Technische und organisatorische Maßnahmen

Tiveo · Sven Brunn Mediasolutions Stephanusstraße 29, 41472 Neuss

Anlage zum Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 lit. c und Art. 32 DSGVO.

Stand: 31.10.2026 · Version 9

> Dieses Dokument beschreibt den tatsächlichen Stand. Jede Zusage darin ist im Produkt umgesetzt und überprüfbar. Wo etwas noch fehlt, sagt der jeweilige Abschnitt das ausdrücklich; gesammelt stehen die offenen Punkte am Ende unter „In Vorbereitung".

---

1. Vertraulichkeit

1.1 Zutrittskontrolle

Datenbank, Dateispeicher, Anwendung, Schutz der Anmeldung, Karte des Fahrtenbuchs und E-Mail-Versand liegen in Rechenzentren in der Bundesrepublik Deutschland. Ausnahme ist die Zustellung von Push-Benachrichtigungen (siehe 2.1).

	Server der Anwendung	**Auslieferung der Anwendung und E-Mail**
Betreiber	netcup GmbH, Karlsruhe	Serverprofis GmbH, Feldkirchen
Standort	Rechenzentrum Nürnberg	Rechenzentrum München
Leistung	Server mit Datenbank, Dateispeicher, Anwendungsdiensten, Schutz der Anmeldung (Cap) und Kartenserver des Fahrtenbuchs	Programmdateien der Anwendung, Postfach und SMTP-Versand
Zertifizierung	ISO/IEC 27001, geprüft durch TÜV Nord, Geltungsbereich unter anderem vServer (Angabe des Anbieters)	vom Anbieter nicht angegeben
Zutritt	Zutrittskontrolle durch den Betreiber des Rechenzentrums	Zutrittskontrolle durch den Betreiber des Rechenzentrums

Der Auftragsverarbeiter selbst unterhält keine Serverräume. Ein Zutritt zu den Systemen ist ihm physisch nicht möglich. Ausnahme ist die zweite Kopie der Sicherung (3.1): Sie liegt auf einem Speichergerät in den Räumen des Auftragsverarbeiters in der Bundesrepublik Deutschland, auf einer verschlüsselten Freigabe; Zutritt dazu hat nur der Auftragsverarbeiter.

1.2 Zugangskontrolle

- Zugriff auf die Server ausschließlich über SSH mit Schlüsselpaar. **Passwortanmeldung ist abgeschaltet.**

- Die Programmdateien der Anwendung werden per FTP mit TLS-Verschlüsselung auf den Webspace übertragen.
- Die Verwaltungsoberflächen sind aus dem Internet erreichbar, aber nur mit Zugangsdaten nutzbar: Supabase Studio hinter einer HTTP-Basic-Anmeldung, die Serververwaltung Coolify mit eigener Anmeldung.
- Der Datenbankport ist nur lokal auf dem Server erreichbar. Zugriffe von außen laufen über einen SSH-Tunnel.
- Anmeldung der Anwender über E-Mail und Passwort oder Einmal-Anmeldelink. Passwörter werden ausschließlich als Hash gespeichert (bcrypt, durch GoTrue).
- Vor Anmeldung, Registrierung und Anmeldelink prüft die quelloffene Software Cap auf dem eigenen Server, ob ein Mensch die Seite bedient: Der Browser löst eine Rechenaufgabe, und eine Prüfung der Browserumgebung erkennt automatisierte Zugriffe. Heraus kommt ein Prüfzeichen, das einmal gilt und nach höchstens zwei Stunden verfällt. Ein Prüftor vor dem Anmeldedienst prüft es bei Cap und lässt Anfragen ohne gültiges Prüfzeichen nicht durch (siehe 2.1).
- Sitzungen laufen ab und werden über kurzlebige Token erneuert.
- Am Terminal der Zeiterfassung meldet sich eine Person mit Stempelnummer und PIN oder mit einem Ausweiscode an. Die PIN wird nur als Hash gespeichert (bcrypt), Ausweiscode, Gerätekennung und Einrichtungscode des Terminals nur als Prüfwert (SHA-256). Nach mehreren Fehlversuchen wird der Zugang vorübergehend gesperrt. Das Terminal zeigt nur Vorname und Stempelstand, keine Abwesenheiten oder anderen Personen. Stundenkonto und Urlaubsrest der angemeldeten Person zeigt es nur, wenn der Betrieb das einschaltet; von Haus aus ist das aus.
- Ohne Netz merkt sich das Terminal Buchungen auf dem Gerät, bis es sie nachsenden kann. Stempelnummer und PIN oder Ausweiscode liegen darin verschlüsselt für einen Schlüssel des Servers (ECDH P-256, AES-256-GCM): Öffnen kann sie nur der Server, nicht wer Zugriff auf den Speicher des Geräts hat. Nach dem Nachsenden ist die Warteschlange leer.

1.3 Zugriffskontrolle

Dies ist die zentrale Maßnahme, weil Tiveo mehrere Unternehmen auf derselben Datenbank verarbeitet.

- **Row Level Security auf jeder Tabelle ohne Ausnahme.** Ein Zugriff außerhalb des eigenen Unternehmens liefert keine Daten — nicht gefiltert durch die Anwendung, sondern durch die Datenbank selbst.
- **Rechteentzug als Ausgangszustand.** Für jede Tabelle werden zunächst alle Rechte entzogen (`REVOKE ALL … FROM PUBLIC, anon, authenticated`) und anschließend gezielt einzelne Spalten freigegeben. Eine neu hinzugefügte Spalte ist damit automatisch gesperrt, bis sie ausdrücklich freigegeben wird.
- **Besonders geschützte Felder** — Rolle, Status, Unternehmenszugehörigkeit, Abrechnungsdaten — sind für Anwender grundsätzlich nicht schreibbar. Sie lassen sich ausschließlich über geprüfte Datenbankfunktionen ändern.
- **Maskierung von Abwesenheitsgründen.** Ob ein Betrachter den Grund einer fremden Abwesenheit sieht, entscheidet die Datenbank. Bei fehlender Berechtigung wird der Grund nicht etwa ausgeblendet, sondern **gar nicht erst übertragen**.
- **Nachweise im geschützten Dateispeicher.** Hochgeladene Nachweise zu Abwesenheiten und Qualifikationen liegen in nicht öffentlichen Bereichen des Dateispeichers. Lesen dürfen sie nur die betroffene Person und die Personalverwaltung, Führungskräfte nicht. Zu Qualifikationen sind nur PDF, JPEG und PNG bis 10 MB zulässig, zu einer arbeitsmedizinischen Vorsorge gar keine Datei.

- **Strecken im Fahrtenbuch.** Die Standortpunkte einer Fahrt liegen in einer eigenen Tabelle ohne Leserechte für Anwender. Gelesen werden sie nur über eine geprüfte Datenbankfunktion, die ausschließlich der fahrenden Person, Eigentümern, Administratoren und der unternehmensweiten Personalverwaltung antwortet; Führungskräfte, die Ansicht als andere Person und die Programmierschnittstelle erhalten sie nicht. Angefügt werden Punkte nur von der fahrenden Person, nur bei betrieblichen Fahrten, nur bei eingeschalteter Aufzeichnung und nur bis einen Tag nach dem Abschluss der Fahrt. Belege zu Fahrzeugkosten liegen in einem nicht öffentlichen Bereich des Dateispeichers (JPEG und PDF bis 5 MB); Fotos werden vor dem Hochladen im Browser neu gezeichnet und tragen danach keine Metadaten wie den Aufnahmeort.
- **Automatisierte Prüfung.** Eine Testsuite legt zwei Unternehmen an und prüft, dass keines die Daten des anderen lesen oder ändern kann. Sie läuft auf einer Wegwerf-Datenbank und wird vor dem Einspielen von Datenbankänderungen von Hand angestoßen. Eine automatische Sperre, die eine Auslieferung bei einem Fehlschlag verhindert, gibt es noch nicht (siehe 5.).

1.4 Trennungskontrolle

- Mandantentrennung logisch über die Unternehmenskennung, durchgesetzt durch Row Level Security (1.3).
- Getrennte Instanzen für Entwicklung und Betrieb. **In der Entwicklungsumgebung werden keine Echtdaten verwendet.**
- Die Instanz wird ausschließlich für Tiveo betrieben und teilt sich keine Datenbank mit anderen Anwendungen. Auf demselben Server laufen weitere, vom Auftragsverarbeiter betriebene Anwendungen, jede in eigenen Containern mit eigener Datenbank.

---

2. Integrität

2.1 Weitergabekontrolle

- Übertragung ausschließlich über TLS (HTTPS, mindestens TLS 1.2), HSTS aktiviert.
- Content-Security-Policy schränkt ein, wohin der Browser Verbindungen aufbauen darf.
- **Keine Analysedienste, keine Werbenetzwerke, kein Massenversanddienst.** Empfänger außerhalb des eigenen Betriebs sind ausschließlich die Unterauftragnehmer nach Anlage 3 des Auftragsverarbeitungsvertrags.
- E-Mails verschickt die Anwendung über ein eigenes Postfach bei der Serverprofis GmbH (SMTP). Dort liegt auch das Postfach info@tiveo.de. Trägt der Verantwortliche einen eigenen Mailserver ein, gehen seine Mitteilungen an die Beschäftigten verschlüsselt über diesen Server; das Passwort dafür liegt verschlüsselt in der Datenbank und erreicht die Anwendung nicht.
- **Schutz der Anmeldung (Cap).** Beim Aufruf der Seite für Anmeldung, Registrierung und Anmeldelink lädt der Browser eine Prüfseite von cap.tiveo.de, die auf dem eigenen Server läuft (1.1). Verarbeitet werden die IP-Adresse, nur zur Begrenzung der Anfragen und wenige Sekunden gespeichert, und technische Merkmale des Browsers, nur für die Prüfung und nicht gespeichert. Cap führt nur Zählungen, keine Profile; abgelehnte Versuche werden mit gekürzter IP-Adresse protokolliert. Keine Cookies, keine Weitergabe an Dritte, keine Übermittlung in Drittländer.

- **Push-Benachrichtigungen.** Sie kommen nur auf Geräte, auf denen die Person sie selbst eingeschaltet hat. Die Nachricht wird Ende-zu-Ende verschlüsselt (RFC 8291) und nennt nur den Anlass, etwa „Neuer Antrag zur Freigabe", ohne Namen, Daten oder Inhalte. Zugestellt wird sie über den Push-Dienst, den der Browser vorgibt (Google, Mozilla oder Apple), auch außerhalb der EU. Der Dienst sieht nur die Geräteadresse und die verschlüsselte Nachricht. Meldet er ein Gerät als ungültig, löscht die Anwendung das Abo.
- **Karte im Fahrtenbuch.** Kartendaten, Schriften und Symbole lädt der Browser ausschließlich von karte.tiveo.de, das auf dem eigenen Server läuft (1.1). Der Kartenserver und der vorgeschaltete Proxy schreiben für diese Abrufe **kein Zugriffsprotokoll**; der Kartenserver selbst kennt die IP-Adresse der Nutzer nicht. Die Content-Security-Policy der Anwendung lässt keinen anderen Kartendienst zu. Ein Dienst, der Adressen in Koordinaten umrechnet, ist nicht eingebunden.
- Reichweitenmessung auf der Marketing-Website erfolgt cookiefrei über eine Matomo-Instanz, die der Auftragsverarbeiter selbst auf seinem Webspace bei der Serverprofis GmbH betreibt. **Die Anwendung selbst wird nicht gemessen.**

2.2 Eingabekontrolle

- Änderungen an Stammdaten, Urlaubsansprüchen, Abwesenheiten, Genehmigungsregeln und Rollen werden mit Zeitpunkt, handelnder Person und geändertem Wert protokolliert.
- Das Protokoll ist für Anwender **nur lesbar**. Geschrieben wird es ausschließlich durch die Datenbank selbst, über Trigger und geprüfte Datenbankfunktionen.
- Gebuchte Arbeitszeiten und Buchungen auf dem Arbeitszeitkonto lassen sich nicht ändern. Eine Korrektur ist ein neuer Eintrag, der auf den alten verweist, mit Grund und Urheber. Eine Monatsbestätigung trägt eine Prüfsumme über die bestätigten Monatswerte; gegenzeichnen lässt sie sich nur, solange die Werte dazu passen.
- Fahrten im Fahrtenbuch lassen sich nicht ändern. Jede Ergänzung, Berichtigung oder Aufhebung ist eine neue Fassung mit Urheber, Zeitpunkt und, nach dem Abschluss, Grund. Der Export für die Finanzverwaltung enthält den Änderungsverlauf und eine SHA-256-Prüfsumme. Ausgenommen sind die Standortpunkte der Strecke: Sie werden nach der eingestellten Frist gelöscht und gehören nicht zum Fahrtenbuch.
- Zugriffe des Auftragsverarbeiters auf Kundendaten über die Anwendung werden gesondert protokolliert und sind für den Kunden einsehbar. Für den administrativen Zugriff auf die Datenbank gilt die Einschränkung in § 10 Abs. 3 des Auftragsverarbeitungsvertrags.

---

3. Verfügbarkeit und Belastbarkeit

3.1 Sicherung

Die Datenbank wird laufend, nachts und täglich gesichert, an zwei Orten, und die Wiederherstellung wird wöchentlich geprüft. Im Einzelnen:

- **Laufend:** Jede Änderung der Datenbank wird in dem Moment mitgeschrieben, in dem sie passiert (Write-Ahead-Log, fortlaufend übertragen), und auf dem Server abgelegt. So lässt sich die Datenbank auf einen Zeitpunkt der letzten Tage zurückholen.

- **Nächtlich und täglich:** Jede Nacht entsteht eine vollständige Basissicherung als Ausgangspunkt für jedes Zurückholen, und täglich zusätzlich ein Auszug der Datenbank (`pg_dump`, Schemata `public`, `auth`, `supabase_migrations`).
- **Zweiter Ort:** Eine Kopie von alledem holt ein Speichergerät in den Räumen des Auftragsverarbeiters in der Bundesrepublik Deutschland laufend vom Server ab. Das Gerät holt nur lesend, über SSH mit eigenem Schlüssel; der Server hat keinen Zugang zu dem Gerät und kann diese Kopie weder ändern noch löschen. Die Freigabe, auf der die Kopie liegt, ist verschlüsselt. Dort bleiben mehrere Wochen vorrätig (derzeit 14 bis 21 Tage).
- **Wöchentlich geprüft:** Die Kopie am zweiten Ort wird in einer Umgebung ohne Netzverbindung probeweise zurückgespielt, die Datenbank wird gestartet und die wichtigsten Tabellen werden nachgezählt (Wiederherstellungstest). Die Ergebnisse stehen für jedes Unternehmen in der Anwendung unter „Systemstatus“.
- **Überwacht:** Ein Wächter prüft alle 30 Sekunden, wie weit die Sicherung reicht und ob sie lückenlos ist. Abweichungen lösen einen Alarm aus. Bleibt die Meldung des Wächters aus, zeigt der Systemstatus keinen Zustand mehr an, statt den letzten gültigen weiter zu zeigen.
- **Hochgeladene Dateien** (Nachweise, Belege, Fotos, Profilbilder, Logos) werden nachts auf dem Server gespiegelt und auf das Speichergerät am zweiten Ort übernommen. Ein Spiegel bildet den jeweils letzten Stand ab: Eine gelöschte Datei verschwindet beim nächsten Lauf, ältere Stände gibt es derzeit nicht.
- **Aufbewahrung:** Sicherungen der Datenbank werden **höchstens 90 Tage** nach ihrer Erstellung aufbewahrt und danach automatisch gelöscht, einschließlich aller Kopien. In der Praxis gilt eine strengere Frist: Das fortlaufend mitgeschriebene Protokoll und die Basissicherungen bleiben auf dem Server wenige Tage, am zweiten Ort bis zu drei Wochen; Auszüge werden 30 Tage täglich und danach wöchentlich aufbewahrt, spätestens nach 55 Tagen gelöscht. Muss eine Sicherung zurückgespielt werden, werden die darin enthaltenen Daten beendeter Verträge unverzüglich erneut gelöscht (§ 11 Abs. 5 der AGB).
- Die Sicherungsdateien auf dem Server liegen **unverschlüsselt** auf dem Server; der Zugang dazu ist wie in 1.2 beschränkt. Die Kopie am zweiten Ort liegt auf einer verschlüsselten Freigabe.

> Eine Sicherung, die nie zurückgespielt wurde, ist keine Sicherung. Der wöchentliche Wiederherstellungstest löst genau das automatisiert ein.

3.2 Wiederherstellbarkeit

- Wiederherstellungszeit (RTO): noch nicht festgelegt.
- Maximal tolerierter Datenverlust (RPO): noch nicht festgelegt. Die Sicherung ist darauf ausgelegt, dass im Ernstfall höchstens Sekunden (auf dem Server) bis etwa eine Minute (am zweiten Ort) fehlen. Das ist die Auslegung, keine Zusage (§ 11 Abs. 5 der AGB).
- Aufbau der Serverumgebung und Einspielen einer Datenbanksicherung sind in der Betriebsdokumentation beschrieben. Der Wiederherstellungstest prüft das Zurückspielen der Datenbank, nicht den Neuaufbau eines ganzen Servers; ein regelmäßig geprobtes Wiederanlaufverfahren dafür gibt es noch nicht.

3.3 Verfügbarkeit

- Störungen werden auf einer öffentlichen Statusseite gemeldet.

- Geplante Wartungsarbeiten werden **in der Regel mindestens 72 Stunden vorher** per E-Mail an Eigentümer und Administratoren angekündigt und nach Möglichkeit außerhalb der üblichen Arbeitszeit gelegt. Dringende Arbeiten, etwa zum Schließen einer Sicherheitslücke, werden auch kurzfristig durchgeführt (§ 11 Abs. 2 der AGB).
- Eine Verfügbarkeit in Prozent wird **nicht zugesichert**. Der Auftragsverarbeiter ist ein Einzelunternehmen ohne Bereitschaftsdienst; eine Zusage, die sich nachts nicht halten lässt, wäre irreführend.

3.4 Fortbestand

Für den Fall, dass der Auftragsverarbeiter den Betrieb des Dienstes einstellt:

- Er kündigt die Verträge mit den Fristen der AGB (§ 8 Abs. 7 und 9). Läuft ein kostenpflichtiger Tarif, sind das **drei Monate zum Monatsende**, sonst **ein Monat zum Monatsende**. Stirbt der Inhaber oder kann er Tiveo aus gesundheitlichen Gründen voraussichtlich länger als drei Monate nicht betreiben, ist es ein Monat zum Monatsende. Im Voraus gezahlte Entgelte werden anteilig erstattet. Maßgeblich ist der Wortlaut der AGB.
- Bis zum Vertragsende und im anschließenden Abrufzeitraum von 30 Tagen kann der Kunde seine Daten mit den Exportfunktionen herunterladen und einen Gesamtexport anfordern (§§ 13 und 14 der AGB, § 11 des Auftragsverarbeitungsvertrags).
- Anschließend nachweisliche Löschung nach § 14 der AGB; die Löschung wird auf Verlangen in Textform bestätigt.

---

4. Verfahren zur Überprüfung

4.1 Datenschutzmanagement

- Verzeichnis der Verarbeitungstätigkeiten liegt vor.
- Löschkonzept liegt vor, abrufbar unter **tiveo.de/sicherheit/**.
- Betroffenenanfragen werden binnen der Fristen des Art. 12 Abs. 3 DSGVO bearbeitet; der Auftragsverarbeiter unterstützt den Verantwortlichen dabei.

4.2 Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

Die Voreinstellungen sind bewusst zurückhaltend gewählt:

Einstellung	Voreinstellung	Begründung
Beitritt über E-Mail-Domain	**Anfrage**, nicht automatisch	Ein Beitritt soll eine bewusste Entscheidung bleiben
Sichtbarkeit von Krankheit	nur Führung und Personal	Der Grund geht Kolleginnen und Kollegen nichts an
Mindestgruppengröße für Auswertungen	5 Personen	Kleinere Gruppen sind faktisch personenbezogen
Auswertung der Bearbeitungsdauer je Führungskraft	**gibt es nicht**	Das wäre eine Leistungsauswertung
Messung in der Anwendung	**keine**	Eingeloggte Nutzung wird nicht ausgewertet
Push-Benachrichtigungen	**aus**, die Person schaltet sie je Gerät ein	Das Gerät gehört der Person
Lesestand eines Aushangs	nur Verfasser und Personalverwaltung	Wer was gelesen hat, geht Kollegen nichts an
Nachweise zu Qualifikationen	nur Person und Personalverwaltung	Bescheinigungen können auf die Gesundheit schließen lassen
Modul Fahrtenbuch	**aus**	Wird nur genutzt, wo der Betrieb es einschaltet
Aufzeichnung der Strecke	**aus**, auch bei eingeschaltetem Modul	Standortdaten nur, wo der Betrieb sie ausdrücklich will
Aufbewahrung der Strecke	**3 Monate**, über 6 Monate nur mit Begründung	Maßgeblich sind die Kilometerstände; die Strecke belegt die Fahrt nur ergänzend
Strecke bei Privatfahrt und Arbeitsweg	**nie**, nicht einstellbar	Private Wege gehen den Arbeitgeber nichts an
Wer die Strecke sieht	fahrende Person, Eigentümer, Administratoren und unternehmensweite Personalverwaltung, **nie** Führungskräfte	Keine Verhaltenskontrolle über die Führungslinie
Partner im Fahrtenbuch	mit Namen; auf Wunsch nur als Nummer	Für Berufsgeheimnisträger (§ 203 StGB)

4.3 Auftragskontrolle

- Unterauftragnehmer werden in einer öffentlich einsehbaren Liste geführt.
- Neue Unterauftragnehmer werden dem Verantwortlichen vorab mitgeteilt; ein Widerspruchsrecht besteht nach den Regelungen des Auftragsverarbeitungs- vertrags.

4.4 Zugriff durch den Auftragsverarbeiter

Ein Zugriff auf Kundendaten zu Supportzwecken erfolgt ausschließlich

1. auf Anlass des Kunden,
2. nach dessen ausdrücklicher Freigabe im Produkt,
3. zeitlich begrenzt,
4. vollständig protokolliert und
5. für den Kunden nachträglich einsehbar.

Zur Einrichtung und Unterstützung kann der Auftragsverarbeiter ohne diese Freigabe einen Einrichtungszugang öffnen (Auftragsverarbeitungsvertrag § 10 Abs. 4, ab der Fassung 2026-09-29). Er

1. wird nur mit festgehaltenem Anlass geöffnet,
2. endet spätestens nach sieben Tagen von selbst,
3. wird dem Kunden in der Anwendung angezeigt und kann von Eigentümer und Administratoren jederzeit beendet werden,
4. steht mit Öffnen, Beenden und Ablauf im Zugriffsprotokoll des Kunden; Änderungen dabei hält das Prüfprotokoll mit dem Auftragsverarbeiter als Handelndem fest,
5. belegt keinen Platz, entscheidet keine Anträge, empfängt keine Benachrichtigungen und kann AGB und Auftragsverarbeitungsvertrag nicht für den Kunden annehmen.

Hat ein Kunde eine ältere Fassung des Auftragsverarbeitungsvertrags angenommen, lässt die Anwendung den Einrichtungszugang nur während einer laufenden Freigabe nach Satz 1 zu.

---

5. In Vorbereitung

Damit dieses Dokument keine Zusagen macht, die noch nicht eingelöst sind:

- **Verschlüsselung der Sicherungsdateien auf dem Server** und **ältere Stände der hochgeladenen Dateien** (derzeit nur der letzte Stand); danach Festlegung von RTO und RPO (3.1, 3.2) — ohne festen Termin
- **Zeitgesteuerte Löschfristen** nach dem Löschkonzept, einschließlich der Anonymisierung nach Austritt — ohne festen Termin. Umgesetzt sind bisher die täglichen Läufe für Entscheidungslinks, für die Strecken im Fahrtenbuch nach der eingestellten Frist, für das Aufrufprotokoll der Programmierschnittstelle nach 90 Tagen und für Dateien, deren Unternehmen, Person oder Konto es nicht mehr gibt
- **Prüfung der Mandantentrennung als Sperre vor jeder Auslieferung** (1.3) — ohne festen Termin

---

Änderungen dieses Dokuments werden dem Verantwortlichen mitgeteilt. Die jeweils aktuelle Fassung ist unter `tiveo.de/sicherheit` abrufbar.
