 2 Satz 2 DS-GVO). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage C abschließend aufgeführt.

Zieht der Auftragnehmer einen weiteren Unterauftragsverarbeiter hinzu oder tauscht er einen bestehenden aus, teilt er dies dem Auftraggeber **unverzüglich, spätestens mit der Umstellung**, in Textform an die hinterlegte Rechnungs-E-Mail-Adresse mit und führt die Änderung in Anlage C nach. Der Auftraggeber kann der Änderung innerhalb von **zwei Wochen** ab Zugang aus einem datenschutzrechtlichen Grund widersprechen. Kommt keine Einigung zustande, steht dem Auftraggeber ein Sonderkündigungsrecht zu.

Bis zum 26.08.2026 sah dieser Vertrag eine Ankündigung vier Wochen vor der Umstellung vor. Diese Frist stand einer schnellen Verbesserung im Weg: Wird erkannt, dass ein Dienstleister ungeeignet ist - etwa weil er außerhalb der EU verarbeitet -, müsste der Zustand vier Wochen fortbestehen, bevor er beendet

werden darf. Der Auftraggeber verliert durch die Änderung keine Rechte; Widerspruch und Sonderkündigung bleiben unverändert. Er erfährt von der Umstellung zeitgleich statt vorher.

Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter auf Pflichten, die den hier vereinbarten entsprechen, und bleibt dem Auftraggeber gegenüber für dessen Verhalten verantwortlich (Art. 28 Abs. 4 DS-GVO).

§ 6 Betroffenenrechte

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Betroffenenrechten (Art. 28 Abs. 3 lit. e DS-GVO). Auskunft, Berichtigung, Export und Löschung sind für den Auftraggeber weitestgehend **selbst durchführbar**; wo das nicht ausreicht, unterstützt der Auftragnehmer auf Anfrage.

Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst.

§ 7 Unterstützung, Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Art. 32 bis 36 DS-GVO, soweit dies angesichts der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen möglich ist (Art. 28 Abs. 3 lit. f DS-GVO).

Eine Verletzung des Schutzes personenbezogener Daten meldet der Auftragnehmer dem Auftraggeber **unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung**, an die hinterlegte Rechnungs-E-Mail-Adresse. Die Meldung enthält, soweit bekannt: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen sowie eine Kontaktstelle. Sind die Angaben nicht vollständig verfügbar, werden sie unverzüglich nachgereicht. Die Meldung an die Aufsichtsbehörde (Art. 33) und an betroffene Personen (Art. 34) obliegt dem Auftraggeber.

§ 8 Löschung und Rückgabe

Während der Vertragslaufzeit kann der Auftraggeber die im Dienst entstandenen Daten jederzeit selbst exportieren. Mails verbleiben ohnehin im Postfach des Auftraggebers - Astreo ist ein Client und kein Postfachanbieter.

Nach Beendigung des Vertrags löscht der Auftragnehmer die im Auftrag verarbeiteten Daten **innerhalb von 30 Tagen**, sofern der Auftraggeber nicht zuvor eine Herausgabe verlangt hat und soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Daten in verschlüsselten Sicherungskopien werden mit dem Ablauf der Sicherungsrotation überschrieben, spätestens nach 90 Tagen; bis dahin bleiben sie von der Verarbeitung ausgenommen.

§ 9 Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind, und ermöglicht Überprüfungen (Art. 28 Abs. 3 lit. h DS-GVO). Der Nachweis kann erbracht werden durch Auskunft, durch die Vorlage dieser Anlagen in aktueller Fassung oder durch Bescheinigungen unabhängiger Stellen.

Genügt das im Einzelfall nicht, kann der Auftraggeber nach Ankündigung mit einer Frist von vier Wochen zu üblichen Geschäftszeiten eine Prüfung vor Ort durchführen oder durchführen lassen - in der Regel einmal jährlich, bei konkretem Anlass auch häufiger. Der Prüfer darf kein Wettbewerber des Auftragnehmers sein und ist zur Verschwiegenheit verpflichtet. Der Betriebsablauf darf nicht mehr als notwendig beeinträchtigt werden.

§ 10 Ort der Verarbeitung

Die Verarbeitung findet ausschließlich in der **Europäischen Union** statt. Eine Übermittlung in ein Drittland erfolgt nicht. Sollte sie künftig erforderlich werden, geschieht das nur unter den Voraussetzungen der Art. 44 ff. DS-GVO und nach dem Verfahren aus § 5.

§ 11 Schlussbestimmungen

Bei Widersprüchen zwischen diesem AVV und den AGB gehen die Regelungen dieses AVV **vor**, soweit es um die Verarbeitung personenbezogener Daten im Auftrag geht.

Änderungen dieses Vertrags teilt der Auftragnehmer mindestens vier Wochen vor Wirksamwerden mit. Änderungen, die die Rechte des Auftraggebers einschränken, bedürfen seiner Zustimmung; im Übrigen gilt das Verfahren der AGB. Die Fassung, der der Auftraggeber zugestimmt hat, ist in seinem Konto einsehbar.

Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. Es gilt deutsches Recht.

Anlage A - Beschreibung der Verarbeitung

Gegenstand und Zweck: Bereitstellung eines webbasierten E-Mail-Clients mit Team-Funktionen (geteiltes Postfach, Zuweisung, interne Notizen, Aufgaben, Auswertung) und optionalen KI-Hilfsfunktionen, ausschließlich zur Erbringung des Dienstes.

Art der Verarbeitung: Erheben, Speichern, Ordnen, Auslesen, Verwenden, Übermitteln an das vom Auftraggeber angebundene Postfach, Einschränken, Löschen.

Arten personenbezogener Daten:

- **Nutzerkonten des Auftraggebers:** Name, E-Mail-Adresse, Rolle und Rechte, Farbe, Geschäftszeiten, Anmeldedaten (Passwort-Hash, TOTP-Geheimnis), Sitzungen, Zeitpunkt der letzten Aktivität.
- **Mail-Verkehr der angebundenen Postfächer:** Absender, Empfänger, Betreff, Datum, Nachrichtentext, Anhänge, Kopfzeilen und Ordnerzuordnung.

- **Im Dienst entstehende Daten:** Zuweisungen, Vorgangsstatus, interne Notizen, Aufgaben, Kennzeichnungen, Verlaufsprotokoll (wer wann zugewiesen, geantwortet, geschlossen hat), Antwortkennzahlen, Vorlagen, Signaturen, Filter, Verteilerlisten.
- **Kontakte und Kalender,** soweit der Auftraggeber diese Funktionen nutzt.
- **Zugangsdaten zu Postfächern** (OAuth-Tokens, IMAP/SMTP-Kennwörter), verschlüsselt gespeichert.
- **Protokolldaten** zum Betrieb (Zeitpunkt, IP-Adresse, Vorgangs-Kennungen) - **ohne** Mail-Inhalte.

Kategorien betroffener Personen: Beschäftigte und beauftragte Personen des Auftraggebers (Nutzer des Dienstes) sowie dessen Kommunikationspartner (Absender und Empfänger der Mails, Kontakte).

Besondere Kategorien (Art. 9 DS-GVO): nicht vorgesehen. Ob solche Daten im Mail-Verkehr enthalten sind, bestimmt allein der Auftraggeber; der Auftragnehmer wertet Inhalte nicht aus.

Dauer: für die Laufzeit des Hauptvertrags, danach nach § 8.

Anlage B - Technische und organisatorische Maßnahmen (Art. 32 DS-GVO)

Vertraulichkeit

- **Zutritt:** Betrieb in Rechenzentren der netcup GmbH in Nürnberg; Zutrittskontrolle, Videoüberwachung und Zutrittsprotokollierung obliegen dem Rechenzentrumsbetreiber.
- **Zugang:** Anmeldung über Google-/Microsoft-SSO, Login-Link oder Passwort; Passwort-Anmeldung **nur mit zweitem Faktor** (TOTP). Anmeldeversuche sind je Konto und je IP-Adresse begrenzt. Sitzungen sind einzeln und gesammelt widerrufbar; Sitzungs-Cookies sind *httpOnly, secure* und *SameSite*.
- **Zugriff:** Rollen- und Rechtemodell je Team (Betrachter, Mitglied, Administrator, Inhaber) mit benannten Aktionsrechten für Zuweisen, Schließen, Verschieben, Spam und Löschen; endgültiges Löschen nur für Administratoren.
- **Trennung:** Mandantentrennung an einer zentralen Zugriffsschicht; jede Abfrage wird auf den angemeldeten Nutzer und dessen Teams eingegrenzt. Keine Datenbankabfrage umgeht diesen Filter.
- **Verschlüsselung:** Übertragung ausschließlich über TLS; Zugangsdaten zu Postfächern und OAuth-Tokens **AES-256-GCM verschlüsselt at rest**; Sicherungskopien verschlüsselt.

Integrität

- Weitergabekontrolle: Verbindungen zu Postfächern und KI-Diensten nur über TLS; keine Übermittlung an unbeteiligte Dritte.
- Eingabekontrolle: Verlaufsprotokoll am Vorgang (Zuweisung, Statuswechsel, Notiz, Verschieben, Spam) und gesondertes, dauerhaftes Protokoll über endgültige Löschungen.
- Anhänge werden vor der Auslieferung auf Schadsoftware geprüft.

Verfügbarkeit und Belastbarkeit

- Tägliche verschlüsselte Sicherung von Datenbank und Konfiguration, mit automatischer Überwachung von Alter und Größe der Sicherung und Alarmierung per E-Mail bei Ausbleiben.
- Überwachung der Dienste; getrennte Umgebungen für Betrieb und Entwicklung.

Verfahren zur Überprüfung und Bewertung

- Datenschutz durch Voreinstellung: Mail-Inhalte werden nicht protokolliert; Protokolldaten enthalten keine Inhalte; KI-Funktionen erzeugen stets nur einen bearbeitbaren Entwurf und versenden nie selbsttätig.
- Auftragskontrolle: schriftliche Weisungen, Verpflichtung der Unterauftragsverarbeiter nach Art. 28 Abs. 4 DS-GVO, dokumentierte Prüfung vor Beauftragung.
- Löschkonzept: Selbstbedienung für Konto- und Datenlöschung, Kaskadenlöschung abhängiger Daten, protokollierte endgültige Löschung.

Anlage C - Unterauftragsverarbeiter

Stand: 26.08.2026. Änderungen richten sich nach § 5.

- **netcup GmbH**, Daimlerstraße 25, 76185 Karlsruhe, Deutschland - *Leistung*: Hosting der Anwendung und der Datenbank. *Ort*: Rechenzentrum Nürnberg, Deutschland.
- **Hetzner Online GmbH**, Industriestraße 25, 91710 Gunzenhausen, Deutschland - *Leistung*: Verwahrung einer ausgelagerten Kopie der Datensicherung. Sie liegt bewusst außerhalb des Rechenzentrums, in dem der Dienst läuft, damit ein Ausfall des Hosting-Anbieters nicht auch die Sicherung trifft. *Ort*: Deutschland. *Besonderheit*: Die Sicherung wird von uns verschlüsselt, bevor sie übertragen wird. Hetzner erhält keinen Schlüssel und kann die Inhalte nicht einsehen; verwahrt wird ausschließlich verschlüsselter Datenbestand.
- **Mistral AI SAS**, 15 rue des Halles, 75001 Paris, Frankreich - *Leistung*: Verarbeitung der für eine KI-Funktion ausgewählten Inhalte (Antwortvorschlag, Übersetzung, Grammatik), nur bei Nutzung dieser Funktionen. *Ort*: Europäische Union. *Besonderheit*: Ein- und Ausgaben werden dort 30 Tage rollierend zur Missbrauchserkennung vorgehalten und nicht zum Training von Modellen verwendet.

Nicht Unterauftragsverarbeiter sind die vom Auftraggeber selbst beauftragten Postfachanbieter (z. B. Microsoft, Google, ein IMAP-Anbieter) sowie der Zahlungsdienstleister des Auftragnehmers - siehe § 0.

Fragen

Fragen zu diesem Vertrag, Weisungen und Anfragen betroffener Personen: datenschutz@becom.net, becom Systemhaus GmbH & Co. KG, Am Feldkreuz 16a, 35578 Wetzlar.

Unterschriften

Dieser Vertrag wird im laufenden Betrieb elektronisch geschlossen (siehe Präambel). Diese Ausfertigung dient der Unterzeichnung, wenn der Auftraggeber ein unterschriebenes Dokument benötigt. Beide Fassungen haben denselben Inhalt; maßgeblich ist Version 1.1 vom 26.08.2026.

Ort, Datum

Ort, Datum

Auftraggeber (Verantwortlicher)
Name, Funktion, Unterschrift

Auftragnehmer - becom Systemhaus GmbH &
Co. KG
Name, Funktion, Unterschrift