

Vertrag zur Auftragsverarbeitung

Erstellt am 16. Oktober 2026

Dieser Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO ergänzt die [Allgemeinen Geschäftsbedingungen](#) und gilt für jede Nutzung von HORAKA, bei der personenbezogene Daten im Auftrag des Kunden verarbeitet werden.

Vertragsparteien

Verantwortlicher (nachfolgend „Auftraggeber“) ist der Kunde, der den Arbeitsbereich angelegt hat, mit den Angaben in seinem Konto.

Auftragsverarbeiter (nachfolgend „Auftragnehmer“) ist:

giant Computer Systems
Inhaber Marc Breuer
Am Altengraben 23
90768 Fürth
Deutschland
E-Mail: info@horaka.com

Präambel

Der Auftraggeber nutzt HORAKA, um Arbeitszeiten für Kunden und Projekte zu erfassen, auszuwerten und abzurechnen, allein oder mit seinen Mitarbeitern. Er entscheidet allein über Zwecke und Mittel dieser Verarbeitung und ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftragnehmer verarbeitet die Daten ausschließlich in seinem Auftrag.

Nicht Gegenstand dieses Vertrags sind die Daten, die der Auftragnehmer für eigene Zwecke verarbeitet, insbesondere die Bestands-, Vertrags- und Abrechnungsdaten des Auftraggebers selbst. Insoweit ist der Auftragnehmer eigener Verantwortlicher; es gilt seine [Datenschutzerklärung](#).

§ 1 Gegenstand und Dauer

1.1 Gegenstand des Auftrags ist der Betrieb von HORAKA für den Arbeitsbereich des Auftraggebers: Speicherung und Verarbeitung der Zeiteinträge und Stammdaten, Verwaltung der Konten seiner Mitarbeiter, Berechnung von Rundung, Pausen und Beträgen, Erstellung von Berichten und Exporten, Versand von Mails und Mitteilungen sowie die Bereitstellung der API und der vom Auftraggeber eingerichteten Webhooks und Verbindungen.

1.2 Die Dauer dieses Vertrags entspricht der Laufzeit des Nutzungsvertrags. Er endet, ohne dass es einer Kündigung bedarf, mit der endgültigen Löschung der Daten nach § 9.

§ 2 Art und Zweck der Verarbeitung, Datenarten, betroffene Personen

2.1 Art der Verarbeitung: Erheben, Erfassen, Speichern, Ordnen, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln an die vom Auftraggeber bestimmten Empfänger, Einschränken und Löschen.

2.2 Zweck: Erfassung, Auswertung und Abrechnung von Arbeitszeiten für den Auftraggeber.

2.3 Datenarten:

- Konten der Mitarbeiter: Name, E-Mail-Adresse, Rolle, Sprache, Zeitzone, Anmeldedaten (Passwort als Hash, Zwei-Faktor und Passkeys, sofern genutzt);
- Zeiteinträge: Beginn, Ende, Dauer, Pausen, Projekt, Tätigkeit, Notizen, Schlagworte, Stundensätze, Beträge und Abrechnungsstatus;
- Stammdaten: Kunden, Projekte und Tätigkeiten des Auftraggebers, einschließlich der dort hinterlegten Namen und Notizen;
- Protokolle: Aktivitätsprotokoll (wer hat wann was geändert), Zustellprotokolle von Webhooks, technische Kennungen von Geräten, Tokens und Push-Abonnements;
- Inhalte von Importen und Exporten, die der Auftraggeber anlegt.

2.4 Kategorien betroffener Personen: der Auftraggeber und seine Mitarbeiter, deren Kunden und Ansprechpartner, soweit der Auftraggeber sie in Stammdaten oder Notizen erfasst.

2.5 Der Auftragnehmer verarbeitet diese Daten nicht für eigene Zwecke. Sie werden insbesondere nicht für Werbung und nicht zum Training von Systemen künstlicher Intelligenz verwendet.

§ 3 Weisungsrecht

3.1 Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die Weisungen ergeben sich aus diesem Vertrag, den AGB und den Einstellungen, die der Auftraggeber in HORAKA vornimmt; letztere gelten als Einzelweisung in elektronischer Form.

3.2 Weitergehende Weisungen erteilt der Auftraggeber in Textform an die oben genannte Adresse. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

3.3 Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er dies dem Auftraggeber unverzüglich mit. Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

3.4 Eine Verarbeitung außerhalb der Weisung erfolgt nur, wenn der Auftragnehmer hierzu nach dem Recht der Union oder der Mitgliedstaaten verpflichtet ist; in diesem Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet.

§ 4 Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verpflichtet die zur Verarbeitung befugten Personen zur Vertraulichkeit, soweit sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.

4.2 Der Auftragnehmer führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

4.3 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine Aufsichtsbehörde Maßnahmen gegen ihn ergreift, die die Verarbeitung im Auftrag betreffen.

4.4 Der Auftragnehmer hat keinen Datenschutzbeauftragten benannt; die Voraussetzungen des Art. 37 DSGVO und des § 38 BDSG liegen nicht vor. Kontaktstelle für alle Datenschutzangelegenheiten ist die oben genannte Adresse.

§ 5 Technische und organisatorische Maßnahmen

5.1 Der Auftragnehmer trifft die in Anlage 1 beschriebenen Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragsdauer aufrecht.

5.2 Die Maßnahmen dürfen im Zuge der technischen Weiterentwicklung angepasst werden, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

§ 6 Unterauftragsverarbeiter

6.1 Der Auftraggeber erteilt hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt und werden hiermit genehmigt.

6.2 Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden auszutauschen, teilt er dies dem Auftraggeber mindestens vier Wochen vorher in Textform mit. Der Auftraggeber kann der Änderung innerhalb von zwei Wochen aus einem wichtigen datenschutzrechtlichen Grund widersprechen; in diesem Fall können beide Seiten den Nutzungsvertrag zum Zeitpunkt der Änderung kündigen.

6.3 Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter auf Datenschutzpflichten, die denen dieses Vertrags entsprechen, und bleibt dem Auftraggeber gegenüber für dessen Verhalten verantwortlich.

6.4 Nicht als Unterauftragsverarbeitung gelten Dienste, an die der Auftraggeber selbst Daten übermitteln lässt (etwa Webhooks, API-Zugriffe, EARLY), sowie Nebenleistungen, bei denen Dritte keinen Zugriff auf die Auftragsdaten haben.

§ 7 Unterstützung des Auftraggebers

7.1 Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch nachzukommen. Dafür stehen in HORAKA insbesondere der Datenexport des Arbeitsbereichs, die Auskunft je Konto, das Bearbeiten und Löschen von Einträgen und Konten sowie die Löschung des Arbeitsbereichs bereit.

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

7.3 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

§ 8 Verletzungen des Schutzes personenbezogener Daten

8.1 Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten des Auftraggebers unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntnis, in Textform.

8.2 Die Meldung enthält, soweit verfügbar, eine Beschreibung der Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Gegenmaßnahmen.

8.3 Die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen obliegen dem Auftraggeber.

§ 9 Rückgabe und Löschung

9.1 Der Auftraggeber kann seine Daten während der gesamten Laufzeit selbst als vollständigen Datenexport (JSON und CSV) herunterladen. Damit ist die Rückgabe im Sinne des Art. 28 Abs. 3 lit. g DSGVO erfüllt.

9.2 Beantragt der Auftraggeber die Löschung des Arbeitsbereichs, löscht der Auftragnehmer nach Ablauf von 14 Tagen sämtliche Auftragsdaten endgültig. Kopien in Datensicherungen werden im regulären Zyklus der Sicherung überschrieben.

9.3 Daten, für die eine gesetzliche Aufbewahrungspflicht besteht (Rechnungen und anonymisierte Abrechnungsbelege), sowie Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, darf der Auftragnehmer über das Vertragsende hinaus aufbewahren.

§ 10 Nachweise und Kontrollen

10.1 Der Auftragnehmer weist die Einhaltung der Pflichten aus diesem Vertrag auf Anfrage in geeigneter Weise nach, insbesondere durch Auskunft und Vorlage der Dokumentation der technischen und organisatorischen Maßnahmen.

10.2 Der Auftraggeber kann sich nach vorheriger Anmeldung mit angemessener Frist und während der üblichen Geschäftszeiten von der Einhaltung überzeugen. Kontrollen sind auf das erforderliche Maß zu beschränken und dürfen den Betrieb nicht unverhältnismäßig stören.

10.3 Für Kontrollen, die über eine einfache Auskunft hinausgehen und nicht durch einen konkreten Anlass veranlasst sind, kann der Auftragnehmer eine angemessene Vergütung des Aufwands verlangen.

§ 11 Ort der Verarbeitung

Die Auftragsdaten werden auf Servern in Deutschland gespeichert und verarbeitet. Bei der Auslieferung über Cloudflare werden Anfragen über Server von Cloudflare geleitet; eine Übermittlung in ein Drittland findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage der EU-Standardvertragsklauseln.

§ 12 Haftung

Es gilt Art. 82 DSGVO. Im Verhältnis der Parteien untereinander gelten ergänzend die Haftungsregelungen der AGB.

§ 13 Schlussbestimmungen

13.1 Widersprechen sich dieser Vertrag und die AGB, geht dieser Vertrag für die Verarbeitung im Auftrag vor.

13.2 Es gilt das Recht der Bundesrepublik Deutschland.

13.3 Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Zutrittskontrolle:** Die Server stehen in einem Rechenzentrum der Hetzner Online GmbH in Deutschland. Den Zutrittsschutz (Vereinzelung, Videoüberwachung, Protokollierung) gewährleistet Hetzner als Betreiberin des Rechenzentrums.
- **Zugangskontrolle:** Anmeldung mit E-Mail-Adresse und Passwort (mindestens zehn Zeichen, gespeichert nur als Hash), optional Zwei-Faktor-Anmeldung und Passkeys; Anmeldeversuche sind begrenzt. Administrative Zugänge zu den Servern sind auf den Auftragnehmer beschränkt und durch Schlüsselverfahren gesichert. Die Server sind für Webanfragen nur über Cloudflare erreichbar.
- **Zugriffskontrolle:** Rollen Inhaber, Admin und Mitglied mit abgestuften Rechten; jede Anfrage wird gegen die Berechtigung geprüft. API-Tokens tragen eingeschränkte Berechtigungen, lassen sich befristen und widerrufen und werden nur als Hash gespeichert.
- **Trennungskontrolle:** Jeder Datensatz gehört genau einem Arbeitsbereich; jede Abfrage ist auf den Arbeitsbereich des angemeldeten Kontos eingegrenzt. Test- und Produktivsystem verwenden getrennte Datenbanken mit getrennten Zugangsdaten.
- **Pseudonymisierung:** Geheimnisse wie Tokens und Links werden nur als Hash oder verschlüsselt gespeichert; Dateien liegen nicht öffentlich erreichbar.

Integrität

- **Weitergabekontrolle:** Jede Übertragung erfolgt TLS-verschlüsselt, auch zwischen Cloudflare und den Servern. Webhooks tragen eine HMAC-Signatur, Zieladressen werden gegen interne Netze geprüft. Exporte stehen nur dem Konto zum Download bereit, das sie angelegt hat.
- **Eingabekontrolle:** Änderungen an Einträgen werden mit Zeitpunkt und auslösendem Konto im Aktivitätsprotokoll gespeichert.

Verfügbarkeit und Belastbarkeit

- Regelmäßige Datensicherung der Datenbank und der Dateien.
- Zeitnahes Einspielen von Sicherheitsaktualisierungen für Betriebssystem und Anwendung.
- Überwachung der Systeme und der Hintergrundverarbeitung.

- Begrenzung der Anfragen je Konto und Token zum Schutz vor Überlastung.

Verfahren zur Überprüfung und Bewertung

- **Datenschutz durch Voreinstellung:** keine Analyse- und Trackingdienste; Mitteilungen per Web Push nur nach Einschalten durch die Person; Erinnerungen abschaltbar.
- **Automatisierte Löschroutinen:** Exporte und Importdateien nach sieben Tagen, Zustellprotokolle von Webhooks und eingehende Ereignisse nach 30 Tagen, Löschvermerke für den Abgleich nach 90 Tagen, Arbeitsbereiche nach Ablauf der Löschfrist.
- **Auftragskontrolle:** Unterauftragsverarbeiter werden nur mit einem Vertrag nach Art. 28 DSGVO eingesetzt; Weisungen werden in Textform erteilt.

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Betrieb der Server einschließlich Datenbank, Dateien und Datensicherung	Deutschland
Cloudflare Germany GmbH, Rosental 7, 80331 München	Auslieferung der Website als Proxy, Abwehr von Angriffen, Schutz der Registrierung (Turnstile)	Europäische Union; ergänzend EU- Standardvertragsklauseln
Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland	Abwicklung von Zahlungen und Rechnungen des Abos; erhält den Namen des Arbeitsbereichs sowie E-Mail-Adresse und Sprache des Inhabers, keine Zeiteinträge	Irland; Übermittlung an Stripe, Inc. (USA) auf Grundlage der EU- Standardvertragsklauseln

Mails verschickt der Auftragnehmer über seinen eigenen Mailserver; dabei ist kein weiterer Dienstleister beteiligt.

Stand: 15. Oktober 2026