empcora

RECHTSDOKUMENT · ART. 28 DSGVO

Auftragsverarbeitungsvereinbarung (AVV)

Version: 2026-08-02-review.1 · Stand: 2. August 2026 · Status: REVIEW_DRAFT

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

REVIEW-ENTWURF — NICHT ZUR ANNAHME FREIGEGEBEN. Diese Fassung ist noch nicht extern rechtlich geprueft. Vertragsnachweise der Unterauftragnehmer, Drittlandtransfers und produktive TOM-Konfigurationen sind offene Freigabe-Gates. Eine Unterschrift oder Online-Bestaetigung dieser Fassung begruendet ueber Empcora derzeit keinen AVV-Abschluss.

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.

Nach vollständiger interner Quellen-, Vertrags- und Konfigurationsevidenz sowie ausdrücklicher Owner-Freigabe soll diese Auftragsverarbeitungsvereinbarung („AVV") zwischen dem oben genannten Verantwortlichen (Auftraggeber) und dem Auftragnehmer geschlossen werden. Sie konkretisiert die datenschutzrechtlichen Pflichten der Parteien für die Verarbeitung personenbezogener Daten im Rahmen des Empcora-SaaS-Nutzungsvertrags (nachfolgend „Hauptvertrag"). Die AVV wird erst in einer als APPROVED gekennzeichneten, technisch zur Annahme freigeschalteten Fassung wirksam.

§ 1 Gegenstand und Dauer der Auftragsverarbeitung

(1) Gegenstand: Der Auftragnehmer verarbeitet im Auftrag des Verantwortlichen personenbezogene Daten zur Bereitstellung der Empcora-SaaS-Plattform. Die Verarbeitung umfasst insbesondere:

- Crawlen öffentlich zugänglicher Webseiten der vom Verantwortlichen zur Prüfung angegebenen Domains
- Analyse der Inhalte auf EmpCo-relevante Werbeaussagen
- Erzeugung technischer Risikoberichte und Exporte (PDF, JSON, CSV)
- Speicherung der Scan-Ergebnisse für 24 Monate
- KI-gestützte Einordnung problematischer Aussagen mittels Anthropic Claude API
- Versand von Benachrichtigungen über einen eigenen E-Mail-Server

(2) Dauer: Die Verarbeitung folgt der Laufzeit des Hauptvertrags und dauert bis zur vertragsgemaessen Rueckgabe oder Loeschung der Auftragsdaten. Fortgeltende gesetzliche Pflichten und konkrete Beendigungsfolgen sind vor Freigabe mit dem Hauptvertrag abzugleichen.

§ 2 Art und Zweck der Verarbeitung

(1) Art der Verarbeitung: Erheben (Crawling), Speichern, Auslesen, Verändern (Bewertung), Übermitteln (an KI-API zur Einordnung), Löschen.

(2) Zweck: Bereitstellung des technischen Risiko-Pre-Checks nach Vorgabe des Verantwortlichen, Erfüllung des SaaS-Hauptvertrags.

§ 3 Art der personenbezogenen Daten

Verarbeitet werden folgende Datenkategorien:

- **Stammdaten Verantwortlicher:** Name, E-Mail, Firma und Anschrift, soweit sie fuer Weisungen, Support oder Vertragsdurchfuehrung benoetigt werden
- **Inhalte gescannter Domains:** öffentliche Webseiten-Texte, Meta-Tags, ggf. beiläufig enthaltene personenbezogene Daten Dritter (z. B. Mitarbeiternamen, Impressums-Daten, Kontakt-Adressen)
- **Scan-Ergebnisse:** erkannte Claims, Bewertungen, KI-gestützte Einordnung
- **Technische Daten:** Sicherheits- und Verbindungsmetadaten; Rate-Limit-Kennungen werden in der Anwendung HMAC-pseudonymisiert. Edge-/Proxy-Logs sind gemaess Datenflussmatrix und Produktivkonfiguration gesondert zu verifizieren.

§ 4 Kategorien betroffener Personen

- Mitarbeiter und Vertretungsberechtigte des Verantwortlichen
- Mitarbeiter, Geschäftsführer und Kontaktpersonen der Inhaber gescannter Domains
- Sonstige natürliche Personen, deren Daten beiläufig auf den gescannten Webseiten enthalten sind

§ 5 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, die Verarbeitung gemäß folgenden Grundsätzen durchzuführen:

- Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO)
- Verpflichtung der Mitarbeiter zur Vertraulichkeit (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO)
- Umsetzung angemessener technischer und organisatorischer Maßnahmen (Art. 32 DSGVO, siehe Anlage 1)
- Unterstützung des Verantwortlichen bei der Wahrnehmung von Betroffenenrechten
- Unterstützung bei Datenschutzverletzungen und den Pflichten nach Art. 32 bis 36 DSGVO; Information des Verantwortlichen unverzueglich nach Kenntnis mit den jeweils verfuegbaren erforderlichen Angaben
- Löschung oder Rückgabe aller Daten nach Beendigung des Auftrags nach Wahl des Verantwortlichen
- Bereitstellung aller für Audits erforderlichen Informationen (Art. 28 Abs. 3 lit. h DSGVO)

§ 6 Unterauftragsverarbeiter (Sub-Processors)

Fuer die von dieser AVV erfasste Scan-Verarbeitung ist folgende Arbeitsliste vorgesehen. Sie ist erst nach Abschluss der jeweils ausgewiesenen Vertrags-/Konfigurationspruefung und in einer APPROVED-Fassung verbindlich. 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 CONTRACT_REVIEW_REQUIRED	Vom Betreiber gewaehlter Produktstandort Deutschland; Accountbeleg vor Freigabe pruefen	**Server-, Datenbank-, Cache- und Mail-Infrastruktur** Scan-Inhalte, Ergebnisdaten, Konto- und technische Betriebsdaten *Kein Drittlandtransfer fuer den gewaehlten DE/EU-Produktstandort erwartet; vertraglich pruefen* Empcora-Loeschkonzept; Backups und Provider-Metadaten vertraglich/config-seitig pruefen **Freigabe-Gate:** Aktuell geschlossene Hetzner-AVV und konkreten Produktstandort im Kundenkonto exportieren.
Cloudflare, Inc. CONFIG_REVIEW_REQUIRED	Globales Edge-Netz; EU-Grenzen nur bei tatsaechlich aktivierten Data-Localization-Funktionen	**DNS, CDN, WAF, DDoS- und Bot-Schutz** IP-Adresse, Request-URL, Header sowie Sicherheits- und Verbindungsmetadaten *Cloudflare-DPA/SCC; konkrete Account-, DPF- und Transferkonfiguration vor Freigabe pruefen* Produkt- und tarifabhaengig; Zone-, Logpush- und Analytics-Einstellungen inventarisieren **Freigabe-Gate:** DLS/CMB darf nicht als aktiv behauptet werden, bevor Entitlement und Zone-Konfiguration belegt sind.

Unterauftragsverarbeiter	Region / Status	Umfang / Transfer / Freigabe-Gate
Anthropic PBC CONTRACT_REVIEW_REQUIRED	USA	**Claude API fuer Text-Einordnung und optionale Bild-Text-Extraktion** Ausgewaehlte Werbetexte/Kontext; bei Bild-Audits Bildinhalt, in dem Personenbezug nicht ausgeschlossen ist *Commercial DPA und SCC; tatsaechlichen Empcora-Accountvertrag vor Freigabe sichern* Standard-API: Loeschung von Ein-/Ausgaben innerhalb 30 Tagen, mit dokumentierten Ausnahmen; ZDR nur bei gesonderter Vereinbarung **Freigabe-Gate:** Kein ZDR behaupten. API-Workspace, Features, DPA, SCC und aktuelle Subprocessor-Liste belegen.

Freigabe-Gate: Vor produktiver Annahme muessen die tatsaechlich geschlossenen DPA/SCC, aktuellen Unterauftragnehmerlisten, Datenregionen und Kontoeinstellungen dokumentiert werden. Eine Anbieter-Webseite oder Produktverfuegbarkeit belegt keine Aktivierung im Empcora-Konto.

Eine spaetere APPROVED-Fassung muss das konkrete Informationsverfahren, eine angemessene Vorankuendigungsfrist, ein Widerspruchsverfahren und die Folgen eines berechtigten Widerspruchs festlegen. Die blosse Online-Veroeffentlichung einer geaenderten Liste ersetzt die individuelle Information nicht.

§ 7 Drittlandstransfer

Bei Anthropic und im globalen Cloudflare-Netz sind Drittlandverarbeitungen nicht ausgeschlossen. Vor Freigabe sind Transferrolle, Importeur-/Exporteur-Modul, SCC 2021/914, zusaetzliche Massnahmen, aktuelle Unterauftragnehmer sowie die tatsaechliche Cloudflare-Datenlokalisierung zu dokumentieren. Diese REVIEW-Fassung behauptet weder ein abgeschlossenes TIA noch eine aktive Data Localization Suite.

§ 8 Pflichten des Verantwortlichen

- Erteilung dokumentierter Weisungen (Standard-Weisung ist die Nutzung des Dienstes im Rahmen der gebuchten Plan-Funktionen)
- Sicherstellung der rechtmäßigen Verarbeitung im Verhältnis zu betroffenen Personen (Information, ggf. Einwilligung)
- Erfüllung der Informationspflichten gegenüber den Inhabern gescannter Domains und deren betroffenen Personen
- Sofern der Verantwortliche Domains Dritter prüfen lässt: eigene rechtliche Grundlage (Auftrag, Einwilligung oder berechtigtes Interesse) im Verhältnis zum jeweiligen Domain-Inhaber
- Benennung eines Datenschutzbeauftragten, sofern nach Art. 37 DSGVO oder § 38 BDSG erforderlich

§ 9 Anfragen betroffener Personen

Wenden sich betroffene Personen direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und unterstützt diesen bei der fristgerechten Beantwortung. Eigenständige Auskünfte erteilt der Auftragnehmer nicht, es sei denn, der Verantwortliche hat zugestimmt.

§ 10 Mitteilungspflichten

Der Auftragnehmer informiert den Verantwortlichen unverzueglich nach Kenntnis und stellt die jeweils verfuegbaren erforderlichen Angaben bereit ueber:

- Datenschutzverletzungen im Sinne des Art. 33 DSGVO
- Behördenanfragen, soweit gesetzlich zulässig
- rechtswidrige Anweisungen anderer Stellen
- Ergebnisse von Datenschutz-Audits, soweit relevant

§ 11 Kontroll- und Auditrechte

Der Verantwortliche ist berechtigt, im erforderlichen Umfang die Einhaltung der gesetzlichen und vertraglichen Vorgaben zu ueberpruefen. Eine APPROVED-Fassung muss ein praktikables Verfahren fuer Informationen, Nachweise und erforderlichenfalls

Inspektionen festlegen, ohne nicht vorhandene Zertifizierungen zu behaupten.

§ 12 Haftung

Die Haftung der Vertragsparteien richtet sich nach Art. 82 DSGVO sowie den allgemeinen Bestimmungen des Hauptvertrags. Der Auftragnehmer haftet insbesondere für die korrekte Umsetzung der technischen und organisatorischen Maßnahmen (Anlage 1) sowie der Anweisungen des Verantwortlichen.

§ 13 Beendigung der Auftragsverarbeitung

Bei Beendigung der AVV wird der Auftragnehmer nach Wahl des Verantwortlichen alle ihm überlassenen Daten löschen oder zurückgeben. Eine Datenrückgabe erfolgt im Format JSON oder CSV (siehe Ziffer 17a der Datenschutzerklärung unter empcora.de/datenschutz). Bestehende gesetzliche Aufbewahrungspflichten bleiben unberührt (z. B. Rechnungen nach § 147 AO).

§ 14 Schlussbestimmungen

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

(2) Im Konfliktfall zwischen dieser AVV und dem Hauptvertrag haben die Bestimmungen dieser AVV Vorrang.

(3) Es gilt deutsches Recht. Der Gerichtsstand richtet sich nach dem Hauptvertrag (siehe AGB § 14, empcora.de/agb).

Anlage 1 — Technische und organisatorische Maßnahmen (TOM)

Die nachfolgende Evidenzliste trennt im Code nachvollziehbare Kontrollen von produktiven Konfigurationen, fuer die vor Freigabe ein Betreiberbeleg erforderlich ist. Sie ersetzt noch keine vollstaendig abgenommene TOM-Anlage.

- **Mandanten- und Berechtigungsgrenzen (CODE_VERIFIED):** Serverseitige orgId-/Rollenpruefungen an geschuetzten Konto-, Scan- und Exportpfaden.
- **Authentisierung und Missbrauchsschutz (CODE_VERIFIED):** Gehashte Passwoerter/Token, MFA-Pfade, Rate-Limits; Rate-Limit-Schluessel werden HMAC-pseudonymisiert.
- **Datenminimierung fuer Scan-URLs und Embeds (CODE_VERIFIED):** Credentials, Tracking-/Token-/Session-Parameter werden an neuen Scan-Persistenzgrenzen entfernt; Embed-Responses setzen no-referrer.
- **Loeschfristen (CODE_VERIFIED):** Taeglicher Retention-Cron nutzt den zentralen Retention-SSOT; Ausfuehrung und Backups sind betrieblich zu ueberwachen.
- **Transport, Edge, Backups und Wiederanlauf (CONFIG_REVIEW_REQUIRED):** Produktive TLS-, Cloudflare-, Backup-, Restore- und Zugriffskonfiguration ist durch signierte Exporte/Protokolle nachzuweisen.

Vor Freigabe nachzuweisen: 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 dieses Entwurfs.

Anlage 2 — Liste der Unterauftragsverarbeiter

Die vorgesehenen Unterauftragnehmer und ihre offenen Nachweise sind in § 6 aufgefuehrt. Vor APPROVED muss Anlage 2 versioniert, mit einem individuellen Aenderungshinweis-Verfahren verbunden und gegen die tatsaechlichen produktiven Anbieter-/Accountdaten abgeglichen werden.

Keine Unterschrift / keine Online-Annahme: Diese REVIEW-Fassung ist nur zur externen Pruefung bestimmt. Der spaetere Annahmekanal wird erst nach Freigabe einer konkreten Version mit dokumentierter SHA-256-Pruefsumme aktiviert.