Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO · Fassung 2026-11-05

> **⚠ 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** bereit und verarbeitet dabei personenbezogene Daten in dessen Auftrag. Tiveo dient der Planung, Beantragung, Genehmigung und Dokumentation von Abwesenheiten und, soweit der Verantwortliche die jeweiligen Module einschaltet, der Erfassung von Arbeitszeiten, der Schichtplanung, der Verwaltung von Qualifikationen und Unterweisungen und der Führung eines Fahrtenbuchs. Dazu kommen Aushänge an der Pinnwand, Dokumente des Betriebs und Benachrichtigungen per E-Mail und Push. Schaltet der Verantwortliche den Geburtstagskalender ein, zeigt der Teamkalender auch Geburtstage.

(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 Auftragsver-

arbeiter 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, Unterstützung und Abrechnung bildet. Das sind Anzahlen, etwa der Plätze, der Beschäftigten mit und ohne Konto, der offenen Einladungen, der in den letzten 7 und 30 Tagen aktiven Konten, der Anträge, Entscheidungen, Zeitbuchungen, Schichten und Fahrten der letzten 30 Tage, der Personen mit Fahrten in diesem Zeitraum, der Fahrzeuge und der fehlgeschlagenen E-Mails, dazu der Zeitpunkt der letzten Aktivität. Kilometer, Orte und Strecken gehören nicht dazu. Namentlich erscheinen darin nur Eigentümer und Administratoren mit ihrem Zeitpunkt der letzten Aktivität. Für diese Kennzahlen 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, den Schutz der Anmeldung vor automatisierten Zugriffen, die Auslieferung der Karte im Fahrtenbuch, die Auslieferung der Software und den Versand von E-Mails (Anlage 3). Ausgenommen ist die zweite Kopie der Sicherung: Sie liegt in der Bundesrepublik Deutschland auf einem Speichergerät in den Räumen des Auftragsverarbeiters, auf einer verschlüsselten Freigabe (Anlage 2, Abschnitte 1.1 und 3.1). Trägt der Verantwortliche einen eigenen Mailserver ein, gehen seine Mitteilungen an die Beschäftigten über diesen Server.

(2) **Eine Ausnahme bilden Push-Benachrichtigungen.** Schaltet ein Nutzer sie auf einem Gerät ein, stellt der Auftragsverarbeiter sie über den Push-Dienst zu, den der Browser dieses Geräts vorgibt: bei Chrome, Edge und Android über Google Firebase Cloud Messaging, bei Firefox über den Dienst der Mozilla Corporation, bei Safari und auf Apple-Geräten über den Dienst der Apple Inc. Diese Dienste können Daten außerhalb der Europäischen Union verarbeiten, insbesondere in den USA. Sie erhalten die Adresse des Geräts beim Push-Dienst und eine Ende-zu-Ende verschlüsselte Nachricht (RFC 8291), die nur den Anlass nennt, etwa „Neuer Antrag zur Freigabe", und keine Namen, Daten oder Inhalte der Software enthält. Schaltet kein Nutzer Push-Benachrichtigungen ein, findet diese Übermittlung nicht statt.

(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.

(3) Unterliegt der Verantwortliche einer Schweigepflicht nach § 203 StGB, etwa als Arztpraxis, Therapiepraxis oder Pflegedienst, ist der Auftragsverarbeiter sonstige mitwirkende Person im Sinne von § 203 Abs. 3 Satz 2 StGB. Er verpflichtet sich, fremde Geheimnisse, die ihm bei der Verarbeitung bekannt werden, geheim zu halten und sich nur insoweit Kenntnis davon zu verschaffen, als das für die Erfüllung dieses Vertrags erforderlich ist. Er sorgt dafür, dass die bei ihm tätigen Personen und seine Unterauftragnehmer ebenso verpflichtet sind, soweit sie Zugang zu solchen Geheimnissen erhalten können. Ihm ist bekannt, dass die unbefugte Offenbarung nach § 203 Abs. 4 StGB strafbar ist.

---

§ 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 Support- und Einrichtungszwecken

(1) Ein Zugriff auf personenbezogene Daten des Verantwortlichen über die Software erfolgt, vorbehaltlich Absatz 4, 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.

(4) Zur Einrichtung der Software und zur Unterstützung des Verantwortlichen bei ihrer Nutzung kann der Auftragsverarbeiter ohne Freigabe nach Absatz 1 einen Einrichtungszugang öffnen. Mit ihm handelt er in der Software mit den Rechten eines Administrators und kann sie aus der Sicht einzelner Nutzer lesend ansehen. Der Einrichtungszugang

a) wird nur aus Anlass geöffnet, etwa auf Bitte des Verantwortlichen um Einrichtung oder Hilfe; der Anlass wird festgehalten, b) endet spätestens nach sieben Tagen von selbst, c) wird dem Verantwortlichen in der Software angezeigt und kann von dessen Eigentümer und Administratoren jederzeit beendet werden, d) belegt keinen Platz, entscheidet keine Anträge, empfängt keine Benachrichtigungen und nimmt keine Verträge für den Verantwortlichen an.

Öffnen, Beenden und Ablauf stehen im Protokoll nach Absatz 2. Änderungen, die der Auftragsverarbeiter dabei vornimmt, hält das Protokoll der Software mit ihm als Handelndem fest. Der Auftragsverarbeiter handelt dabei nach den Weisungen des Verantwortlichen (§ 2).

> Dieser Paragraph beschreibt keine Absichtserklärung, sondern eine technische Eigenschaft: **Über die Anwendung** ist ein Zugriff auf personenbezogene Daten ohne Freigabe des Verantwortlichen nur über den Einrichtungszugang nach Absatz 4 möglich — und den sehen Sie, er endet von selbst, und Sie können ihn jederzeit beenden. Die Freigabe nach Absatz 1 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, jede tatsächliche Einsicht und jeder Einrichtungszugang — 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 Be-

reitstellung (§ 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. Soweit der Verantwortliche die Module einschaltet, außerdem:

- **Zeiterfassung:** Erfassung von Arbeitszeiten und Pausen, Führen von Arbeitszeitkonten, Projektzeiten, Monatsabschluss, Monatsbestätigung und Export für die Lohnabrechnung,
- **Schichtplanung:** Planung und Veröffentlichung von Schichten und Diensten, Wünsche, Tausch und Meldung geleisteter Dienste,
- **Qualifikationen und Unterweisungen:** Nachweis von Qualifikationen, Unterweisungen, Fortbildungen, Belehrungen und Vorsorgeterminen mit ihrer Gültigkeit,
- **Fahrtenbuch:** Führung eines Fahrtenbuchs für Fahrzeuge des Verantwortlichen und für Privatfahrzeuge von Beschäftigten, die betrieblich genutzt werden, als Nachweis gegenüber der Finanzverwaltung; Zuordnung von Fahrzeugen zu Personen und Schichten; Erfassung von Fahrzeugkosten mit Belegen; Berechnung und Freigabe von Kilometergeld und Export für die Lohnabrechnung; auf Wunsch des Verantwortlichen die Aufzeichnung der Strecke betrieblicher Fahrten.

Für alle Unternehmen gehören dazu Aushänge an der Pinnwand, Dokumente des Betriebs wie Arbeitsanweisungen und Benachrichtigungen per E-Mail und, auf Wunsch der einzelnen Nutzer, per Push. Soweit der Verantwortliche den Geburtstagskalender einschaltet, außerdem die Anzeige von Geburtstagen im Teamkalender.

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

Kategorien betroffener Personen: Beschäftigte des Verantwortlichen, einschließlich Auszubildender, Aushilfen und Werkstudenten. Soweit der Verantwortliche das Fahrtenbuch nutzt, außerdem Kunden, Patienten, Klienten und andere Geschäftspartner des Verantwortlichen, die als Ziel oder aufgesuchter Partner einer Fahrt eingetragen werden, und deren Ansprechpersonen.

Kategorien personenbezogener Daten:

Gruppe	Daten
Person	Name, Anzeigename, dienstliche E-Mail-Adresse, Personalnummer, Sprache der E-Mails und der Oberfläche, Profilbild (freiwillig)
Organisation	Abteilung oder Team, weitere Abteilungen, Leitung von Abteilungen, Recht zur Schichtplanung, Region des Arbeitsorts (Bundesland oder Kanton), Rolle in der Software
Einstellungen	Benachrichtigungen, die die Person für sich ein- oder ausschaltet; gespeicherte Ansichten
Arbeitsverhältnis	Eintritts- und Austrittsdatum, Status, Arbeitszeitmuster, Wochenstunden, Bemerkung zum Arbeitszeitmodell
Geburtstag	nur wenn der Verantwortliche den Geburtstagskalender einschaltet: Geburtsdatum und je Person, was der Teamkalender zeigt (nichts, nur den Tag oder den Tag mit dem neuen Alter; Vorgabe nichts). Die Person kann das selbst ändern
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, Entscheidung mit Kommentar und der Person, die entschieden hat, freiwilliger Grund als Freitext, freiwilliger kurzer Hinweis für den Teamkalender
Vertretungen	wer wen bei Freigaben in welchem Zeitraum vertritt
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
Arbeitszeiten	Kommen, Gehen, Beginn und Ende von Pausen mit Zeitpunkt und Arbeitstag; Quelle der Buchung (Stempeln, Nachtrag, Korrektur, Terminal, Import, automatische Buchung); auf Wunsch der vom Nutzer gewählte Arbeitsort „Im Betrieb" oder „Mobil"; Grund einer Korrektur; wer erfasst hat
Anerkannte Zeit	Zeit außerhalb von Schicht oder Zeitrahmen: Person, Arbeitstag, Minuten, Begründung, Antrag oder Anerkennung durch die Leitung, Entscheidung mit Person, Zeitpunkt und Antwort
Stempeln am PC	soweit der Verantwortliche es einschaltet: Zeitpunkt des letzten Lebenszeichens des Rechners je Person, gelöscht beim Gehen
Arbeitsorte	Orte, an denen der Verantwortliche das Einstempeln zulässt: Name, Koordinaten und Umkreis, ohne Bezug zu einzelnen Personen
Arbeitszeitkonto	Sollzeit aus dem Arbeitszeitmodell, Anfangssaldo, Korrekturen und Auszahlungen mit Grund
Projektzeiten	Projekte mit Nummer, Titel, Link und Ansprechperson; Zeiten je Person, Tag und Projekt mit Notiz; auf Wunsch das beim Stempeln gewählte Projekt mit Zeitpunkt

Gruppe	Daten
Stempeln am Terminal	Terminals mit Name und Abteilung, Stempelnummer, PIN nur als Hashwert, Ausweiscode nur als Prüfwert, Fehlversuche
Monatsabschluss	Monatssummen je Person (Arbeit, Soll, Saldo, Nacht-, Sonntags- und Feiertagsstunden, offene Tage) mit Name und Personalnummer zum Zeitpunkt des Abschlusses; Abschlüsse und Wiederöffnungen mit Grund
Monatsbestätigung	Bestätigung der Monatswerte durch die Person mit Zeitpunkt und Prüfsumme, Gegenzeichnung mit Name und Zeitpunkt
Schutzmerkmale	Jugendliche, Mutterschutz, Schwerbehinderung (keine Mehrarbeit auf Verlangen), eingeschränkte Nachtarbeit, jeweils mit Zeitraum und kurzer Notiz
Schichtplanung	Schichten mit Datum, Zeiten, Schichtart, Abteilung, Status und Notiz; Wünsche, Eintragungen, Angebote und Tausch mit Entscheidung; Schichtmuster und ihre Zuordnung; Wochenvorlagen mit den eingeplanten Personen; veröffentlichte Zeiträume; gemeldete Dienste je Woche
Checklisten zu Schichten	Vorlagen und Punkte; je Schicht erledigte Punkte und Kommentare mit Person und Zeitpunkt; bis zu drei Fotos je Punkt
Qualifikationen	Art und Kategorie, Erwerbsdatum, Gültigkeit, Punkte, kurze Bemerkung; Unterweisungen mit Datum, Thema, Durchführendem und Teilnahme; hochgeladene Nachweise (PDF oder Bild)
Fahrzeuge	Kennzeichen, Bezeichnung, Art (Firmenfahrzeug oder Privatfahrzeug einer beschäftigten Person), Nutzung (Pool oder zugeordnet), erlaubte Privatnutzung, Antrieb, Bruttolistenpreis, Erstzulassung, Kilometerstand zu Beginn, Termine von Hauptuntersuchung und Unfallverhütungsprüfung, zugeordnete Einheit, Notiz; bei Privatfahrzeugen die haltende beschäftigte Person
Fahrzeugzuordnungen	wer ein Fahrzeug als Dienstwagen nutzt oder fahren darf (Person oder Einheit), mit Zeitraum; Entfernung zwischen Wohnung und erster Tätigkeitsstätte, soweit für die Bewertung des Arbeitswegs eingetragen; Fahrzeug je Schicht
Fahrten	Fahrzeug, fahrende Person, Art (betrieblich, privat, Arbeitsweg), Beginn und Ende, Kilometerstand zu Beginn und Ende oder gefahrene Kilometer, Grund einer Lücke im Kilometerstand; bei betrieblichen Fahrten Start und Ziel, Zweck, aufgesuchter Geschäftspartner, Umweg und Projekt; Herkunft der Eintragung, wer wann erfasst, ergänzt, berichtigt oder aufgehoben hat und warum; Abschluss der Fahrt. Bei Privatfahrt und Arbeitsweg nur Datum, Kilometer und Art
Strecke	nur wenn der Verantwortliche die Aufzeichnung einschaltet und nur bei betrieblichen Fahrten: Standortpunkte (geografische Breite und Länge) mit Zeitabstand und Genauigkeit, Länge und Lücken der Aufzeichnung. Keine Live-Anzeige für andere Nutzer. Löschung nach der eingestellten Frist (Vorgabe drei Monate) und, wenn eine Fahrt privat oder Arbeitsweg wird
Orte und Geschäftspartner	Adressbuch des Verantwortlichen: Name, Kürzel, Anschrift, Koordinaten und Umkreis für den Vorschlag in der Nähe, zugeordnetes Projekt; auf Wunsch Partner mit Nummer, die im Fahrtenbuch nur als Nummer erscheinen

Gruppe	Daten
Fahrzeugkosten	Datum, Art (etwa Kraftstoff, Laden, Werkstatt, Versicherung), Betrag brutto und netto, Menge, Kilometerstand, Notiz, hochgeladener Beleg (Foto oder PDF), wer erfasst hat
Kilometergeld	je Person und Monat die mit dem Privatfahrzeug gefahrenen Kilometer, Satz, Betrag, zugehörige Fahrten, Freigabe mit Person und Zeitpunkt, Fassungen
Führerscheinkontrolle	Datum und Gültigkeit der Kontrolle als Qualifikation (siehe „Qualifikationen"). Die Software verlangt kein Abbild des Führerscheins
Karte	beim Laden eines Kartenausschnitts IP-Adresse und angefragter Ausschnitt, nur für die Auslieferung, ohne Protokoll. Die Karte läuft auf dem Server nach Anlage 3, ohne Übermittlung an Dritte
Zwischenspeicher im Browser	noch nicht gesendete Fahrten und Standortpunkte auf dem Gerät des Nutzers, bis sie gesendet sind, höchstens 30 Tage
Pinnwand	Aushänge mit Titel, Text, Zielabteilungen, Zeitraum und Verfasser; Lesebestätigungen mit Zeitpunkt
Dokumente	Dokumente des Betriebs mit Titel, Beschreibung, Gruppe, Text oder hochgeladener PDF-Datei und Zielabteilungen; Name der Person, die zuletzt geändert hat, und Zeitpunkte
Benachrichtigungen	Empfänger, Anlass und Inhalt der E-Mails, etwa zu Antrag, Entscheidung, Resttagen, Verfall, Zeiten, Schichten, Qualifikationen, Fahrten und Aushängen; bei einem eigenen Mailserver des Verantwortlichen dessen Anschrift und Zugangsdaten, das Passwort verschlüsselt
Push	je Gerät die Adresse beim Push-Dienst, die Schlüssel zur Verschlüsselung und eine gekürzte Browserkennung
Zugang	Einladungen, Beitrittsanfragen mit dem angegebenen Namen, Entscheidungslinks, Kalenderabonnement (Schlüssel nur als Prüfwert, Zeitpunkt des letzten Abrufs)
Anmeldung	IP-Adresse (nur zur Begrenzung der Anfragen, wenige Sekunden gespeichert) und technische Merkmale des Browsers (nur für die Prüfung, nicht gespeichert) bei der Sicherheitsprüfung von Anmeldung, Registrierung und Anmeldelink; abgelehnte Versuche mit gekürzter IP-Adresse. Die Prüfung läuft auf dem Server nach Anlage 3, ohne Übermittlung an Dritte
Schnittstellen	soweit der Verantwortliche sie einrichtet: bei Personio Kopien von Stammdaten, Abwesenheiten und Zeiten, Zuordnungen und das Protokoll der Anbindung; bei DATEV Berater- und Mandantennummer, Zuordnung der Lohnarten, Ausnahmen je Person und die erzeugten Dateien; bei der Programmierschnittstelle Name, Rechte und Prüfwert der Schlüssel und das Aufrufprotokoll mit der IP-Adresse des aufrufenden Systems
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, ebenso die Schutzmerkmale Mutterschutz, Schwerbehinderung und eingeschränkte Nachtar-

beit. Bei den Qualifikationen können Termine der arbeitsmedizinischen Vorsorge und hochgeladene Bescheinigungen, etwa über eine Eignung, auf die Gesundheit schließen lassen. **Die Software fragt keine Diagnosen, Krankheitsursachen, Befunde oder Angaben zur Behandlung ab.** Zu einer Vorsorge speichert sie nur das Datum; eine Datei lässt sich dort nicht hochladen. Freitextfelder — der Grund einer Abwesenheit, die Beschreibung beim Sonderurlaub, die Notiz zu einem Eingliederungsvorgang oder einem Schutzmerkmal, die Bemerkung zu einer Qualifikation — und hochgeladene Dateien können solche Angaben aber enthalten, wenn Nutzer sie eintragen.

Im Fahrtenbuch können Ziel, Zweck und aufgesuchter Partner einer Fahrt auf die Gesundheit Dritter schließen lassen, etwa der Hausbesuch bei einem Patienten oder Klienten. Für solche Partner kann der Verantwortliche einstellen, dass sie im Fahrtenbuch, in Exporten des Fahrtenbuchs und über die Programmierschnittstelle nur mit einer Nummer erscheinen; Name und Anschrift stehen dann nur im Adressbuch. Die Software fragt keine Diagnosen oder Behandlungen ab; das Freitextfeld „Zweck" kann solche Angaben aber enthalten, wenn Nutzer sie eintragen.

Hochgeladene Nachweise zu Abwesenheiten und Qualifikationen sehen nur die betroffene Person und die Personalverwaltung, Führungskräfte also nicht. Die Vorgänge des Eingliederungsmanagements sieht nur die Personalverwaltung, die Schutzmerkmale nur die Personalverwaltung und die betroffene Person. Wer einen Aushang gelesen hat, sehen nur dessen Verfasser und die Personalverwaltung. Das Geburtsdatum selbst sehen nur die Person, ihre Führungskraft und Nutzer mit den Rollen Eigentümer, Administrator und Personalverwaltung; im Teamkalender stehen nur der Tag und, wenn gewählt, das neue Alter.

Die Software speichert **keine biometrischen Merkmale**. Am Terminal meldet sich die Person mit Stempelnummer und PIN oder mit einem Ausweiscode an.

Standortdaten speichert die Software nur im Fahrtenbuch, und dort nur die Strecke betrieblicher Fahrten, wenn der Verantwortliche die Aufzeichnung eingeschaltet hat (Zeile „Strecke"). Die Zeiterfassung speichert keinen Standort; die Prüfung beim Einstempeln am Arbeitsort vergleicht ihn nur.

Die Strecke einer Fahrt sehen nur die fahrende Person und Nutzer mit den Rollen Eigentümer, Administrator und Personalverwaltung ohne Begrenzung auf einen Bereich; Führungskräfte sehen sie nicht, auch nicht über die Ansicht als andere Person. Die Programmierschnittstelle gibt sie nicht heraus. Der Gesamtexport des Eigentümers enthält sie, solange sie nicht gelöscht ist.

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, Anwendungsdienste, der Schutz der Anmeldung vor automatisierten Zugriffen (Cap) und der Kartenserver des Fahrtenbuchs 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

Zum Schutz der Anmeldung: Die Sicherheitsprüfung vor Anmeldung, Registrierung und Anmeldelink betreibt der Auftragsverarbeiter selbst, mit der quelloffenen Software Cap auf dem Server bei der netcup GmbH. Ein weiterer Dienstleister ist nicht beteiligt.

Zur Karte im Fahrtenbuch: Die Karte betreibt der Auftragsverarbeiter selbst, mit Kartendaten von OpenStreetMap, auf dem Server bei der netcup GmbH. Ein Karten- oder Adressdienst Dritter ist nicht beteiligt; Abrufe werden nicht protokolliert. Den Standort ermittelt das Gerät des Nutzers selbst. Je nach Geräteeinstellung bezieht dessen Betriebssystem dafür Ortungsdienste seines Herstellers ein, etwa von Google oder Apple. Diese handeln nicht im Auftrag des Auftragsverarbeiters und erhalten von ihm keine Daten.

Zur zweiten Kopie der Sicherung: Das Speichergerät nach § 3 Abs. 1 betreibt der Auftragsverarbeiter selbst in seinen Räumen. Ein weiterer Dienstleister ist nicht beteiligt.

Zum eigenen Mailserver: Trägt der Verantwortliche einen eigenen Mailserver ein, bestimmt er selbst, wer ihn betreibt. Dieser Betreiber ist nicht Unterauftragnehmer des Auftragsverarbeiters.

Zu den Push-Diensten: Google (Firebase Cloud Messaging), Mozilla und Apple stellen Push-Benachrichtigungen zu, wenn ein Nutzer sie auf einem Gerät eingeschaltet hat (§ 3 Abs. 2). Welcher Dienst das ist, bestimmt der Browser des Nutzers, nicht der Auftragsverarbeiter. Der Dienst erhält nur die Adresse des Geräts bei ihm und die verschlüsselte Nachricht, die er nicht lesen kann. **Namen, Daten und Inhalte der Software erreichen ihn nicht.**

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**.
