

Auftragsverarbeitungsvereinbarung (AVV)

Version: 2026-09-01 · Stand: 1. September 2026 · Status: APPROVED · Fassung: Standard

Blanko-Vorlage, Auftraggeber-Felder vom Vertragspartner ausfüllen lassen.

FREIGELEGTE FASSUNG, Status, Wirksamkeitsbeginn und Freigabeverantwortung sind in den versionierten Freigabemetadaten dokumentiert. Für die elektronische Annahme ist ausschließlich der geschützte Konto-Pfad mit Dokumentprüfsumme und Annahmenachweis massgeblich.

AUFTRAGGEBER, VERANTWORTLICHER

Firma / Name
Ansprechpartner
Anschrift
Land
E-Mail
USt-IdNr.

AUFTRAGNEHMER, AUFTRAGSVERARBEITER

Marcel Schlüter IT-Services, Empcora

Kollwitzstraße 76
10435 Berlin, Deutschland
kontakt@empcora.de

Betreiber der Empcora-SaaS-Plattform für technische EmpCo-Risiko-Pre-Checks.

Diese Auftragsverarbeitungsvereinbarung („AVV“) wird zwischen dem oben genannten Verantwortlichen (Auftraggeber) und dem Auftragnehmer geschlossen. Sie konkretisiert die datenschutzrechtlichen Pflichten der Parteien für die Verarbeitung personenbezogener Daten im Rahmen des Empcora-SaaS-Nutzungsvertrags (nachfolgend „Hauptvertrag“).

§ 1 Gegenstand, Rollenabgrenzung und Dauer der Auftragsverarbeitung

(1) Auftragsdaten: Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers nur die personenbezogenen Daten, die bei den nachfolgend beschriebenen Scan-, Analyse-, Nachweis-, Monitoring- und Berichtsfunktionen anfallen („Auftragsdaten“). Der konkrete Funktionsaufruf, die vom Auftraggeber ausgewählten Inhalte und Ziele sowie seine dokumentierten Konfigurationen bilden die Weisung innerhalb des Hauptvertrags.

(2) Erfasste Leistungen: Die Auftragsverarbeitung kann, soweit die jeweilige Funktion gebucht und vom Auftraggeber aktiviert ist, insbesondere umfassen:

- Crawling und technische Analyse der vom Auftraggeber bestimmten eigenen oder fremden Domains, Wettbewerber-, Benchmark- und Vergleichsseiten;
- Analyse von Webseiten, Dokumenten, PDF-Dateien, Bildern und sonstigen bereitgestellten Texten, einschliesslich lokaler Textextraktion und OCR/Docling sowie optionaler KI-gestützter Text- oder Bildeinordnung;
- Prüfung vom Auftraggeber bereitgestellter Inhalte aus Social-Media-, Newsletter-, Kampagnen- oder sonstigen Kommunikationskanälen;
- Speicherung und Bearbeitung von Scans, Fundstellen, Bewertungen, Kommentaren, Ausnahmen, Freigaben, Mandanten- und Zuordnungsdaten sowie Nachweisdateien und deren Metadaten;
- Erzeugung und Bereitstellung von Berichten und Exporten, insbesondere als PDF, JSON, CSV oder XLSX, sowie Monitoring, Re-Scans und Benachrichtigungen;
- auf Weisung ausgelagerte Ein- oder Ausgaben über CMS-Anbindungen und Webhooks sowie die Übermittlung von Meldungen an vom Auftraggeber ausgewählte Slack-, Teams- oder sonstige Zielkanäle.

(3) Eigene Verantwortlichkeit: Nicht als Auftragsdaten im Sinne dieser AVV verarbeitet Empcora Daten für eigene, von Empcora festgelegte Zwecke, insbesondere Konto-, Organisations-, Login-, Team-, Vertrags-, Abrechnungs- und Zahlungsdaten, Sicherheits- und Auditprotokolle, eigenen Kundensupport einschliesslich Hanna-/LedgerOS-Abläufen, AVV- und Annahmenachweise sowie eigene

Produkt-, Nutzungs- oder aggregierte Statistikzwecke. Fuer diese Verarbeitungen handelt Empcora nach der jeweils tatsaechlichen Funktion in eigener datenschutzrechtlicher Verantwortung; die Datenschutzerklaerung und die gesetzlichen Pflichten hierfuer bleiben unberuehrt. Wird dasselbe Datum fuer beide Zweckbereiche genutzt, ist jede Verarbeitung getrennt nach ihrem tatsaechlichen Zweck und ihrer Rolle zu beurteilen.

(3a) Aggregierte Branchenstatistik: Empcora erstellt in eigener datenschutzrechtlicher Verantwortung aggregierte Branchen-Kennzahlen (z. B. Durchschnitts-Score und mittlere Fundstellenzahlen je Branche) aus abgeschlossenen Scans. In die Aggregation fliessen ausschliesslich Zahlenwerte ein, keine Inhalte, Texte, Domains oder Namen; eine Branchen-Kennzahl wird erst ab einer Mindeststichprobe von fuenf Scans ausgewiesen, damit kein Rueckschluss auf einen einzelnen Auftraggeber moeglich ist. Eine darueber hinausgehende Nutzung von Auftragsdaten fuer organisationsuebergreifende Auswertungen, fuer Werbung oder fuer das Training allgemeiner KI-Modelle findet nicht statt.

(4) Dauer: Die Auftragsverarbeitung beginnt mit der ersten Nutzung einer erfassten Funktion und dauert fuer den jeweiligen Datenbestand bis zur vertragsgemaessen Rueckgabe oder Loeschung, laengstens bis zur vollstaendigen Abwicklung nach Beendigung des Hauptvertrags. Im derzeitigen technischen Stand werden Scan-Ergebnisse waehrend des laufenden Vertrags ohne automatische Regelfrist gespeichert und auf dokumentierte Weisung gelöscht. Das begruendet keine Befugnis zur unbegrenzten Speicherung nach Ende der Auftragsverarbeitung.

(5) Speicher- und Loeschregeln: Scan-Ergebnisse, Fundstellen, Nachweisdateien und Exporte werden fuer die Dauer des Hauptvertrags gespeichert und auf dokumentierte Weisung nach § 13 gelöscht oder zurueckgegeben. Sicherungskopien werden turnusmaessig ueberschrieben; § 13 Abs. 3 gilt entsprechend. Abrechnungs-, Vertrags- und Sicherheitsnachweise nach Abs. 3 unterliegen eigenen gesetzlichen Aufbewahrungsfristen (insbesondere § 147 AO, § 257 HGB) und bleiben unberuehrt.

§ 2 Art und Zweck der Verarbeitung

(1) Art: Die Verarbeitung umfasst, soweit fuer die gewaehlte Funktion erforderlich, Erheben und Abrufen durch Crawling oder Schnittstellen, Entgegennehmen und Hochladen, Ordnen und Zuordnen, Extrahieren und OCR, Vergleichen, Klassifizieren und Bewerten, Speichern, Anzeigen, Berichten und Exportieren, Uebermitteln an genehmigte Unterauftragsverarbeiter oder vom Auftraggeber bestimmte Empfaenger, Einschraenken, Berichtigen sowie Loeschen oder Zurueckgeben.

(2) Zweckbindung: Zweck ist ausschliesslich die technische Pruefung, Dokumentation, Nachweisfuehrung, Beobachtung und Ausgabe der vom Auftraggeber bestimmten Inhalte im Rahmen des Hauptvertrags. Diese AVV erteilt keine Weisung zur Nutzung von Auftragsdaten fuer Werbung, organisationsuebergreifende Profile, eigene Produktzwecke oder das Training eigener oder fremder allgemeiner KI-Modelle.

(3) Kundenbestimmte Empfaenger: Veranlasst der Auftraggeber einen Export, ein CMS-Ziel, einen Webhook oder eine Nachricht an Slack, Teams oder einen anderen von ihm bestimmten Dienst, bestimmt er Empfaenger und Inhalt dieser Uebermittlung. Soweit Empcora einen solchen Dienst nicht selbst fuer die Leistungserbringung beauftragt, ist er nicht allein durch die technische Uebermittlung Unterauftragsverarbeiter von Empcora. Die Pflichten des Auftragnehmers zur sicheren Ausfuehrung der Weisung bleiben unberuehrt.

(4) Optionale Verarbeitungswege: Nur wenn die jeweilige Funktion aktiviert und tatsaechlich konfiguriert ist, koennen an Anthropic ausgewaehlte Texte und Kontexte sowie bei einer Bildanalyse Bildbytes uebermittelt werden; Einzelheiten und Freigabe-Gates ergeben sich aus §§ 6 und 7. Lokal oder auf betreibereigener Infrastruktur ausgefuehrte Komponenten wie Docling, Apple Vision oder Ollama sind nicht allein durch ihren Einsatz externe Unterauftragsverarbeiter, muessen aber hinsichtlich Betriebsort, Zugriff und Sicherheitsmassnahmen in der technischen Evidenz erfasst werden. Diese Vereinbarung behauptet nicht, dass jeder optionale Pfad produktiv aktiv ist.

§ 3 Kategorien personenbezogener Daten und sensible Inhalte

Je nach Weisung und gewaehlter Funktion koennen insbesondere verarbeitet werden:

- **Quell- und Inhaltsdaten:** Start-, Seiten-, Dokument- und Bild-URLs, Webseiten- und Metadaten, Texte, Bilder, PDF- und sonstige Dokumentinhalte, Impressums-, Kontakt- und Kommunikationsinhalte;
- **vom Auftraggeber bereitgestellte Daten:** Mandanten-, Kunden-, Ansprechpartner-, Kontakt-Snapshot- und Zuordnungsdaten, Social-Media-, Newsletter- und Kampagneninhalte sowie Kommentare, Ausnahmen, False-Positive-Markierungen, Freigaben und Weisungsangaben;
- **Nachweise:** hochgeladene PDF-, JPEG- und PNG-Dateien, Bezeichnungen, Aussteller, Gueltigkeits- und Zuordnungsangaben sowie sonstige vom Auftraggeber eingetragene Metadaten;
- **Analyse- und Ergebnisdaten:** extrahierte Texte, Claims, Fundstellen und Quellreferenzen, Klassifikationen, Bewertungen, Aenderungsvergleiche, Berichte, Exporte und Benachrichtigungsinhalte;

- **auftragsbezogene Betriebsdaten:** Scan-, Job-, Fehler- und Zustandskennungen, Zeitpunkte und fuer die Ausfuehrung erforderliche technische Metadaten. Eigene Sicherheits-, Vertrags- und Abrechnungsprotokolle fallen unter § 1 Abs. 3.

Sensible Inhalte: Die Leistung ist nicht auf die gezielte Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO oder von Daten zu strafrechtlichen Verurteilungen und Straftaten nach Art. 10 DSGVO ausgerichtet. Solche Angaben koennen jedoch in oeffentlichen Seiten, Bildern, Dokumenten oder Nachweisen beiläufig enthalten sein. Der Auftraggeber bleibt fuer Zulaessigkeit, Transparenz und seine Weisung verantwortlich; die eigenen Pflichten des Auftragnehmers aus Art. 28 und 32 DSGVO werden dadurch nicht eingeschaenkt. Eine vorhersehbare oder gezielte Verarbeitung setzt eine vorherige ergaenzende dokumentierte Weisung und risikogerechte besondere Schutzmassnahmen voraus.

Vereinbarte Grenze: Die gezielte Pruefung oder Auswertung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) oder von Daten nach Art. 10 DSGVO ist nicht Vertragsgegenstand; hierauf gerichtete Weisungen werden nicht erteilt und nicht ausgefuehrt. Eine automatische inhaltliche Filterung solcher Angaben erfolgt nicht; beilaeufig enthaltene Angaben unterliegen denselben Massnahmen der Anlage 1 und werden nicht gesondert ausgewertet. Fuer eine gezielte Verarbeitung waere eine gesonderte schriftliche Vereinbarung mit zusaetzlichen, risikogerechten Schutzmassnahmen erforderlich.

§ 4 Kategorien betroffener Personen

- Beschaeftigte, Organmitglieder, Beauftragte, Kunden, Interessenten und sonstige Kontaktpersonen des Auftraggebers oder der von ihm verwalteten Mandanten;
- Inhaber, Beschaeftigte, Vertretungsberechtigte und Kontaktpersonen der gescannten Domains, Unternehmen, Wettbewerber oder sonstigen Inhaltsanbieter;
- Autoren, Unterzeichner und sonstige Personen, die in Webseiten, Bildern, Dokumenten, Nachweisen, Social-Media-, Newsletter- oder Kampagneninhalten genannt, beschrieben oder abgebildet sind;
- Aussteller, Ansprechpartner und sonstige Personen mit Bezug zu hochgeladenen Nachweisen.

§ 5 Weisungen und Pflichten des Auftragnehmers

(1) Weisungsbindung: Der Auftragnehmer verarbeitet Auftragsdaten nur auf dokumentierte Weisung des Auftraggebers, einschliesslich Weisungen zu Uebermittlungen in Drittlaender oder an internationale Organisationen. Als dokumentierte Ausgangsweisung gelten der Hauptvertrag, diese AVV sowie die vom Auftraggeber authentifiziert ausgelosten Funktionsaufrufe und gespeicherten Konfigurationen innerhalb des in §§ 1 bis 3 beschriebenen Umfangs.

(2) Weitere Weisungen: Weitere Weisungen koennen ueber einen authentifizierten Konto- oder Supportkanal oder in Textform an kontakt@empcora.de erteilt werden. Sie muessen Auftraggeber, betroffenen Datenbestand oder Mandanten, verlangte Verarbeitung und gegebenenfalls Ziel und Frist hinreichend bezeichnen. Der Auftragnehmer dokumentiert Weisung und Umsetzung gemeinsam mit dem Vertragsnachweis. Weisungen unmittelbar von Dritten werden nur nach dokumentierter Bestaetigung des Auftraggebers ausgefuehrt.

(3) Gesetzliche Verarbeitung: Ist der Auftragnehmer nach Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung ausserhalb der Weisung verpflichtet, informiert er den Auftraggeber vor der Verarbeitung ueber die Rechtsanforderung, soweit das betreffende Recht dies nicht aus wichtigen Gruenden des oeffentlichen Interesses verbietet.

(4) Rechtswidrige oder nicht ausfuehrbare Weisung: Haelt der Auftragnehmer eine Weisung fuer einen Verstoss gegen die DSGVO oder sonstiges Datenschutzrecht der Union oder eines Mitgliedstaats, informiert er den Auftraggeber unverzueglich. Die beanstandete Weisung wird bis zur Klaerung nicht ausgefuehrt, soweit dies zur Vermeidung des angenommenen Verstosses erforderlich ist. Kann der Auftragnehmer eine Weisung aus technischen, rechtlichen oder organisatorischen Gruenden nicht vollstaendig ausfuehren, informiert er den Auftraggeber ebenfalls unverzueglich ueber Grund und betroffenen Umfang.

(5) Personen und Sicherheit: Der Auftragnehmer gewaehrt Zugriff auf Auftragsdaten nur Personen, die ihn fuer Durchfuehrung, Verwaltung oder Ueberwachung der Leistung benoetigen und zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er trifft die nach Art. 32 DSGVO erforderlichen und in Anlage 1 beschriebenen technischen und organisatorischen Massnahmen und unterstuetzt den Auftraggeber nach §§ 9 bis 11.

§ 6 Unterauftragsverarbeiter (Sub-Processors)

Fuer die von dieser AVV erfasste Auftragsverarbeitung gilt die folgende fuer diese Version freigegebene Unterauftragnehmerliste. Stripe ist nicht pauschal als Scan-Unterauftragsverarbeiter eingeordnet; die Zahlungsrolle wird separat pro Verarbeitung bewertet.

Unterauftragsverarbeiter	Region / Status	Umfang / Transfer / Freigabe-Gate
Hetzner Online GmbH RELEASE_EVIDENCE_VERIFIED	Rechenzentrum Falkenstein, Deutschland (am 19.08.2026 per IP, Reverse-DNS und AS24940 verifiziert)	Server-, Datenbank-, Cache- und Mail-Infrastruktur Scan-Inhalte, Ergebnisdaten, Konto- und technische Betriebsdaten <i>Kein Drittlandtransfer: Produktivstandort Deutschland; Hetzner-AVV nach Art. 28 DSGVO ueber das Anbieter- Kundenkonto</i> Empcora-Loeschkonzept (§ 1 Abs. 5, § 13); Sicherungen mit turnusmaessiger Ueberschreibung, woechentlicher Restore- Test Freigabe-Gate: Standort am 19.08.2026 auf dem Produktivsystem verifiziert (docs/avv-betriebsnachweis-2026- 08-19.md); Vertragsbeleg liegt im Anbieter-Konto des Betreibers, mit der Owner-Freigabe dieser Fassung bestaetigt.
Cloudflare, Inc. RELEASE_EVIDENCE_VERIFIED	Globales Edge-Netz; eine aktive Datenlokalisierung wird NICHT behauptet (§ 7 Abs. 4 benennt das transparent)	DNS, CDN, WAF, DDoS- und Bot-Schutz IP-Adresse, Request-URL, Header, Sicherheits- und Verbindungsmetadaten sowie potenziell transient weitergeleiteter Request-Inhalt <i>SCC nach (EU) 2021/914 als Bestandteil des Cloudflare Customer DPA (Clause 6.2, am 19.08.2026 gegen den offiziellen Vertragstext geprueft)</i> Transiente Edge-Verarbeitung; kein Logpush/Analytics-Export von Request-Inhalten konfiguriert Freigabe-Gate: DPA/SCC-Grundlage am 19.08.2026 gegen den veroeffentlichten Vertragstext verifiziert; Datenlokalisierung wird bewusst nicht zugesagt, das Dokument bleibt insoweit ehrlich.
Anthropic PBC RELEASE_EVIDENCE_VERIFIED	Speicherung laut Anbieter in den USA; Verarbeitung und Routing koennen weitere globale Regionen einbeziehen	Claude API fuer Text-Einordnung und optionale Bild-Text- Extraktion Ausgewaehlte Werbetexte/Kontext; bei Bild-Audits Bildinhalt, in dem Personenbezug nicht ausgeschlossen ist <i>SCC-Module 2 und 3 nach (EU) 2021/914, einbezogen ueber das Anthropic Data Processing Addendum (Sektion I; Bestandteil der Commercial Terms, am 19.08.2026 gegen die offiziellen Vertragstexte geprueft)</i> Standard-API: Loeschung von Ein-/Ausgaben innerhalb 30 Tagen, mit dokumentierten Ausnahmen; ZDR wird NICHT behauptet Freigabe-Gate: DPA-Einbeziehung und SCC-Module am 19.08.2026 gegen Commercial Terms (Abschnitt C) und DPA (Sektion I, Schedule 3) verifiziert; eigener API-Workspace fuer empcora (Owner-Vorgabe) besteht.

Genehmigungsmodell fuer die Freigabefassung: Vorgesehen ist eine allgemeine schriftliche Genehmigung fuer die in der versionierten Anlage aufgefuehrten Unterauftragsverarbeiter. Vor der Hinzufuegung oder Ersetzung eines Unterauftragsverarbeiters soll der Auftragnehmer den Auftraggeber individuell in Textform ueber Anbieter, Ort, Aufgabe, betroffene Daten, Transfermechanismus und wesentliche Garantien informieren und ihm vor dem Einsatz Gelegenheit zum Widerspruch geben. Eine blosser Aenderung der Online-Liste gilt nicht als individuelle Information.

Bei einem begruendeten Widerspruch pruefen die Parteien zunaechst eine zumutbare Abhilfe oder Alternative. Solange keine abgestimmte Loesung besteht, darf der neue Anbieter fuer den betroffenen Datenbestand nicht eingesetzt werden; ob stattdessen die betroffene Funktion beendet werden kann, richtet sich nach der noch freizugebenden Regelung und dem Hauptvertrag.

Jeder Unterauftragsverarbeiter ist vor Beginn der Verarbeitung durch einen schriftlichen Vertrag an im Wesentlichen dieselben Datenschutzpflichten zu binden, die fuer den Auftragnehmer gelten, einschliesslich Weisungsbindung, Vertraulichkeit, Sicherheit, Unterstützung, Loeschung und Audit. Der Auftragnehmer bleibt dem Auftraggeber fuer die Erfuellung der Datenschutzpflichten des Unterauftragsverarbeiters in vollem Umfang verantwortlich und informiert ihn, wenn ein Unterauftragsverarbeiter seine

Datenschutzpflichten nicht erfüllt. Auf Verlangen stellt er die fuer die Kontrolle erforderlichen Vertragsinformationen bereit; Geschäftsgeheimnisse und personenbezogene Daten Dritter dürfen in einer Vertragskopie geschwärzt werden.

Vereinbartes Verfahren: Die Genehmigung wird als allgemeine schriftliche Genehmigung fuer die in Anlage 2 aufgeführten Unterauftragsverarbeiter erteilt. Beabsichtigte Hinzufuegungen oder Ersetzungen teilt der Auftragnehmer dem Auftraggeber mindestens 30 Tage vor dem Einsatz individuell in Textform an die im Konto hinterlegte E-Mail-Adresse mit. Der Auftraggeber kann binnen 30 Tagen ab Zugang aus datenschutzrechtlichen Gruenden in Textform widersprechen. Bis zur Klaerung wird der neue Unterauftragsverarbeiter fuer die Auftragsdaten des widersprechenden Auftraggebers nicht eingesetzt; finden die Parteien keine zumutbare Abhilfe und ist die betroffene Funktion ohne den Anbieter nicht erbringbar, kann jede Partei die betroffene Funktion mit einer Frist von 30 Tagen zum Monatsende beenden. Ist ein sofortiger Wechsel aus Sicherheits- oder Verfuegbarkeitsgruenden erforderlich, darf der Auftragnehmer ihn vorab vollziehen und holt die individuelle Information unverzueglich nach; das Widerspruchsrecht bleibt unberuehrt.

Versionierter Freigabenachweis: Die tatsaechlich geschlossenen DPA/SCC, die bei Freigabe aktuelle Unterauftragnehmerliste, Datenregionen und Kontoeinstellungen sind Bestandteil der dokumentierten Freigabeevidenz dieser Fassung.

Aenderungen folgen dem fuer diese Version freigegebenen Informations-, Vorankuendigungs- und Widerspruchsverfahren.

§ 7 Drittlandstransfer

(1) Weisung und Kapitel V: Jede Uebermittlung von Auftragsdaten in ein Drittland oder an eine internationale Organisation, einschliesslich Weiteruebermittlungen und Fernzugriffen aus einem Drittland, erfolgt nur auf dokumentierte Weisung des Auftraggebers und unter Einhaltung von Kapitel V DSGVO. Die Einbeziehung eines in § 6 genehmigten Unterauftragsverarbeiters umfasst nur die dort transparent beschriebene Uebermittlung.

(2) Transferinstrument: Soweit kein anwendbarer Angemessenheitsbeschluss nach Art. 45 DSGVO besteht, ist vor der Uebermittlung ein geeignetes Instrument nach Art. 46 DSGVO festzulegen. Bei Verwendung der Standardvertragsklauseln des Durchfuhrungsbeschlusses (EU) 2021/914 ist das nach der tatsaechlichen Rollenbeziehung anwendbare Modul zu verwenden. Die Standardvertragsklauseln fuer Verantwortliche und Auftragsverarbeiter innerhalb der EU/des EWR nach Beschluss (EU) 2021/915 sind fuer sich allein kein Transferinstrument nach Kapitel V.

(3) Pruefung und laufende Kontrolle: Der Auftragnehmer dokumentiert Empfaenger, Verarbeitungsorte und Weiteruebermittlungen, bewertet das Schutzniveau im konkreten Uebermittlungskontext, vereinbart erforderliche zusaetzliche technische, vertragliche oder organisatorische Massnahmen und ueberprueft die Bewertung bei relevanten Aenderungen. Kann ein im Wesentlichen gleichwertiges Schutzniveau nicht hergestellt oder aufrechterhalten werden, wird die betroffene Uebermittlung nicht begonnen beziehungsweise ausgesetzt oder beendet und der Auftraggeber informiert.

Bei Anthropic und im globalen Cloudflare-Netz sind Drittlandverarbeitungen Bestandteil beziehungsweise nicht ausgeschlossen; Abs. 4 benennt die konkreten Pfade und Instrumente.

(4) Konkrete Drittlandpfade: Bei aktivierter KI-Einordnung werden ausgewaehlte Texte beziehungsweise Bildinhalte an Anthropic PBC (USA) uebermittelt; Grundlage sind die Standardvertragsklauseln nach Durchfuhrungsbeschluss (EU) 2021/914 (Module 2 und 3), die als Bestandteil des Anthropic Data Processing Addendum in dessen Vertragswerk einbezogen sind. Im Cloudflare-Netz kann Request-Inhalt transient auch ausserhalb der EU verarbeitet werden; Grundlage sind die Standardvertragsklauseln als Bestandteil des Cloudflare Customer DPA (dort Clause 6.2). Eine aktive Datenlokalisierung wird nicht behauptet. Der Auftragnehmer ueberprueft diese Bewertungen nach Abs. 3 bei relevanten Aenderungen und informiert den Auftraggeber, wenn ein Transferinstrument entfaellt.

§ 8 Pflichten und Rechte des Auftraggebers

- Festlegung und Dokumentation der Zwecke, Rechtsgrundlagen, Datenkategorien, betroffenen Personen, Speicheranforderungen und Weisungen fuer die von ihm veranlasste Verarbeitung;
- Rechtmassigkeit der Erhebung und Bereitstellung, Erfuellung der Transparenz- und Betroffenenpflichten sowie erforderlichenfalls Festlegung einer Ausnahme nach Art. 9 oder Art. 10 DSGVO;
- Pruefung der hinreichenden Garantien des Auftragnehmers und seiner Unterauftragnehmer sowie Erteilung der erforderlichen Genehmigungen;
- Festlegung der erforderlichen Sicherheit und Mitteilung besonderer Risiken, Schutzbedarfe, gesetzlicher Fristen oder Aufbewahrungspflichten;
- Verantwortung fuer Berechtigung, Inhalt und Datenminimierung bei der Pruefung fremder Domains, Wettbewerber, Dokumente oder Kommunikationskanaele und bei der Auswahl von Export-, CMS-, Webhook-, Slack- oder Teams-Empfaengern;

- Information des Auftragnehmers ueber unrichtige Daten, geaenderte Weisungen und die Beendigung eines Zwecks oder einzelnen Mandantenverhaeltnisses.

Der Auftraggeber kann waehrend der Verarbeitung weitere dokumentierte Weisungen erteilen, Informationen nach § 11 verlangen, Audits veranlassen und die Verarbeitung bei einer behaupteten Nichteinhaltung im erforderlichen Umfang aussetzen lassen.

§ 9 Anfragen betroffener Personen

(1) Eingang: Erhaelt der Auftragnehmer eine Anfrage einer betroffenen Person nach Kapitel III DSGVO, unterrichtet er den Auftraggeber unverzueglich ueber den vereinbarten Kontaktweg. Er beantwortet die Anfrage nicht selbst, ausser der Auftraggeber hat ihn hierzu dokumentiert angewiesen oder eine gesetzliche Pflicht verlangt dies.

(2) Entscheidung und Zuordnung: Der Auftraggeber entscheidet ueber Identitaetspruefung, Zulaessigkeit, Umfang und Antwort. Er bezeichnet in seiner Weisung soweit moeglich Organisation, Mandant, Domain, Scan, Datei oder sonstigen Datenbestand; der Auftragnehmer legt gegenueber einer anfragenden Person keine Kundenbeziehung offen, bevor der Auftraggeber die Zuordnung bestaetigt hat.

(3) Technische Unterstuetzung: Nach dokumentierter Weisung unterstuetzt der Auftragnehmer den Auftraggeber, soweit dies unter Beruecksichtigung der Art der Verarbeitung moeglich ist, insbesondere durch Suche und Zuordnung, Bereitstellung vorhandener Daten, Berichtigung von Zuordnungen oder Inhalten, Einschraenkung weiterer Verarbeitung sowie Loeschung oder Export in den technisch vorhandenen Formaten. Die gesetzlichen Antwortfristen des Auftraggebers werden durch die Einbindung des Auftragnehmers nicht verlaengert.

(4) Kanal und Fristen: Eingangskanal fuer Anfragen betroffener Personen ist kontakt@empcora.de beziehungsweise der authentifizierte Support-Kanal im Konto. Der Auftragnehmer leitet eingehende Anfragen unverzueglich, in der Regel binnen drei Arbeitstagen, an den Auftraggeber weiter. Technisch unterstuetzt werden insbesondere Suche und Zuordnung ueber Organisation, Mandant, Domain und Scan, die Bereitstellung vorhandener Daten in den Formaten des § 13 Abs. 2, die Berichtigung von Zuordnungen sowie Loeschung und Einschraenkung durch Sperrung des betroffenen Bestands.

§ 10 Datenschutzverletzungen und Unterstuetzung nach Art. 32 bis 36 DSGVO

(1) Meldung: Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes von Auftragsdaten unverzueglich nach Bekanntwerden ueber den vereinbarten Sicherheitskontakt; Meldungen des Auftraggebers koennen bis zur Freigabe eines gesonderten Kanals an kontakt@empcora.de gerichtet werden. Eine Erstmeldung enthaelt die zu diesem Zeitpunkt verfuegbaren Angaben und wird ohne unangemessene Verzoegerung ergaenzt.

(2) Mindestangaben: Soweit moeglich nennt die Meldung:

- Art und Zeitraum der Verletzung, betroffene Systeme und Datenkategorien sowie ungefaehre Zahl betroffener Personen und Datensatze;
- Organisationen, Mandanten oder Verarbeitungsvorgaenge, die nach dem aktuellen Kenntnisstand betroffen sind;
- Name und Kontaktdaten einer Anlaufstelle fuer weitere Informationen;
- wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Eindämmungs-, Behebungs- und Abhilfemassnahmen.

(3) Zusammenarbeit: Der Auftragnehmer sichert relevante Informationen, dokumentiert den Vorfall und unterstuetzt den Auftraggeber unter Beruecksichtigung der Art der Verarbeitung und der verfuegbaren Informationen bei Risikobewertung, Meldungen nach Art. 33 DSGVO und Benachrichtigungen nach Art. 34 DSGVO. Er meldet ausserdem gesetzlich zulaessige Behoerdenanfragen und erhebliche Nichteinhaltungen, soweit Auftragsdaten betroffen sind.

(4) Weitere Unterstuetzung: Auf dokumentierte Anfrage stellt der Auftragnehmer die fuer die Pflichten nach Art. 32 bis 36 DSGVO vorhandenen Informationen zur Verfuegung und unterstuetzt insbesondere bei Sicherheitsbewertung, Datenschutz-Folgenabschaetzung, vorheriger Konsultation und der Beurteilung von Datenrichtigkeit oder Schutzmassnahmen.

(5) Kontakt und Frist: Sicherheitskontakt ist kontakt@empcora.de. Der Auftragnehmer meldet eine Verletzung des Schutzes von Auftragsdaten ohne unangemessene Verzoegerung, spaetestens 48 Stunden nach Bekanntwerden, und ergaenzt die Meldung fortlaufend um neue Erkenntnisse. Vorfaelle werden einschliesslich Zeitverlauf, Bewertung und Massnahmen dokumentiert; dieselbe Meldepflicht gilt fuer Vorfaelle bei Unterauftragsverarbeitern, sobald sie dem Auftragnehmer bekannt werden.

§ 11 Kontroll- und Auditrechte

(1) Informationen: Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfuegung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind. Dazu koennen die relevanten Teile des Verzeichnisses der Verarbeitungstaetigkeiten, System- und

Datenorte, Zugriffsrollen, TOM, Aufbewahrungs- und Loeschverfahren, Empfaenger, Unterauftragnehmer, Transfers, Vorfalldaten und geeignete aktuelle Pruefnachweise gehoeren. Nicht vorhandene Zertifizierungen oder Pruefungen werden nicht behauptet.

(2) Audits und Inspektionen: Der Auftraggeber darf die erfasste Verarbeitung in angemessenen Abstaenden und bei konkreten Anzeichen einer Nichteinhaltung selbst oder durch einen von ihm beauftragten unabhangigen und zur Vertraulichkeit verpflichteten Pruefer auditieren. Die Pruefung kann Dokumente, Remote-Nachweise und, soweit fuer den Kontrollzweck erforderlich, eine Inspektion der einschlaegigen Raeume oder Systeme umfassen. Die Parteien stimmen Umfang, Termin und Sicherheitsvorkehrungen in gutem Glauben ab; bei einem dringenden Sicherheitsvorfall darf eine sonst angemessene Vorankuendigung verkuerzt werden.

(3) Zusammenarbeit: Audits sollen fremde Daten, Geschäftsgeheimnisse, Systemverfuegbarkeit und Rechte anderer Kunden schonen, duerfen aber das gesetzliche Kontrollrecht nicht leerlaufen lassen. Der Auftragnehmer wirkt mit, dokumentiert festgestellte Abweichungen und informiert ueber Abhilfemassnahmen. Gesetzliche Befugnisse von Aufsichtsbehoerden bleiben unberuehrt.

(4) Vereinbartes Verfahren: Regelaudits finden hoechstens einmal je Vertragsjahr statt und werden mindestens 30 Tage vorher angekuendigt; sie werden vorrangig durch Bereitstellung von Dokumenten, Konfigurations- und Protokollauszuegen ueber einen gesicherten Kanal erfuellt. Eine Pruefung vor Ort ist bei konkreten Anhaltspunkten einer Nichteinhaltung oder nach einem meldepflichtigen Vorfall moeglich und wird gemeinsam terminiert. Jede Partei traegt die ihr entstehenden Kosten selbst. Fuer Unterauftragsverarbeiter stellt der Auftragnehmer die ihm vorliegenden Pruef- und Vertragsnachweise nach § 6 bereit.

§ 12 Haftung

Die gesetzliche Verantwortlichkeit und Haftung der Parteien, insbesondere nach Art. 82 DSGVO, bleibt unberuehrt. Ergaenzende Haftungsregelungen des Hauptvertrags gelten nur, soweit sie zwingende Rechte betroffener Personen oder gesetzliche Verantwortlichkeiten nicht beschraenken. Diese Vereinbarung enthaelt keine Zusage einer Rechtssicherheit, Zertifizierung oder Fehlerfreiheit der technischen Pruefergebnisse.

§ 13 Beendigung der Auftragsverarbeitung

(1) Wahl und Weisung: Der Auftraggeber kann vor oder bei Beendigung der jeweiligen Verarbeitungsleistung in Textform zwischen Rueckgabe und Loeschung der Auftragsdaten waehlen. Die Weisung muss den betroffenen Bestand bezeichnen; fehlt sie, fordert der Auftragnehmer sie ueber den vereinbarten Kontaktweg an. Bis zum Abschluss verarbeitet der Auftragnehmer die Daten nur fuer Rueckgabe, Sicherheit, Loeschung und gesetzlich zwingende Aufbewahrung.

(2) Rueckgabe: Der Auftragnehmer stellt die Auftragsdaten in den fuer die jeweilige Funktion tatsaechlich vorhandenen Formaten bereit. Der aktuelle Produktstand erzeugt insbesondere Berichte oder Teilauszuege als PDF, JSON, CSV oder XLSX; dies ist noch kein Nachweis eines vollstaendigen, strukturierten Exports aller Scan-, Mandanten-, Ausnahme-, Nachweis-, Datei- und Historienbestaende. Nach bestaetigter Rueckgabe werden bestehende Kopien nach Absatz 3 geloescht, soweit keine gesetzliche Ausnahme greift.

(3) Loeschung und Bestaetigung: Nach einer Loeschweisung oder abgeschlossener Rueckgabe loescht der Auftragnehmer die betroffenen produktiven Auftragsdaten und vorhandenen Kopien sicher und bestaetigt Abschluss und Umfang. Daten in nicht selektiv veraenderbaren Sicherungen werden bis zur planmaessigen Ueberschreibung fuer andere Zwecke gesperrt und bei einer Wiederherstellung nicht wieder in die aktive Verarbeitung uebernommen.

(4) Gesetzliche Ausnahme: Verlangt Unionsrecht oder das Recht eines Mitgliedstaats die weitere Speicherung bestimmter Auftragsdaten, informiert der Auftragnehmer den Auftraggeber, soweit zulaessig, ueber Rechtsgrundlage, Datenkategorie, Zweck und voraussichtliche Dauer. Diese Daten werden von der sonstigen Verarbeitung getrennt und nur fuer die gesetzliche Pflicht verwendet. Eigene Abrechnungs-, Sicherheits- oder Vertragsnachweise nach § 1 Abs. 3 sind keine aufgrund dieser AVV aufbewahrten Auftragsdaten.

(5) Vereinbarter Vollzug: Loeschung oder Rueckgabe nach Abs. 1 bis 3 wird als dokumentierter Vorgang ausgefuehrt und dem Auftraggeber binnen 30 Tagen nach Zugang der vollstaendigen Weisung in Textform bestaetigt; die Bestaetigung benennt den betroffenen Bestand. Der Export erfolgt in den in Abs. 2 genannten, tatsaechlich vorhandenen Formaten; ein darueber hinausgehendes Exportformat wird nicht zugesagt. Fuer Sicherungskopien gilt Abs. 3; eine sofortige Loeschung in Sicherungen wird nicht zugesagt.

§ 14 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieser AVV unwirksam sein, bleibt die Wirksamkeit der uebrigen Bestimmungen unberuehrt.

(2) Im Konfliktfall haben fuer die Verarbeitung personenbezogener Daten die Bestimmungen dieser AVV Vorrang vor dem Hauptvertrag. Zwingende Rechte und Pflichten aus der DSGVO werden durch diese Rangfolge nicht beschraenkt.

Anlage 1, Technische und organisatorische Maßnahmen (TOM)

Die nachfolgende TOM-Anlage verbindet die im Code nachvollziehbaren Kontrollen mit den fuer diese Version freigegebenen Betreiberbelegen der produktiven Konfiguration.

- **Mandanten- und Berechtigungsgrenzen (CODE_VERIFIED):** Serverseitige orgId-/Rollenpruefungen an geschuetzten Konto-, Scan- und Exportpfaden.
- **Authentisierung und Missbrauchsschutz (CODE_VERIFIED):** Passwoerter werden gehasht; ausgewaehlte kurzlebige Nachweise und Rate-Limit-/IP-Schluessel werden gehasht oder HMAC-pseudonymisiert. Betriebsnotwendig wieder lesbare TOTP-, E-Mail-, Domain-, Embed-, Webhook- und Provider-Secrets sind davon ausdruecklich nicht umfasst; deren Ablage ist produktiv belegt: Secrets-Dateien mit Modus 600/700, Zugriff nur Betreiber-Systemkonto (Nachweis 19.08.2026, docs/avv-betriebsnachweis-2026-08-19.md).
- **Datenminimierung fuer Scan-URLs und Embeds (CODE_VERIFIED):** Credentials, Tracking-/Token-/Session-Parameter werden an neuen Scan-Persistenzgrenzen entfernt; Embed-Responses setzen no-referrer.
- **Aufbewahrung und Loeschung (CODE_VERIFIED):** Der allgemeine Aufbewahrungs-Cron folgt dem zentralen Aufbewahrungs-SSOT (src/lib/retention-policy.ts). Loeschung und Rueckgabe je Bestand erfolgen als dokumentierter Vorgang mit Textform-Bestaetigung binnen 30 Tagen (§ 13 Abs. 5; Partnerfassung ergaenzend P 5 Abs. 4), vertraglich zugesagt ist das Verfahren, kein Selbstbedienungs-Knopf. Sicherungen: turnusmaessige Ueberschreibung, keine selektive Backup-Loeschung zugesagt (§ 13 Abs. 3).
- **Transport, Edge, Backups und Wiederanlauf (CODE_VERIFIED):** Am 19.08.2026 auf dem Produktivsystem erhoben: TLS am Edge (Let's Encrypt, gueltig), Datenbank/Cache/Docling ausschliesslich Loopback-gebunden, taegliches Voll-Backup (DB, Uploads, Konfiguration) um 03:40 mit protokolliertem woeentlichem Restore-Test in eine Wegwerf-Datenbank (docs/avv-betriebsnachweis-2026-08-19.md).

Freigabenachweis dieser Version: aktueller Hetzner-Standort und AVV, Admin-/SSH-/Datenbank-Berechtigungen, TLS-/Cloudflare-Zonenexport, Backup-Zeitplan und verschluesselte Speicherorte, erfolgreicher Restore-Test, Incident-Kontaktweg, Patch-/Vulnerability-Prozess sowie die tatsaechliche Logrotation. Nicht belegte Zertifizierungen, Penetrationstest-Intervalle oder biometrische Zutrittsdetails sind bewusst nicht Vertragsbestandteil dieser Fassung.

Anlage 2, Liste der Unterauftragsverarbeiter

Die fuer diese Version freigegebenen Unterauftragnehmer sind in § 6 aufgefuehrt. Anlage 2 ist mit dem freigegebenen Aenderungshinweis-Verfahren und den belegten produktiven Anbieter-/Accountdaten verbunden.

Elektronische Annahme: Der geschuetzte Konto-Pfad dokumentiert die konkrete Version, Fassung, Organisation, handelnde Person, Annahmezeit und SHA-256-Dokumentidentitaet in einem unveraenderlichen Nachweis.