Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO · Fassung 2026-09-25

> **⚠ Bitte zuerst lesen**
>
> **Dieses Dokument ersetzt keine Rechtsberatung.** Es beschreibt die technischen Gegebenheiten von Tiveo zutreffend — die rechtliche Würdigung für Ihren Betrieb kann es nicht leisten.
>
> *Sven Brunn Mediasolutions erbringt keine Rechtsdienstleistungen im Sinne von § 2 RDG.*

---

zwischen

<Unternehmen>, <Anschrift> — nachfolgend **„Verantwortlicher"** —

und

Sven Brunn Mediasolutions, Inhaber Sven Brunn Stephanusstraße 29, 41472 Neuss — nachfolgend **„Auftragsverarbeiter"** —

---

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die Software **Tiveo** zur Planung, Beantragung, Genehmigung und Dokumentation von Abwesenheiten bereit und verarbeitet dabei personenbezogene Daten in dessen Auftrag.

(2) Die Laufzeit entspricht der des zugrunde liegenden Hauptvertrags. Dieser Vertrag endet mit ihm.

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

---

§ 2 Weisungsbindung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dieser Vertrag und die Nutzung der Software stellen die Weisung dar.

(2) Weisungen erteilen der Nutzer mit der Rolle „Eigentümer" in der Software und Personen, die den Verantwortlichen vertreten dürfen; weitere weisungsberechtigte Personen kann der Verantwortliche in Textform benennen. Weisungen erfolgen in Textform an **info@tiveo.de**. Bestehen Zweifel an der Berechtigung, kann der Auftragsverarbeiter vor der Ausführung eine Bestätigung verlangen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies unverzüglich mit und darf ihre Ausführung bis zur Klärung aussetzen (Art. 28 Abs. 3 Satz 3 DSGVO).

(4) Eine Verarbeitung zu eigenen Zwecken findet nicht statt. Insbesondere werden die Daten **nicht** zur Produktverbesserung, zum Training von Modellen oder zu Werbezwecken ausgewertet.

(5) Ausgenommen von Absatz 4 sind Rückmeldungen, die Nutzer über die Rückmeldefunktion der Software selbst an den Auftragsverarbeiter richten, und Kennzahlen je Unternehmen, die der Auftragsverarbeiter für Betrieb und Abrechnung bildet: die Zahl der Plätze und der Administratoren, die Zahl der Anträge der letzten 30 Tage und der Zeitpunkt der letzten Aktivität. Für sie ist der Auftragsverarbeiter selbst verantwortlich; die Datenschutzerklärung unter tiveo.de/datenschutz/ beschreibt sie.

---

§ 3 Ort der Verarbeitung

(1) Die Daten des Verantwortlichen werden in Rechenzentren in der Bundesrepublik Deutschland gespeichert und verarbeitet. Das gilt für die Datenbank, den Dateispeicher, die Anwendungsdienste, die Auslieferung der Software und den Versand von E-Mails (Anlage 3).

(2) **Eine Ausnahme bildet der Schutz der Anmeldung vor automatisierten Zugriffen.** Dafür setzt der Auftragsverarbeiter den Dienst Cloudflare Turnstile der Cloudflare, Inc., USA, ein (Anlage 3). Beim Aufruf der Seite für Anmeldung, Registrierung und Anmeldelink überträgt der Browser technische Merkmale an Cloudflare, insbesondere die IP-Adresse, die Browserkennung und Merkmale der verschlüsselten Verbindung. Eine Verarbeitung in den USA ist dabei nicht ausgeschlossen. E-Mail-Adresse, Passwort und die Inhalte der Software erreichen Cloudflare nicht. Die Übermittlung stützt sich auf den Angemessenheitsbeschluss der Europäischen Kommission zum EU-US Data Privacy Framework (Art. 45 DSGVO), unter dem Cloudflare, Inc. zertifiziert ist.

(3) Jede weitere Übermittlung in Drittländer bedarf der vorherigen Zustimmung des Verantwortlichen in Textform und der Erfüllung der Voraussetzungen der Art. 44 ff. DSGVO.

---

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in **Anlage 2** beschriebenen Maßnahmen nach Art. 32 DSGVO.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Änderungen sind zulässig, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dem Verantwortlichen mitgeteilt.

(3) Die jeweils aktuelle Fassung ist unter `tiveo.de/sicherheit` abrufbar.

---

§ 5 Vertraulichkeit

(1) Der Auftragsverarbeiter setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b DSGVO).

(2) Die Verpflichtung besteht über das Ende der Tätigkeit hinaus fort.

§ 6 Unterauftragsverhältnisse

(1) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer ergeben sich aus **Anlage 3**. Ihrem Einsatz stimmt der Verantwortliche zu.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen **mindestens vier Wochen vorher** über die Hinzuziehung eines weiteren oder den Wechsel eines bestehenden Unterauftragnehmers. Muss ein Unterauftragnehmer kurzfristig ersetzt werden, etwa weil er ausfällt, den Vertrag beendet oder die Sicherheit es verlangt, darf der Auftragsverarbeiter ihn ohne diese Frist durch einen Unterauftragnehmer mit Verarbeitung in der Bundesrepublik Deutschland und mindestens gleichem Schutzniveau ersetzen; er informiert den Verantwortlichen dann unverzüglich, spätestens mit dem Wechsel, und Absatz 3 gilt entsprechend.

(3) Der Verantwortliche kann binnen zwei Wochen ab Zugang widersprechen. Bei Widerspruch aus sachlichem Grund darf der Auftragsverarbeiter diesen Vertrag und den Hauptvertrag mit einer Frist von einem Monat kündigen (§ 10 Abs. 2 der AGB).

(4) Der Auftragsverarbeiter verpflichtet Unterauftragnehmer auf ein Schutzniveau, das dem dieses Vertrags entspricht.

---

§ 7 Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei

a) der Beantwortung von Anfragen betroffener Personen (Art. 12–23 DSGVO), b) der Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34 DSGVO), c) der Datenschutz-Folgenabschätzung (Art. 35 DSGVO), d) der vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO).

(2) Anfragen betroffener Personen, die den Auftragsverarbeiter erreichen, werden **nicht selbst beantwortet**, sondern unverzüglich an den Verantwortlichen weitergeleitet.

(3) Die Software ermöglicht dem Verantwortlichen ohne Mitwirkung des Auftragsverarbeiters, die Daten einzusehen und zu exportieren; einen Gesamtexport aller Daten erhält er nach § 13 der AGB. Reicht das zur Beantwortung einer Anfrage nicht aus, stellt der Auftragsverarbeiter die benötigten Daten auf Anforderung bereit.

---

§ 8 Meldung von Verletzungen

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten **unverzüglich**, nachdem sie ihm bekannt geworden ist, möglichst innerhalb von 24 Stunden.

(2) Die Meldung enthält, soweit bekannt: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Liegen noch nicht alle Angaben vor, meldet er zunächst, was bekannt ist, und reicht den Rest unverzüglich nach.

(3) Die Meldung erfolgt an die vom Verantwortlichen benannte Stelle: **<Name, E-Mail>**. Solange der Verantwortliche keine Stelle benannt hat, geht sie an den Eigentümer und die Administratoren unter ihren in der Software

hinterlegten E-Mail-Adressen.

---

§ 9 Kontrollrechte

(1) Der Verantwortliche hat das Recht, die Einhaltung dieses Vertrags zu überprüfen (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Nachweis erfolgt vorrangig durch die aktuelle Fassung der technischen und organisatorischen Maßnahmen sowie durch Auskunft in Textform.

(3) Eine Vor-Ort-Kontrolle ist nach Anmeldung mit angemessener Frist während der üblichen Geschäftszeiten möglich. Sie wird so durchgeführt, dass der Betrieb nicht unverhältnismäßig beeinträchtigt wird und die Rechte anderer Kunden gewahrt bleiben.

(4) Für den Aufwand über eine Kontrolle im Kalenderjahr hinaus kann der Auftragsverarbeiter eine angemessene Vergütung verlangen.

---

§ 10 Zugriff zu Supportzwecken

(1) Ein Zugriff auf personenbezogene Daten des Verantwortlichen erfolgt ausschließlich

a) auf Anlass des Verantwortlichen, b) nach dessen ausdrücklicher Freigabe in der Software, c) zeitlich begrenzt, d) vollständig protokolliert.

(2) Das Protokoll dieser Zugriffe ist für den Verantwortlichen in der Software einsehbar.

(3) Unberührt bleibt der administrative Zugriff auf die Datenbank, der für den Betrieb technisch erforderlich ist. Er erfolgt ausschließlich auf Anlass und unterliegt der Verpflichtung auf Vertraulichkeit nach § 5. Anders als der Zugriff über die Software wird er nicht vollständig protokolliert: Änderungen an protokollierten Daten hält das Protokoll der Software fest, lesende Zugriffe nicht.

> Dieser Paragraph beschreibt keine Absichtserklärung, sondern eine technische Eigenschaft: **Über die Anwendung** ist ein Zugriff auf personenbezogene Daten ohne Freigabe des Verantwortlichen nicht möglich. Die Freigabe wird in den Einstellungen erteilt, gilt für eine vom Verantwortlichen bestimmte Dauer von höchstens acht Stunden und kann jederzeit widerrufen werden. Jeder Schritt — Anfrage, Freigabe, Ablehnung, Widerruf und jede tatsächliche Einsicht — hinterlässt einen Eintrag, den der Verantwortliche selbst einsehen kann und den der Auftragsverarbeiter über die Anwendung nicht löschen kann.
>
> Absatz 3 ist die ehrliche Einschränkung dazu: Wer eine Datenbank betreibt, kann sie administrativ erreichen. Das lässt sich nicht wegprogrammieren, und ein Vertrag, der es behauptet, wäre an der Stelle falsch, an der er am meisten zählt.

---

§ 11 Löschung und Rückgabe

(1) Nach dem Ende des Hauptvertrags bleibt der Zugang während eines Abrufzeitraums von **30 Tagen** bestehen (§ 14 Abs. 2 der AGB). In dieser Zeit kann der Verantwortliche seine Daten mit den Exportfunktionen der Software herunterladen und einen Gesamtexport aller Daten einschließlich der hochgeladenen Dateien anfordern (§ 13 Abs. 1 der AGB). Stellt der Auftragsverarbeiter den Dienst insgesamt ein, kann er den Zugang dadurch ersetzen, dass er den Gesamtexport zum Herunterladen bereitstellt (§ 14 Abs. 2 der AGB).

(2) Danach löscht der Auftragsverarbeiter die Daten unverzüglich, spätestens 30 Tage nach Ablauf des Abrufzeitraums; hat der Verantwortliche einen Gesamtexport angefordert, frühestens 14 Kalendertage nach dessen Bereitstellung (§ 14 Abs. 3 der AGB). Die Löschung wird von Hand ausgelöst und umfasst den Datenbestand in der Datenbank, die hochgeladenen Dateien und die Benutzerkonten, die danach keinem Unternehmen mehr angehören. Sie wird auf Verlangen in Textform bestätigt.

(3) Sicherungen bewahrt der Auftragsverarbeiter **höchstens 90 Tage** nach ihrer Erstellung auf und löscht sie danach, einschließlich aller Kopien. Aus einer vorhandenen Sicherung lassen sich die Daten eines einzelnen Verantwortlichen nicht gezielt entfernen; sie verschwinden mit der Löschung der Sicherung und werden bis dahin nicht wiederhergestellt. Muss eine Sicherung zurückgespielt werden, löscht der Auftragsverarbeiter die darin enthaltenen Daten beendeter Verträge unverzüglich erneut.

(4) Unberührt bleiben gesetzliche Aufbewahrungspflichten, insbesondere nach § 257 HGB und § 147 AO für Rechnungen und Zahlungsbelege. Diese enthalten keine Beschäftigtendaten. Als eigene Vertragsunterlage bewahrt der Auftragsverarbeiter außerdem den Nachweis nach § 14 Abs. 4 der AGB auf, welche Fassungen der AGB und dieses Vertrags wann und von wem angenommen wurden; diesen verarbeitet er als Verantwortlicher, nicht im Auftrag.

(5) Einzelheiten regelt das Löschkonzept (**Anlage 4**).

(6) Überträgt der Auftragsverarbeiter den Hauptvertrag nach § 19 der AGB und kündigt der Verantwortliche deshalb, erhält der Übernehmer dessen Daten nicht, auch nicht in Sicherungen. Sie werden vor der Übertragung nach den Absätzen 1 und 2 bereitgestellt und gelöscht.

---

§ 12 Haftung und Schlussbestimmungen

(1) Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO. Im Verhältnis der Parteien zueinander, auch für den Ausgleich nach Art. 82 Abs. 5 DSGVO, gilt die Haftungsregel des Hauptvertrags (§ 17 der AGB).

(2) Wird der Hauptvertrag nach § 19 der AGB auf einen Übernehmer übertragen, geht dieser Vertrag mit ihm über. Der Übernehmer führt die technischen und organisatorischen Maßnahmen mindestens gleichwertig fort; für einen Wechsel von Unterauftragnehmern gilt § 6.

(3) Änderungen bedürfen der Textform.

(4) Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

(5) Es gilt das Recht der Bundesrepublik Deutschland.

<Ort>, den <Datum>

Verantwortlicher	Auftragsverarbeiter

Anlage 1 — Gegenstand der Verarbeitung

Zweck: Planung, Beantragung, Genehmigung und Dokumentation von Abwesenheiten von Beschäftigten.

Art der Verarbeitung: Erheben, Speichern, Ordnen, Auslesen, Verwenden, Offenlegen durch Übermittlung (E-Mail-Benachrichtigungen), Löschen.

Kategorien betroffener Personen: Beschäftigte des Verantwortlichen, einschließlich Auszubildender, Aushilfen und Werkstudenten.

Kategorien personenbezogener Daten:

Gruppe	Daten
Person	Name, Anzeigename, dienstliche E-Mail-Adresse, Personalnummer, Sprache, Profilbild (freiwillig)
Organisation	Abteilung oder Team, Region des Arbeitsorts (Bundesland oder Kanton), Rolle in der Software
Arbeitsverhältnis	Eintritts- und Austrittsdatum, Status, Arbeitszeitmuster, Wochenstunden, Bemerkung zum Arbeitszeitmodell
Ansprüche	Urlaubsanspruch, Übertrag, Sonderurlaub, Zusatztage (etwa Zusatzurlaub nach § 208 SGB IX), Korrekturen mit Begründung, Datum des Hinweises auf drohenden Verfall
Abwesenheiten	Art, Zeitraum, halbe Tage, Anzahl der Arbeitstage, Status, Genehmigungen und Vertretungen, Entscheidung mit Kommentar, freiwilliger Grund als Freitext
Sonderurlaub	Anlass (etwa Hochzeit, Geburt, Todesfall, Pflege, Wiedereingliederung) und Beschreibung
Nachweise	hochgeladene Dateien zu einer Abwesenheit, insbesondere Arbeitsunfähigkeitsbescheinigungen (PDF oder Bild)
Eingliederungsmanagement	Vorgänge nach § 167 Abs. 2 SGB IX mit Datum, Status und Notiz; Summe der Arbeitsunfähigkeitstage je Person
Benachrichtigungen	Empfänger, Anlass und Inhalt der E-Mails, etwa zu Antrag, Entscheidung, Resttagen und Verfall
Zugang	Einladungen, Beitrittsanfragen, Entscheidungslinks, Kalenderabonnement (Schlüssel nur als Prüfwert, Zeitpunkt des letzten Abrufs)
Anmeldung	IP-Adresse, Browserkennung und Verbindungsmerkmale beim Aufruf der Anmeldeseite (§ 3 Abs. 2)
Protokoll	Zeitpunkt, handelnde Person, geänderter Wert vorher und nachher

Besondere Kategorien nach Art. 9 DSGVO: Gesundheitsdaten sind die Tatsache und der Zeitraum einer krankheitsbedingten Abwesenheit, hochgeladene Arbeitsunfähigkeitsbescheinigungen und die Vorgänge des betrieblichen Eingliederungsmanagements. Auch ein Zusatzurlaub wegen Schwerbehinderung lässt einen Rückschluss auf die Gesundheit zu. **Die Software fragt keine Diagnosen, Krankheitsursachen oder Angaben zur Behandlung ab.** Freitextfelder — der Grund einer Abwesenheit, die Beschreibung beim Sonderurlaub, die Notiz zu einem Eingliederungsvorgang — und hochgeladene Dateien können solche Angaben aber enthalten, wenn Nutzer sie eintragen.

Hochgeladene Nachweise sehen nur die betroffene Person und die Personalverwaltung, die Vorgänge des Eingliederungsmanagements nur die Personalverwaltung.

Der Grund einer Abwesenheit wird nur denjenigen angezeigt, die nach der Konfiguration des Verantwortlichen dazu berechtigt sind; allen übrigen wird ausschließlich „abwesend" angezeigt, ohne dass der Grund an deren Browser übertragen wird.

Anlage 2 — Technische und organisatorische Maßnahmen

Die Maßnahmen nach Art. 32 DSGVO sind im Dokument **„Technische und organisatorische Maßnahmen"** beschrieben. Es ist Bestandteil dieses Vertrages und wird mit ihm übergeben.

Abrufbar unter **tiveo.de/sicherheit/**, als PDF unter **tiveo.de/dokumente/technische-und-organisatorische-massnahmen.pdf**.

Anlage 3 — Unterauftragnehmer

Unternehmen	Leistung	Ort
netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe	Bereitstellung des Servers, auf dem Datenbank, Dateispeicher und Anwendungsdienste laufen	Rechenzentrum Nürnberg, Deutschland
Serverprofis GmbH, Otto-Lilienthal-Ring 34–36, 85622 Feldkirchen	Auslieferung der Programmdateien der Software (app.tiveo.de); Postfach und Versand der E-Mail-Benachrichtigungen per SMTP	Rechenzentrum München, Deutschland
Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA	Schutz der Anmeldeseite vor automatisierten Zugriffen (Cloudflare Turnstile)	USA

> **Zu Cloudflare:** Cloudflare erhält beim Aufruf der Anmeldeseite die IP-Adresse, die Browserkennung und Merkmale der verschlüsselten Verbindung (§ 3 Abs. 2). **E-Mail-Adresse, Passwort und Inhalte der Software erreichen Cloudflare nicht.** Grundlage der Übermittlung in die USA ist die Zertifizierung der Cloudflare, Inc. unter dem EU-US Data Privacy Framework. Nach eigenen Angaben verwendet Cloudflare diese Merkmale außerdem in eigener Verantwortung, um die Erkennung automatisierter Zugriffe zu verbessern.
>
> **Zu Stripe:** Der Zahlungsdienstleister Stripe ist kein Unterauftragnehmer im Sinne dieses Vertrags. Er erhält ausschließlich Vertrags- und Rechnungsdaten des Verantwortlichen, für die der Auftragsverarbeiter selbst verantwortlich ist. **Beschäftigtendaten erreichen Stripe nicht.**

Die jeweils aktuelle Liste ist unter **tiveo.de/sicherheit/** abrufbar.

Anlage 4 — Löschkonzept

Die Löschfristen und das Verfahren sind im Dokument **„Löschkonzept"** beschrieben. Es ist Bestandteil dieses Vertrages und wird mit ihm übergeben.

Abrufbar unter **tiveo.de/sicherheit/**, als PDF unter **tiveo.de/dokumente/loeschkonzept.pdf**.