



ART. 28 ABS. 3 DSGVO · ANLAGE ZU DEN AGB

Vertrag über die *Auftragsverarbeitung*

für die Nutzung der Organisationsplattform „TreueTakt“ durch ambulante Betreuungs-, Entlastungs- und Pflegedienste.

Version 0.9 (Entwurf) · Stand 30. September 2026

Entwurf, noch nicht unterschreiben lassen. Der Vertrag deckt alle Pflichtinhalte nach Art. 28 Abs. 3 DSGVO ab und beschreibt die tatsächlich umgesetzten Maßnahmen von TreueTakt. Vor dem Einsatz sollte eine Anwältin oder ein Anwalt für Datenschutz- und IT-Recht den Text prüfen. **Hervorgehobene Stellen** sind noch zu klären.

VERANTWORTLICHER („KUNDE“)

Name des Dienstes, Rechtsform

Anschrift

Vertreten durch

AUFTRAGSVERARBEITER („ANBIETER“)

Daniel Kroh, handelnd unter „TreueTakt“
(Einzelunternehmer)

Ausblick 1, 33100 Paderborn

info@treuetakt.de · +49 176 410 45 997

Auf einen Blick

- TreueTakt verarbeitet Ihre Daten nur nach Ihrer Weisung und nie für eigene Zwecke.
- Datenbank in Irland, Anwendung in Frankfurt; strikte Mandantentrennung auf Datenbankebene.
- Datenpannen meldet TreueTakt unverzüglich, spätestens innerhalb von 48 Stunden.
- Neue Unterauftragsverarbeiter werden vier Wochen vorher angekündigt, mit Widerspruchs- und Kündigungsrecht.
- Gesundheitsdaten und Schweigepflicht nach § 203 StGB sind ausdrücklich geregelt.
- Nach Vertragsende: 30 Tage Export, danach Löschung mit Bestätigung.

§ 1 *Gegenstand und Dauer*

- (1) Der Anbieter stellt dem Kunden die Plattform „TreueTakt“ nach den Allgemeinen Geschäftsbedingungen des Anbieters und etwaigen Individualvereinbarungen bereit („Hauptvertrag“). Dabei verarbeitet er personenbezogene Daten im Auftrag des Kunden. Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien. Die Begriffe haben die Bedeutung aus Art. 4 DSGVO.

- (2) Gegenstand, Art und Zweck der Verarbeitung, die Datenarten und die Kategorien betroffener Personen beschreibt Anlage 1.
 - (3) Dieser Vertrag gilt für die gesamte Dauer des Hauptvertrags, einschließlich einer unentgeltlichen Pilotphase, und darüber hinaus, solange der Anbieter noch Daten des Kunden verarbeitet (§ 11).
-

§ 2 Weisungen

- (1) Der Anbieter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Kunden, auch was Übermittlungen in Drittländer betrifft. Ausgenommen sind Verarbeitungen, zu denen der Anbieter nach dem Recht der EU oder Deutschlands verpflichtet ist. In diesem Fall teilt er dem Kunden die rechtliche Anforderung vorher mit, soweit das Recht dies nicht verbietet.
 - (2) Der Hauptvertrag, dieser Vertrag und die Einstellungen und Aktionen, die der Kunde in der Plattform vornimmt, gelten als Weisungen, zum Beispiel das Anlegen, Ändern, Exportieren und Anonymisieren von Datensätzen oder das Einschalten optionaler Funktionen. Darüber hinausgehende Weisungen erteilt der Kunde in Textform. Weisungsberechtigt sind die gesetzlichen Vertreter des Kunden und die Personen, die in der Plattform die Rolle „Administrator“ haben.
 - (3) Hält der Anbieter eine Weisung für rechtswidrig, teilt er das dem Kunden unverzüglich mit. Er darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.
-

§ 3 Pflichten des Anbieters

- (1) Der Anbieter nutzt die Daten nur für die Leistungen nach dem Hauptvertrag. Er verwendet sie nicht für eigene Zwecke, gibt sie nicht an Dritte weiter und fertigt keine Kopien an, außer Sicherungskopien und Kopien, die für den Betrieb technisch nötig sind. Technische Betriebsdaten ohne Bezug zu betreuten Personen darf er nach § 14 Abs. 3 der AGB auswerten.
 - (2) Alle Personen, die für den Anbieter Zugriff auf die Daten haben, sind schriftlich oder in Textform zur Vertraulichkeit verpflichtet und über den Datenschutz belehrt, soweit sie nicht schon gesetzlich zur Verschwiegenheit verpflichtet sind. Derzeit hat nur der Inhaber des Anbieters Zugriff.
 - (3) Der Anbieter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind (§ 5).
 - (4) Ansprechpartner für den Datenschutz ist Daniel Kroh, info@treuetakt.de. Der Anbieter hat derzeit keinen Datenschutzbeauftragten benannt. Sobald er nach Art. 37 DSGVO oder § 38 BDSG dazu verpflichtet ist, benennt er einen und teilt dem Kunden die Kontaktdaten mit. **Pflicht mit wachsender Kundenzahl prüfen**
-

§ 4 Pflichten des Kunden

- (1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für eine Rechtsgrundlage, die Information der betroffenen Personen und etwa erforderliche Einwilligungen.

- (2) Der Kunde informiert den Anbieter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.
- (3) Gesetzliche Aufbewahrungspflichten, etwa für Rechnungen und Leistungsnachweise, erfüllt der Kunde selbst, zum Beispiel über die Exportfunktion. Der Anbieter bewahrt Daten nicht über das Vertragsende hinaus für den Kunden auf.

§ 5 Technische und organisatorische Maßnahmen

- (1) Die Maßnahmen in Anlage 2 berücksichtigen den Stand der Technik, die Kosten, Art, Umfang und Zweck der Verarbeitung sowie das Risiko für die betroffenen Personen. Wegen der Gesundheitsdaten legt der Anbieter dabei ein erhöhtes Schutzniveau zugrunde.
- (2) Der Anbieter darf die Maßnahmen weiterentwickeln und durch gleichwertige oder bessere ersetzen, solange das Schutzniveau nicht sinkt. Wesentliche Änderungen dokumentiert er und teilt sie dem Kunden mit. Als „geplant“ gekennzeichnete Maßnahmen sind noch nicht umgesetzt; der Anbieter informiert, sobald sie in Betrieb sind.

§ 6 Unterauftragsverarbeiter

- (1) Der Kunde genehmigt die in Anlage 3 genannten Unterauftragsverarbeiter. Unterauftragsverarbeiter, die in Anlage 3 als optional gekennzeichnet sind, werden nur tätig, wenn der Kunde die zugehörige Funktion in der Plattform einschaltet.
- (2) Weitere oder andere Unterauftragsverarbeiter setzt der Anbieter nur ein, wenn er dies dem Kunden mindestens vier Wochen vorher in Textform ankündigt. Der Kunde kann der Änderung innerhalb dieser Frist aus sachlichem Grund widersprechen. Finden die Parteien keine Lösung, darf der Kunde den Hauptvertrag zum Zeitpunkt der Änderung außerordentlich kündigen. Ist ein Wechsel aus dringenden Gründen der Sicherheit oder Verfügbarkeit sofort nötig, informiert der Anbieter unverzüglich; das Widerspruchs- und Kündigungsrecht gilt dann entsprechend.
- (3) Der Anbieter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Datenschutzniveau, das diesem Vertrag entspricht, insbesondere auf geeignete technische und organisatorische Maßnahmen. Bei großen Infrastrukturanbietern geschieht dies über deren Auftragsverarbeitungsverträge, die der Anbieter vor dem Einsatz prüft.
- (4) Erfüllt ein Unterauftragsverarbeiter seine Datenschutzpflichten nicht, haftet der Anbieter dem Kunden dafür wie für eigenes Handeln (Art. 28 Abs. 4 Satz 2 DSGVO).
- (5) Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikation, Post und Transport sowie die Weiterleitung verschlüsselter Push-Nachrichten durch die Dienste der Browser- und Betriebssystemhersteller, die keinen Zugriff auf die Inhalte haben.

§ 7 Rechte der betroffenen Personen

- (1) Der Anbieter unterstützt den Kunden mit geeigneten Maßnahmen bei der Erfüllung der Rechte nach Art. 12 bis 23 DSGVO. Die Plattform bietet dafür insbesondere Funktionen zum Einsehen, Berichtigen, Exportieren und Anonymisieren von Daten.

- (2) Wendet sich eine betroffene Person direkt an den Anbieter, leitet er die Anfrage unverzüglich an den Kunden weiter und beantwortet sie nicht selbst, es sei denn, der Kunde weist ihn dazu an.
-

§ 8 *Meldung von Datenschutzverletzungen*

- (1) Der Anbieter meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden ist, möglichst innerhalb von 24 Stunden und spätestens innerhalb von 48 Stunden. Die Meldung erfolgt per E-Mail an die hinterlegte Adresse des Kunden und zusätzlich telefonisch, wenn die Verletzung Gesundheitsdaten betrifft.
 - (2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, betroffene Kategorien und ungefähre Zahl der Personen und Datensätze, wahrscheinliche Folgen und ergriffene oder vorgeschlagene Maßnahmen. Fehlende Angaben reicht der Anbieter nach, sobald er sie kennt.
 - (3) Der Anbieter ergreift unverzüglich die nötigen Maßnahmen, um die Daten zu sichern und nachteilige Folgen zu mindern. Er unterstützt den Kunden bei dessen Meldung an die Aufsichtsbehörde und der Benachrichtigung betroffener Personen (Art. 33, 34 DSGVO). Die Meldung selbst nimmt der Kunde vor.
-

§ 9 *Weitere Unterstützung*

- (1) Der Anbieter unterstützt den Kunden unter Berücksichtigung der verfügbaren Informationen bei den Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung und einer vorherigen Konsultation der Aufsichtsbehörde. Er stellt dafür die Beschreibung der Verarbeitung und der Maßnahmen (Anlagen 1 bis 3) bereit.
 - (2) Für Unterstützung, die über die Funktionen der Plattform und die Bereitstellung dieser Unterlagen hinausgeht und nicht durch einen Verstoß des Anbieters veranlasst ist, kann der Anbieter eine angemessene Vergütung verlangen, wenn er diese vorher ankündigt.
-

§ 10 *Nachweise und Kontrollen*

- (1) Der Anbieter stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind. Dazu gehören eine aktuelle Beschreibung der Maßnahmen, die Liste der Unterauftragsverarbeiter und die Nachweise der Infrastrukturanbieter, etwa deren SOC-2- oder ISO-27001-Berichte, soweit diese weitergegeben werden dürfen.
- (2) Reichen diese Nachweise im Einzelfall nicht aus, darf der Kunde Überprüfungen einschließlich Inspektionen durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, der kein Wettbewerber des Anbieters ist. Überprüfungen sind mindestens vier Wochen vorher anzukündigen, finden während der üblichen Geschäftszeiten statt und sollen den Betrieb nicht unverhältnismäßig stören. Außer nach einer Datenschutzverletzung sind sie auf eine im Kalenderjahr beschränkt.
- (3) Die Kosten einer Überprüfung trägt der Kunde, es sei denn, sie deckt einen erheblichen Verstoß des Anbieters auf. Rechte der Aufsichtsbehörden bleiben unberührt.

§ 11 Rückgabe und Löschung

- (1) Nach dem Ende des Hauptvertrags kann der Kunde seine Daten noch 30 Tage lang über die Plattform exportieren oder beim Anbieter einen Export in gängigen Formaten (CSV, PDF) anfordern.
- (2) Nach Ablauf dieser Frist löscht der Anbieter alle personenbezogenen Daten des Kunden innerhalb von weiteren 30 Tagen, einschließlich gespeicherter Dateien wie Unterschriften und Dokumente. Sicherungskopien werden im regulären Rotationszyklus überschrieben, spätestens 30 Tage nach der Löschung. Bis dahin sind sie gegen jede weitere Nutzung gesperrt. **Aufbewahrungsdauer der Backups prüfen**
- (3) Eine Pflicht des Anbieters, Daten länger zu speichern, besteht nicht, soweit nicht eine Rechtsvorschrift ihn selbst dazu verpflichtet. Der Anbieter bestätigt die Löschung auf Anfrage in Textform.

§ 12 Gesundheitsdaten und Schweigepflicht

- (1) Die Verarbeitung kann besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO umfassen, insbesondere Pflegegrade, Angaben zu Leistungen der Pflegeversicherung und Tätigkeitsbeschreibungen aus Einsätzen. Der Kunde gibt solche Daten nur ein, soweit sie für seine Leistung und Abrechnung erforderlich sind.
- (2) Soweit der Kunde oder seine Beschäftigten einer Schweigepflicht nach § 203 StGB unterliegen, wirkt der Anbieter als sonstige mitwirkende Person im Sinne von § 203 Abs. 3 Satz 2 StGB mit. Der Kunde verpflichtet den Anbieter hiermit zur Geheimhaltung; der Anbieter nimmt diese Verpflichtung an und wurde auf die Strafbarkeit einer Verletzung (§ 203 Abs. 4 StGB) hingewiesen. Er nimmt von geschützten Geheimnissen nur Kenntnis, soweit dies für die Leistung erforderlich ist.
- (3) Der Anbieter verpflichtet Personen, die er selbst hinzuzieht, in Textform zur Geheimhaltung. Bei Unterauftragsverarbeitern stellt er eine entsprechende Vertraulichkeit vertraglich sicher, bei großen Infrastrukturanbietern über deren Vertraulichkeitsregelungen. **Anwaltlich prüfen**

§ 13 Ort der Verarbeitung und Drittländer

- (1) Die Daten werden in Rechenzentren in der Europäischen Union gespeichert und verarbeitet: die Datenbank und Dateiablage in Irland, die Anwendung in Frankfurt am Main (Anlage 3).
- (2) Mehrere Unterauftragsverarbeiter haben ihren Sitz in den USA oder gehören zu Unternehmen dort. Ein Zugriff aus einem Drittland oder eine Übermittlung dorthin ist daher nicht vollständig auszuschließen, etwa im Rahmen von Support oder Wartung. Solche Übermittlungen erfolgen nur auf Grundlage der Art. 44 ff. DSGVO, insbesondere nach einem Angemessenheitsbeschluss (EU-US Data Privacy Framework) oder mit EU-Standardvertragsklauseln. Die jeweilige Grundlage nennt Anlage 3.
- (3) Der Kunde erteilt mit diesem Vertrag die Weisung für diese Übermittlungen im Umfang von Anlage 3.

§ 14 Haftung

Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO. Im Verhältnis zwischen den Parteien gelten die Haftungsregeln des Hauptvertrags (§§ 5 und 13 der AGB), soweit Art. 82 DSGVO nicht entgegensteht.

§ 15 Schlussbestimmungen

- (1) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht in Fragen des Datenschutzes dieser Vertrag vor.
- (2) Änderungen und Ergänzungen bedürfen der Textform. Anlage 3 ändert der Anbieter nach dem Verfahren in § 6 Abs. 2, Anlage 2 nach § 5 Abs. 2.
- (3) Ist eine Bestimmung unwirksam, bleiben die übrigen Bestimmungen wirksam. Im Übrigen gelten die Schlussbestimmungen der AGB, einschließlich Rechtswahl und Gerichtsstand.
- (4) Der Vertrag kann in Textform geschlossen werden, auch elektronisch in der Plattform (Art. 28 Abs. 9 DSGVO).

Ort, Datum, Unterschrift
Verantwortlicher (Kunde)

Paderborn, Datum, Unterschrift
Auftragsverarbeiter (Daniel Kroh, TreueTakt)

ANLAGE 1

Beschreibung der Verarbeitung

Merkmal	Beschreibung
Gegenstand	Bereitstellung und Betrieb der Plattform „TreueTakt“ als Software as a Service für den Kunden, einschließlich Support und Fehlerbehebung.
Zweck	Stammdatenverwaltung, Einsatz- und Dienstplanung, mobile Leistungserfassung und Zeiterfassung, digitale Unterschriften und Leistungsnachweise, Rechnungsstellung, Übersicht über Leistungsbudgets der Pflegeversicherung, Personalverwaltung des Kunden, Benachrichtigungen per E-Mail und Push, optional KI-gestützte Kürzung von Tätigkeitstexten.
Art der Verarbeitung	Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln (E-Mail, PDF-Erzeugung), Einschränken, Anonymisieren, Löschen.
Betroffene Personen	Betreute Personen des Kunden · deren Angehörige, Kontaktpersonen und abweichende Rechnungsempfänger · Beschäftigte des Kunden (Verwaltung und Mitarbeitende im Einsatz) · Ansprechpartner bei Kostenträgern.
Datenarten betreute Personen	Name, Anschrift, Kontaktdaten, Geburtsdatum, Kundennummer, Pflegekasse und Versichertennummer, Termine und Einsätze, erbrachte Leistungen und Zeiten, gefahrene Kilometer, Tätigkeitsbeschreibungen, Unterschriften, Leistungsnachweise, Rechnungen, Budgetstände, hochgeladene Dokumente, Sterbedatum.
Datenarten Beschäftigte	Name, Kontaktdaten, Login-Daten, Rolle, Personalnummer, Qualifikationen, Lohnfaktoren (Stundensatz, Kilometergeld, Zuschläge), Arbeitszeiten und Einsätze, Foto, Personaldokumente, Unterschriften, Push-Abonnements.
Besondere Kategorien (Art. 9 DSGVO)	Gesundheitsdaten, insbesondere Pflegegrad und Pflegegrad-Datum, Leistungsansprüche nach SGB XI und SGB V sowie Angaben in Tätigkeitsbeschreibungen und Dokumenten, soweit der Kunde sie einträgt.
Nicht vorgesehen	Daten aus Leistungen nach dem Vierten Kapitel des SGB V, insbesondere häusliche Krankenpflege (§ 37 SGB V) und Haushaltshilfe (§ 38 in Verbindung mit § 132 SGB V), wegen § 393 SGB V (§ 9 Abs. 7 AGB). Medizinische und ärztliche Dokumentation.

ANLAGE 2

Technische und organisatorische Maßnahmen

Stand 30. September 2026. Die Kennzeichnung zeigt, was heute in Betrieb ist **UMGESETZT** und was noch folgt **GEPLANT**.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Bereich	Maßnahme	Status
Zutritt	Betrieb ausschließlich in Rechenzentren der Infrastrukturanbieter (Supabase auf AWS in Irland, Vercel in Frankfurt), die nach SOC 2 Typ II bzw. ISO 27001 geprüft sind. Der Anbieter betreibt keine eigenen Server.	UMGESETZT
Zugang	Persönliche Benutzerkonten, keine Sammelkonten. Passwörter werden nur als Hash gespeichert (Supabase Auth, bcrypt). Anmeldung ausschließlich über HTTPS.	UMGESETZT
Zugang	Zwei-Faktor-Anmeldung für Administratoren des Kunden.	GEPLANT
Zugang Anbieter	Administrativer Zugriff auf Datenbank und Hosting nur durch den Inhaber, mit Zwei-Faktor-Anmeldung bei Supabase, Vercel und GitHub. Arbeitsgerät mit Festplattenverschlüsselung und automatischer Bildschirmsperre. bestätigen	UMGESETZT
Zugriff	Rollenkonzept (Plattform-Administrator, Administrator des Kunden, Mitarbeitende). Mitarbeitende sehen nur ihre eigenen Einsätze und die dafür nötigen Daten. Durchgesetzt auf Datenbankebene durch PostgreSQL Row Level Security auf jeder Tabelle; Rechte werden explizit vergeben.	UMGESETZT
Zugriff	Der Schlüssel mit Vollzugriff auf die Datenbank wird nur serverseitig verwendet, liegt nicht im Quellcode und wird nie an Endgeräte ausgeliefert.	UMGESETZT
Trennung	Mandantentrennung: Jeder Datensatz ist an die Organisation des Kunden gebunden; die Datenbank erzwingt die Trennung unabhängig von der Anwendung. Die öffentliche Website läuft in einem getrennten Datenbankprojekt ohne Kundendaten.	UMGESETZT
Trennung	Entwicklung und automatisierte Tests laufen gegen eine lokale Datenbank mit Testdaten.	UMGESETZT
Datenminimierung	KI-Funktionen sind standardmäßig ausgeschaltet und nur nach Einschalten durch den Kunden aktiv. Keine Werbe-Tracker in der Anwendung, kein Profiling.	UMGESETZT

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Bereich	Maßnahme	Status
Weitergabe	Transportverschlüsselung (TLS) für alle Verbindungen zwischen Endgerät, Anwendung und Datenbank. Verschlüsselung der gespeicherten Daten und Dateien durch den Infrastrukturanbieter (AES-256). Push-Nachrichten sind Ende-zu-Ende verschlüsselt (Web-Push-Standard).	UMGESETZT
Eingabe	Zentrale Datensätze speichern Zeitpunkt der Erstellung und Änderung und die handelnde Person. Leistungsnachweise mit Unterschrift werden automatisch ungültig, wenn der zugrunde liegende Einsatz nachträglich geändert wird.	UMGESETZT
Eingabe	Vollständiges Änderungsprotokoll (Audit-Log) für personenbezogene Daten.	GEPLANT

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

Bereich	Maßnahme	Status
Datensicherung	Tägliche automatische Sicherung der Datenbank durch Supabase, verschlüsselt, in der EU. Supabase-Plan prüfen: im Free-Plan gibt es keine Backups	UMGESETZT
Wiederherstellung	Dokumentiertes Wiederherstellungsverfahren und jährlicher Test der Wiederherstellung.	GEPLANT
Überwachung	Fehlerüberwachung mit Alarmierung (Sentry, ohne personenbezogene Inhalte) und Verfügbarkeitsüberwachung (Better Stack).	GEPLANT
Aktualität	Abhängigkeiten und Laufzeitumgebung werden regelmäßig aktualisiert; die Infrastruktur wird vom Anbieter der Plattform gepatcht.	UMGESETZT

Überprüfung und Organisation (Art. 32 Abs. 1 lit. d, Art. 25 DSGVO)

Bereich	Maßnahme	Status
Entwicklung	Jede Änderung durchläuft vor der Auslieferung automatische Prüfungen (Typprüfung, Linting, Build, Unit-Tests, Datenbanktests gegen die Zugriffsregeln).	UMGESETZT
Entwicklung	Auslieferung nur bei erfolgreichen Prüfungen (Deploy-Gate), automatische Suche nach versehentlich gespeicherten Zugangsdaten.	GEPLANT
Löschkonzept	Zweistufiges Löschkonzept: Anonymisierung von Stammdaten nach Ablauf der Verjährung, Löschung von Belegen nach Ablauf der Aufbewahrungsfristen. Löschanträge werden in der Plattform erfasst und dokumentiert.	UMGESETZT
Auftragskontrolle	Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern; Prüfung von Datenstandort und Drittlandgarantien vor dem Einsatz; jährliche Überprüfung der Liste.	UMGESETZT
Datensparsamkeit	In der Plattform sind keine Analyse-, Tracking- oder Sitzungsaufzeichnungsdienste eingebunden. Die Nutzungsanalyse der öffentlichen Website (PostHog, EU-Server) ist technisch von der Plattform getrennt, läuft nur nach Einwilligung der Websitebesucher und verarbeitet keine Daten nach Anlage 1.	UMGESETZT
Vorfälle	Schriftlicher Ablauf zum Erkennen, Bewerten und Melden von Datenschutzverletzungen (§ 8).	GEPLANT
Überprüfung	Überprüfung dieser Maßnahmen mindestens jährlich und bei wesentlichen Änderungen der Plattform.	UMGESETZT

ANLAGE 3

Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Standort der Daten	Daten	Drittland-Grundlage
Supabase, Inc. San Francisco, USA	Datenbank, Anmeldung, Dateiablage (Unterschriften, Fotos, Dokumente)	Irland (AWS eu-west-1)	Alle Daten nach Anlage 1	EU-Standardvertragsklauseln DPA prüfen
Vercel Inc. Covina, USA	Betrieb der Anwendung, Serverfunktionen, zeitgesteuerte Aufgaben	Frankfurt am Main (fra1)	Alle Daten nach Anlage 1 im Durchlauf, keine dauerhafte Speicherung	EU-US Data Privacy Framework, ergänzend Standardvertragsklauseln DPA prüfen
Resend (Plus Five Five, Inc.) USA	Versand von E-Mails, etwa Einladungen und Unterschriften-Erinnerungen	Region prüfen (EU verfügbar)	Name und E-Mail der Empfänger, Inhalt der E-Mail	EU-Standardvertragsklauseln DPA prüfen
Anthropic USA · <i>optional</i>	KI-gestützte Kürzung von Tätigkeitstexten, nur wenn der Kunde die Funktion einschaltet	USA prüfen	Übergebener Tätigkeitstext, keine Stammdaten	EU-Standardvertragsklauseln; vor Aktivierung AVV abschließen

Keine Unterauftragsverarbeiter (§ 6 Abs. 5): Die Push-Dienste der Browser- und Betriebssystemhersteller (Google, Apple, Mozilla) leiten nur Ende-zu-Ende verschlüsselte Benachrichtigungen an die Geräte der Mitarbeitenden weiter und haben keinen Zugriff auf deren Inhalt. Ebenfalls kein Unterauftragsverarbeiter ist **PostHog**: Der Dienst wertet nur die Nutzung der öffentlichen Website treuetakt.de aus, in eigener Verantwortung des Anbieters und mit Einwilligung der Besucher, und erhält keine Daten aus der Plattform.

AUFTRAGSVERARBEITER

TreueTakt · Inhaber Daniel Kroh (Einzelunternehmer) · Ausblick 1 · 33100 Paderborn
info@treuetakt.de · +49 176 410 45 997 · treuetakt.de