



Auftragsverarbeitungsvertrag

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO

Stand: 09.10.2026

zwischen

Auftraggeber (Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO)	Der Kunde des Auftragnehmers, der sich auf der Plattform „Collectu“ registriert und den Hauptvertrag abgeschlossen hat. Firma, Anschrift und Kontaktdaten ergeben sich aus den bei der Registrierung angegebenen bzw. im Kundenkonto hinterlegten Angaben.
--	---

– nachfolgend „Auftraggeber“ –

und

Auftragnehmer (Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO)	Collectu GmbH Seidenstraße 36 70174 Stuttgart, Deutschland Registergericht: Amtsgericht Stuttgart, HRB 803639 Vertreten durch: Dr. Colin Reiff, Dr. Frederik Wulle E-Mail (Datenschutz): info@collectu.de
--	--

– nachfolgend „Auftragnehmer“ –

– gemeinsam die „Parteien“ –

Präambel

Der Auftraggeber hat sich auf der Plattform des Auftragnehmers registriert und mit diesem einen Vertrag über die Bereitstellung und Nutzung der Software „Collectu“ auf Grundlage der Allgemeinen Geschäftsbedingungen der Collectu GmbH geschlossen (nachfolgend „Hauptvertrag“). Im Rahmen der Leistungserbringung verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien und erfüllt die Anforderungen des Art. 28 Abs. 3 DSGVO.

Collectu GmbH
Seidenstraße 36
70174 Stuttgart
Germany

Zahlungsdetails
Baden-Württembergische Bank
IBAN: DE33600501010405966093
BIC: SOLADEST600

USt-ID: DE461208298
Handelsregisternummer: HRB 803639
Registergericht: Amtsgericht Stuttgart
Geschäftsführer: Dr. Colin Reiff und Dr. Frederik Wulle

Der Auftraggeber bleibt für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich.

§ 1 Gegenstand, Umfang und Dauer der Auftragsverarbeitung; Vertragsschluss

(1) Gegenstand der Auftragsverarbeitung ist die Erbringung der im Hauptvertrag vereinbarten Leistungen, soweit hierbei personenbezogene Daten des Auftraggebers verarbeitet werden.

(2) Die Software wird in einer hybriden Betriebsform bereitgestellt: Eine Softwarekomponente (nachfolgend „Core“) wird in der Infrastruktur des Auftraggebers installiert und betrieben; die Verwaltung, Konfiguration, Speicherung und Auswertung erfolgt über eine vom Auftragnehmer betriebene Cloud-Plattform (nachfolgend „Hub“). Eine Auftragsverarbeitung nach dieser Vereinbarung liegt vor, soweit personenbezogene Daten an den Hub übermittelt oder dort verarbeitet werden sowie soweit der Auftragnehmer im Rahmen von Support- und Fernwartungsleistungen auf Systeme oder Daten des Auftraggebers zugreift.

(3) Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich abschließend aus Anlage 1.

(4) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Eine Kündigung des Hauptvertrags beendet auch diese Vereinbarung; Pflichten, die ihrer Natur nach fortgelten (insbesondere §§ 5, 11 und 13), bleiben davon unberührt.

(5) Diese Vereinbarung wird elektronisch geschlossen. Sie wird wirksam, sobald der Auftraggeber sie im Rahmen der Registrierung bzw. des Abschlusses des Hauptvertrags oder zu einem späteren Zeitpunkt akzeptiert, insbesondere durch Anklicken eines entsprechenden Kontrollkästchens. Einer Unterschrift der Parteien bedarf es nicht; der Abschluss in elektronischer Form genügt den Anforderungen des Art. 28 Abs. 9 DSGVO.

(6) Die natürliche Person, die diese Vereinbarung für den Auftraggeber akzeptiert, sichert zu, zu dessen Vertretung berechtigt zu sein.

(7) Der Auftragnehmer stellt den Text dieser Vereinbarung beim Vertragsschluss zum Abruf und zur Speicherung bereit und übermittelt ihn dem Auftraggeber auf Anfrage jederzeit erneut in Textform.

§ 2 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, einschließlich in Bezug auf die Übermittlung an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung

mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Diese Vereinbarung einschließlich ihrer Anlagen sowie der Hauptvertrag stellen die initiale Weisung des Auftraggebers dar. Weitere Weisungen erteilt der Auftraggeber grundsätzlich in Textform. Mündlich erteilte Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(3) Weisungsberechtigt und weisungsempfangsberechtigt sind die in Anlage 4 benannten Personen. Änderungen sind der jeweils anderen Partei in Textform mitzuteilen. Mitteilungen des Auftragnehmers nach dieser Vereinbarung, insbesondere nach §§ 7 und 9, erfolgen per E-Mail an die im Kundenkonto des Auftraggebers hinterlegte E-Mail-Adresse. Der Auftraggeber ist dafür verantwortlich, diese E-Mail-Adresse aktuell zu halten.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

(5) Erfordert die Umsetzung einer Weisung, die über die im Hauptvertrag vereinbarten Leistungen hinausgeht, einen erheblichen Mehraufwand, kann der Auftragnehmer hierfür eine angemessene Vergütung nach seinen jeweils gültigen Sätzen verlangen. Er weist den Auftraggeber vor Ausführung darauf hin.

§ 3 Pflichten des Auftraggebers

(1) Der Auftraggeber ist als Verantwortlicher für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen allein verantwortlich. Er hat insbesondere sicherzustellen, dass für die Verarbeitung eine Rechtsgrundlage besteht, die Informationspflichten nach Art. 13 und 14 DSGVO erfüllt sind und erforderliche Einwilligungen wirksam eingeholt wurden.

(2) Der Auftraggeber ist verpflichtet, keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO in den Hub einzubringen, sofern dies nicht ausdrücklich in Anlage 1 vereinbart und durch entsprechende zusätzliche Schutzmaßnahmen abgesichert ist.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist für die Sicherung seiner Daten selbst verantwortlich, soweit im Hauptvertrag keine Datensicherung durch den Auftragnehmer vereinbart ist.

§ 4 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Auftrags und der Weisungen des Auftraggebers. Eine Verarbeitung zu eigenen Zwecken erfolgt nicht.
- (2) Der Auftragnehmer richtet seine innerbetriebliche Organisation so ein, dass sie den besonderen Anforderungen des Datenschutzes genügt, und trifft die technischen und organisatorischen Maßnahmen nach § 6 dieser Vereinbarung.
- (3) Der Auftragnehmer bestätigt, dass er die für die Auftragsverarbeitung geltenden Vorschriften, insbesondere die DSGVO und das BDSG, kennt und beachtet.
- (4) Der Auftragnehmer führt ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.
- (5) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten seines Datenschutzbeauftragten bzw. – sofern eine Benennungspflicht nicht besteht – seines Ansprechpartners für den Datenschutz mit. Ansprechpartner ist:

Dr. Colin Reiff, info@collectu.de
- (6) Werden dem Auftragnehmer Kontrollhandlungen einer Aufsichtsbehörde bekannt, die sich auf die Verarbeitung für den Auftraggeber beziehen, informiert er den Auftraggeber unverzüglich, soweit dies rechtlich zulässig ist.
- (7) Erhält der Auftragnehmer eine Anfrage einer Behörde oder eines Gerichts auf Herausgabe personenbezogener Daten des Auftraggebers, informiert er den Auftraggeber hierüber unverzüglich, soweit dies rechtlich zulässig ist, verweist die anfragende Stelle auf den Auftraggeber und gibt keine Daten heraus, solange er hierzu nicht rechtlich verpflichtet ist.
- (8) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung der Daten aus dem Auftragsverhältnis nur nach Weisung des Auftraggebers ein.

§ 5 Vertraulichkeit

- (1) Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).
- (2) Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Beschäftigungs- bzw. Auftragsverhältnisses und nach Beendigung dieser Vereinbarung fort.
- (3) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung betrauten Personen regelmäßig hinsichtlich der datenschutzrechtlichen Anforderungen unterwiesen und sensibilisiert werden.

(4) Der Zugriff auf personenbezogene Daten des Auftraggebers erfolgt nach dem Grundsatz der Erforderlichkeit („need to know“) und wird protokolliert.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Der zum Zeitpunkt des Vertragsschlusses maßgebliche Stand dieser Maßnahmen ist in Anlage 2 beschrieben. Sofern besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO Gegenstand der Verarbeitung sind, trifft der Auftragnehmer zusätzlich die sich aus § 22 Abs. 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragnehmer ist gestattet, alternative, gleichwertige Maßnahmen umzusetzen. Das Sicherheitsniveau der in Anlage 2 festgelegten Maßnahmen darf dabei nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anfrage mitzuteilen.

§ 7 Unterauftragsverarbeiter

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 3 genannten Unterauftragsverarbeiter durchgeführt. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und werden hiermit genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mit einer angemessenen Vorlaufzeit vor der Beauftragung in Textform. Der Auftraggeber kann der Änderung innerhalb von zwei (2) Wochen nach Zugang der Information aus wichtigem datenschutzrechtlichen Grund in Textform widersprechen. Erfolgt innerhalb dieser Frist kein begründeter Widerspruch, gilt die Hinzuziehung bzw. Ersetzung als genehmigt.

(3) Widerspricht der Auftraggeber und kann der Auftragnehmer die betreffende Leistung ohne den Unterauftragsverarbeiter nicht mit zumutbarem Aufwand erbringen, sind beide Parteien berechtigt, den Hauptvertrag mit einer Frist von einem (1) Monat außerordentlich zu kündigen. Bereits im Voraus gezahlte Entgelte werden für den nicht genutzten Zeitraum anteilig erstattet.

(4) Der Auftragnehmer ist verpflichtet, Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Sofern eine Einbeziehung von Unterauftragsverarbeitern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Unterauftragsverarbeiter ein angemessenes Datenschutzniveau gewährleistet ist. Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragsverarbeitern nachweisen.

(5) Der Auftragnehmer verpflichtet den Unterauftragsverarbeiter vertraglich zu denselben Datenschutzpflichten, die in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO). Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Einhaltung dieser Pflichten.

(6) Nicht als Unterauftragsverhältnis im Sinne dieser Vorschrift gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt und die nicht auf die Verarbeitung personenbezogener Daten des Auftraggebers gerichtet sind (z. B. Telekommunikationsleistungen, Reinigung, Wartung ohne Datenzugriff). Der Auftragnehmer stellt auch hier die Wahrung des Datenschutzes und der Datensicherheit sicher.

§ 8 Unterstützung des Auftraggebers, Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO nachzukommen (Art. 28 Abs. 3 lit. e DSGVO).

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

(3) Der Auftragnehmer unterstützt den Auftraggeber ferner bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgenabschätzung und der vorherigen Konsultation (Art. 28 Abs. 3 lit. f DSGVO), unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

(4) Für Unterstützungsleistungen, die über die gesetzlich geschuldete Unterstützung hinausgehen oder die nicht auf einem vom Auftragnehmer zu vertretenden Umstand beruhen, kann der Auftragnehmer eine angemessene Vergütung verlangen.

§ 9 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten des Auftraggebers unverzüglich in Textform.

(2) Die Meldung enthält, soweit möglich, mindestens die in Art. 33 Abs. 3 DSGVO genannten Angaben:

- eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze;
- den Namen und die Kontaktdaten des Ansprechpartners für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und stimmt sich hierüber mit dem Auftraggeber ab.

(4) Meldungen an die Aufsichtsbehörde nach Art. 33 DSGVO und Benachrichtigungen betroffener Personen nach Art. 34 DSGVO obliegen ausschließlich dem Auftraggeber. Der Auftragnehmer nimmt solche Meldungen nicht eigenständig im Namen des Auftraggebers vor.

§ 10 Nachweis- und Kontrollrechte

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen, die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Nachweis kann insbesondere erbracht werden durch:

- die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Datenschutzbeauftragte, IT-Sicherheitsabteilung, ISO 27001-Zertifikat, SOC-2-Bericht);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit-Verfahren;
- die Vorlage einer aktuellen Selbstauskunft bzw. Dokumentation der technischen und organisatorischen Maßnahmen.

(3) Reichen die vorgelegten Nachweise im Einzelfall nicht aus, ist der Auftraggeber berechtigt, sich nach rechtzeitiger Ankündigung mit einer Frist von mindestens zwei (2) Wochen zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs von der Einhaltung dieser Vereinbarung zu überzeugen. Der Auftraggeber führt Vor-Ort-Kontrollen in der Regel höchstens einmal pro Kalenderjahr durch; bei konkreten Anhaltspunkten für einen Verstoß oder nach einer Verletzung des Schutzes personenbezogener Daten sind Kontrollen auch anlassbezogen und kurzfristig zulässig. Die Vor-Ort-Kontrollen sind auf den zur Überprüfung der vertragsgegenständlichen Auftragsverarbeitung erforderlichen Umfang zu beschränken.

(4) Der Auftraggeber stellt sicher, dass Kontrollen nur durch Personen durchgeführt werden, die zur Verschwiegenheit verpflichtet sind und nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen. Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie Daten anderer Kunden sind zu wahren.

(5) Für den Aufwand, der dem Auftragnehmer durch Vor-Ort-Kontrollen entsteht, kann er eine angemessene Vergütung verlangen, sofern die Kontrolle nicht auf einem vom Auftragnehmer zu vertretenden Umstand beruht.

§ 11 Löschung und Rückgabe nach Beendigung

- (1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO).
- (2) Der Auftraggeber teilt seine Wahl spätestens bis zum Wirksamwerden der Vertragsbeendigung in Textform mit. Trifft er keine Wahl, stellt der Auftragnehmer die Daten für einen Zeitraum von dreißig (30) Kalendertagen ab Vertragsende zum Export in einem gängigen, strukturierten und maschinenlesbaren Format bereit und löscht sie anschließend.
- (3) Die Löschung erfolgt spätestens innerhalb von neunzig (90) Kalendertagen nach Vertragsende, einschließlich der Löschung aus Sicherungskopien im Rahmen des regulären Backup-Zyklus. Der Auftragnehmer bestätigt die vollständige Löschung auf Anforderung in Textform.
- (4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, dürfen vom Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden. Er kann sie zur Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 12 Verarbeitung in Drittländern

- (1) Eine Verarbeitung personenbezogener Daten in einem Drittland im Sinne der DSGVO findet nur statt, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (2) Zulässig ist eine Übermittlung insbesondere auf Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission (Art. 45 DSGVO) oder auf Grundlage der von der Europäischen Kommission erlassenen Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) nebst einer dokumentierten Prüfung der Wirksamkeit der Garantien im Empfängerland (Transfer Impact Assessment) und – soweit erforderlich – zusätzlicher Schutzmaßnahmen.
- (3) Ein Fernzugriff auf personenbezogene Daten aus einem Drittland, insbesondere im Rahmen von Support- oder Wartungsleistungen, gilt als Übermittlung im Sinne dieser Vorschrift.

§ 13 Haftung

- (1) Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrags, soweit in dieser Vereinbarung nichts Abweichendes bestimmt ist.
- (2) Im Außenverhältnis gegenüber betroffenen Personen gilt Art. 82 DSGVO.
- (3) Die Parteien stellen sich im Innenverhältnis von Ansprüchen betroffener Personen sowie von Geldbußen entsprechend ihrem jeweiligen Verantwortungsanteil frei.

§ 14 Schlussbestimmungen

- (1) Diese Vereinbarung geht den Regelungen des Hauptvertrags einschließlich der Allgemeinen Geschäftsbedingungen des Auftragnehmers vor, soweit sie die Verarbeitung personenbezogener Daten im Auftrag betrifft. Im Übrigen gelten die Regelungen des Hauptvertrags.
- (2) Änderungen und Ergänzungen dieser Vereinbarung und ihrer Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.
- (3) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen Zweck der ersetzten Bestimmung am nächsten kommt.
- (4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist – soweit gesetzlich zulässig – Stuttgart.
- (5) Die Anlagen 1 bis 4 sind Bestandteil dieser Vereinbarung.
- (6) Diese Vereinbarung liegt in deutscher und englischer Sprache vor. Bei Abweichungen ist die deutsche Fassung maßgeblich.

Diese Vereinbarung wird elektronisch geschlossen (§ 1 Abs. 5) und ist ohne Unterschrift wirksam.

Anlage 1

Beschreibung der Verarbeitung

1. Gegenstand der Verarbeitung

Bereitstellung und Betrieb der Software „Collectu“ zur Erfassung, Übertragung, Speicherung, Verarbeitung und Auswertung von Daten aus den Systemen des Auftraggebers sowie die Erbringung zugehöriger Support-, Wartungs- und Betriebsleistungen.

2. Art und Zweck der Verarbeitung

- Bereitstellung, Betrieb und Wartung des Hubs sowie der beim Auftraggeber installierten Cores
- Verwaltung von Benutzerkonten, Rollen und Berechtigungen des Auftraggebers
- Speicherung und Verarbeitung der vom Auftraggeber eingebrachten Daten („Nutzerdaten“)
- Erstellung von Auswertungen, Visualisierungen und Berichten innerhalb des Hubs
- Verarbeitung durch KI-gestützte Funktionen des Hubs, soweit vom Auftraggeber aktiviert
- Protokollierung zur Gewährleistung der Systemsicherheit und der Nachvollziehbarkeit von Zugriffen
- Datensicherung und Wiederherstellung
- Fehleranalyse, Support und – nach vorheriger Zustimmung des Auftraggebers – temporärer Remote-Zugriff nach Ziffer 12.5 der AGB

3. Art der personenbezogenen Daten

Die Verarbeitung umfasst folgende Datenarten:

Kategorie	Beispiele
Stamm- und Kontaktdaten der Nutzer des Auftraggebers	Name, Vorname, dienstliche E-Mail-Adresse, Benutzername, Organisationszugehörigkeit, Rolle
Vertrags- und Abrechnungsdaten	Firmierung, Rechnungsanschrift, gebuchter Tarif, Zahlungsdaten (soweit erhoben)
Nutzungs- und Protokolldaten	Zeitstempel, IP-Adresse, Geräte- und Browserinformationen, aufgerufene Funktionen, Konfigurationsänderungen, Fehler- und Sicherheitsprotokolle
Authentifizierungsdaten	Passwort-Hashes, Token, API-Schlüssel, Sitzungsinformationen

Kategorie	Beispiele
Kommunikations- und Supportdaten	Inhalte von Support-Anfragen, E-Mail-Korrespondenz, Fehlerbeschreibungen und übermittelte Protokolldateien
Vom Auftraggeber eingebrachte Inhaltsdaten	Von den Systemen des Auftraggebers erfasste Prozess-, Maschinen- und Sensordaten sowie sonstige Inhalte, soweit diese einen Personenbezug aufweisen (z. B. Bediener- oder Schichtkennungen, Auftrags- oder Zeiterfassungsbezüge). Umfang und Personenbezug bestimmt allein der Auftraggeber.

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand der Verarbeitung, sofern nicht abweichend vereinbart.

4. Kategorien betroffener Personen

- Beschäftigte des Auftraggebers (insbesondere Nutzer, Administratoren, Ansprechpartner)
- Beschäftigte verbundener Unternehmen und externer Dienstleister des Auftraggebers, soweit ihnen ein Zugang eingeräumt wird
- Kunden, Lieferanten und sonstige Geschäftspartner des Auftraggebers, soweit deren Daten vom Auftraggeber eingebracht werden
- Sonstige natürliche Personen, deren Daten der Auftraggeber in den Hub einbringt

5. Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des Hauptvertrags. Nach dessen Beendigung gilt § 11 dieser Vereinbarung.

6. Ort der Verarbeitung

Rechenzentrumsstandorte innerhalb der Bundesrepublik Deutschland. Die Verwaltung und Administration der Systeme erfolgt vom Sitz des Auftragnehmers in Stuttgart aus.

Anlage 2

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Betrieb der Server ausschließlich in zertifizierten Rechenzentren der in Anlage 3 genannten Dienstleister mit Zutrittskontrollsystem, Videoüberwachung, Alarmanlage und dokumentierter Besucherverwaltung
- Geschäftsräume des Auftragnehmers: Schließsystem mit dokumentierter Schlüsselvergabe, Besucher werden begleitet

Zugangskontrolle

- Persönliche, nicht geteilte Benutzerkonten für alle Systeme
- Passwortrichtlinie mit Mindestlänge, Komplexitätsanforderungen und Sperrung nach Fehlversuchen
- Speicherung von Passwörtern ausschließlich als Hash mit Salt
- Mehr-Faktor-Authentifizierung soweit vom Auftraggeber aktiviert
- Automatische Sperrung inaktiver Sitzungen
- Administrativer Zugriff auf die Produktivumgebung ausschließlich über verschlüsselte Verbindungen und aus definierten Netzbereichen

Zugriffskontrolle

- Rollen- und Berechtigungskonzept nach dem Grundsatz der geringsten Privilegien
- Mandantentrennung: logische Trennung der Daten unterschiedlicher Auftraggeber
- Protokollierung administrativer Zugriffe auf Produktivdaten
- Geregelter Verfahren zur Vergabe, Änderung und Entziehung von Berechtigungen, insbesondere beim Ausscheiden von Beschäftigten
- Datenträger werden vor Aussonderung sicher gelöscht bzw. vernichtet (DIN 66399)

Trennungskontrolle

- Logische Trennung von Produktiv-, Test- und Entwicklungsumgebung
- Keine Verwendung von Produktivdaten in Test- und Entwicklungsumgebungen

Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung sämtlicher Verbindungen (TLS 1.2 oder höher)
- Verschlüsselung der Daten im Ruhezustand auf Speichermedien und in Datensicherungen
- Verschlüsselung der Festplatten von Endgeräten der Beschäftigten
- Pseudonymisierung, soweit der Verarbeitungszweck dies zulässt

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Übertragung zwischen Core und Hub ausschließlich verschlüsselt und authentifiziert
- Keine Übermittlung personenbezogener Daten an Dritte außerhalb der in Anlage 3 genannten Unterauftragsverarbeiter
- Dokumentation der Datenflüsse

Eingabekontrolle

- Protokollierung sicherheitsrelevanter Ereignisse und von Änderungen an Konfigurationen und Berechtigungen
- Nachvollziehbarkeit, welches Benutzerkonto welche Änderung vorgenommen hat
- Manipulationsgeschützte Aufbewahrung der Protokolldaten für einen definierten Zeitraum

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Redundante Auslegung der Infrastruktur im Rechenzentrum (Strom, Klimatisierung, Netzanbindung, Brandschutz)
- Regelmäßige, automatisierte Datensicherung mit definierten Aufbewahrungsfristen
- Getrennte Aufbewahrung der Datensicherungen von den Produktivsystemen
- Regelmäßige Prüfung der Wiederherstellbarkeit der Datensicherungen
- Einsatz von Firewalls, Netzsegmentierung und Schutzmaßnahmen gegen Überlastungsangriffe
- Monitoring und Alarmierung bei Systemstörungen
- Zeitnahes Einspielen sicherheitsrelevanter Updates (Patch-Management)
- Dokumentierter Notfallplan (Business Continuity und Disaster Recovery) mit definierten Wiederanlaufzielen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Datenschutz-Management mit dokumentierten internen Richtlinien
- Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO
- Verpflichtung aller Beschäftigten auf Vertraulichkeit und regelmäßige Datenschutz- und IT-Sicherheitsschulungen
- Dokumentierter Prozess zur Erkennung, Bewertung und Meldung von Verletzungen des Schutzes personenbezogener Daten
- Dokumentierter Prozess zur Bearbeitung von Anfragen betroffener Personen
- Auftragskontrolle: Auswahl und regelmäßige Überprüfung von Unterauftragsverarbeitern, Abschluss von Verträgen nach Art. 28 DSGVO
- Berücksichtigung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen, mindestens jährlich

- Sicherheitsprüfungen des Quellcodes und der Abhängigkeiten im Entwicklungsprozess

Anlage 3

Genehmigte Unterauftragsverarbeiter

Unternehmen, Anschrift	Leistung	Ort der Verarbeitung
IONOS SE Elgendorfer Str. 57 56410 Montabaur, Germany	Hosting und Betrieb der Server- und Speicherinfrastruktur des Hubs einschließlich Datensicherung	Deutschland, EU
OpenAI Ireland Limited 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	Bereitstellung von KI-Modellen für die KI-gestützten Funktionen des Hubs	Irland und USA Übermittlung auf Grundlage der EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)

Änderungen werden nach Maßgabe des § 7 dieser Vereinbarung mitgeteilt.

Anlage 4

Ansprechpartner und weisungsberechtigte Personen

	Auftraggeber	Auftragnehmer
Weisungsberechtigte Person(en)	Nutzer mit Inhaber- bzw. Administratorrechten im Kundenkonto des Auftraggebers	Name: Dr. Colin Reiff Funktion: Geschäftsführer E-Mail: colin.reiff@collectu.de Name: Dr. Frederik Wulle Funktion: Geschäftsführer E-Mail: frederik.wulle@collectu.de
Weisungsempfangsberechtigte Person(en)	Entfällt	Benannte Mitarbeiter des Auftragnehmers gemäß interner Zuständigkeitsregelung
Datenschutzbeauftragter bzw. Ansprechpartner Datenschutz	Datenschutzbeauftragter des Auftraggebers, sofern dem Auftragnehmer benannt; im Übrigen die im Kundenkonto hinterlegte E-Mail-Adresse	Name: Dr. Colin Reiff E-Mail: info@collectu.de
Meldestelle für Sicherheitsvorfälle	Die im Kundenkonto hinterlegte E-Mail-Adresse	E-Mail: security@collectu.de

Abweichende oder zusätzliche Ansprechpartner sowie einen Datenschutzbeauftragten kann der Auftraggeber jederzeit in Textform an info@collectu.de mitteilen.