Auftragsverarbeitungsvertrag (AVV)

Software TimeShift - Schichtplanung, Arbeitszeiterfassung, Mitarbeiterverwaltung

Stand: Juni 2026

Zwischen

1. Verantwortlicher (Auftraggeber / Kunde)	
Firma / Name	
Ansprechpartner	
Straße, Hausnummer	
PLZ, Ort	
Land	Deutschland
E-Mail	
Telefon (optional)	

2. Auftragsverarbeiter (Anbieter)	
Firma	TimeShift (Einzelunternehmen)
Inhaber	Robin Stenzel
Geschäftsanschrift	Lange Straße 43, 32791 Lage, Deutschland
E-Mail	info@trytimeshift.com
Handelsregister	entfällt (Einzelunternehmen)
USt-IdNr.	[wird nach Eintragung ergänzt]

Präambel

Der Verantwortliche nutzt die Software **TimeShift** zur digitalen Schichtplanung, Arbeitszeiterfassung und Organisation von Mitarbeitern. TimeShift stellt hierfür die technische Plattform bereit und verarbeitet personenbezogene Daten **ausschließlich im Auftrag** und nach **Weisung** des Verantwortlichen gemäß Art. 28 DSGVO.

Dieser Vertrag konkretisiert die in den Allgemeinen Geschäftsbedingungen (AGB) geregelte Auftragsverarbeitung.

---

§ 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch TimeShift im Auftrag des Verantwortlichen bei Nutzung der Software TimeShift (Web-App, iOS-App, Android-App).

(2) Die Verarbeitung beginnt mit Abschluss des Hauptvertrages (Nutzungsvertrag / Abonnement) und läuft für dessen Dauer. Sie endet mit Beendigung des Hauptvertrages, vorbehaltlich § 10 (Löschung / Rückgabe).

(3) TimeShift verarbeitet Daten **nicht** zu eigenen Zwecken, insbesondere nicht zu Werbung, Profilbildung oder Weiterverkauf von Daten.

§ 2 Art und Zweck der Verarbeitung

TimeShift verarbeitet personenbezogene Daten ausschließlich zu folgenden Zwecken im Auftrag des Verantwortlichen:

Zweck	Beschreibung
Bereitstellung der Plattform	Betrieb, Wartung und Weiterentwicklung der Software
Schichtplanung	Erstellung, Veröffentlichung und Verwaltung von Schichtplänen
Arbeitszeiterfassung	Erfassung von Arbeits-, Pausen- und Buchungszeiten
Mitarbeiterverwaltung	Verwaltung von Mitarbeiterkonten, Rollen, Einladungen, PIN-Zugängen
Kommunikation im System	Kommentare, Hinweise, Tauschanfragen, Benachrichtigungen
Check-In / Standortprüfung	Ereignisbezogene Standortprüfung zur Missbrauchsvermeidung (sofern aktiviert)
Abrechnung des Vertrages	Verwaltung von Abo-Status und Tarifinformationen (ohne Speicherung von Zahlungsdaten)
Sicherheit & Stabilität	Protokollierung, Fehleranalyse, Missbrauchsprävention
Support	Bearbeitung von Anfragen des Verantwortlichen

§ 3 Art der personenbezogenen Daten

3.1 Personen- und Kontodaten: Name, E-Mail-Adresse, Benutzer-ID (Firebase UID), Rolle, Arbeitgeber-ID, Registrierungsstatus

3.2 Organisations- und Mitarbeiterdaten: Zuordnung zu Arbeitgebern, Einladungen, PIN-Zuweisungen, Beschäftigungsart, Stundenlimits, Status (aktiv/deaktiviert), optional Personalnummer

3.3 Arbeitszeit- und Schichtdaten: Schichtzeiten, Arbeitszeiten, Pausen, Buchungen, veröffentlichte Schichten, Status, Vergütungsstatus, Historie

3.4 Mitarbeiteraktionen: Schichtwünsche, Stornierungen, Begründungen (Freitext - Verantwortung beim Verantwortlichen)

3.5 Abwesenheitsdaten: Abwesenheitsstatus (z. B. krank, abwesend) - keine medizinischen Diagnosen

3.6 Kommunikationsdaten: Kommentare, Hinweise, Anweisungen im Rahmen der Schichtplanung

3.7 Standortdaten: Ereignisbezogene Standortdaten beim Check-In/Check-Out (keine Dauerortung)

3.8 Geräte- und Terminaldaten: Geräte-IDs, Terminal-Kennungen, Zuordnung zu Check-In-Vorgängen

3.9 Technische Zugriffsdaten: IP-Adresse (ggf. gekürzt), Datum/Uhrzeit, Browser-/Geräteinformationen, App-Version, Log- und Sicherheitsdaten

3.10 Abrechnungs- und Vertragsdaten: Tarif, Abo-Status, Laufzeit - keine Kreditkarten- oder Kontodaten (Verarbeitung durch Stripe / App Store)

Besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO werden nicht vorsätzlich verarbeitet. Soweit der Verantwortliche dennoch solche Daten in Freitextfeldern erfasst, liegt die Verantwortung hierfür beim Verantwortlichen.

§ 4 Kategorien betroffener Personen

• Arbeitnehmer und Beschäftigte des Verantwortlichen (Nutzer mit Mitarbeiterrolle)

• Bevollmächtigte des Verantwortlichen (Administratoren, Planer)

• Ggf. eingeladene, noch nicht registrierte Personen (Einladungs-E-Mail)

§ 5 Weisungsrecht des Verantwortlichen

(1) TimeShift verarbeitet personenbezogene Daten **nur auf dokumentierte Weisung** des Verantwortlichen, sofern nicht eine gesetzliche Verpflichtung besteht (Art. 28 Abs. 3 lit. a DSGVO).

(2) Weisungen ergeben sich aus diesem AVV, dem Nutzungsvertrag / den AGB, der Datenschutzerklärung von TimeShift, der Konfiguration in der Software sowie weiteren schriftlichen Weisungen per E-Mail an TimeShift.sp@gmail.com.

(3) Hält TimeShift eine Weisung für rechtswidrig, teilt sie dies dem Verantwortlichen unverzüglich mit (Art. 28 Abs. 3 Satz 3 DSGVO).

§ 6 Pflichten des Auftragsverarbeiters

(1) TimeShift verpflichtet sich, personenbezogene Daten nur im Rahmen dieses Vertrages zu verarbeiten;

(2) TimeShift verpflichtet sich, sicherzustellen, dass sich zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet haben;

(3) TimeShift verpflichtet sich, die in **Anlage 1** (TOMs) beschriebenen Maßnahmen umzusetzen;

(4) TimeShift verpflichtet sich, den Verantwortlichen bei der Erfüllung der Rechte betroffener Personen (Art. 15-22 DSGVO) zu unterstützen;

(5) TimeShift verpflichtet sich, den Verantwortlichen bei Datenschutz-Folgenabschätzungen (Art. 35, 36 DSGVO) angemessen zu unterstützen;

(6) TimeShift verpflichtet sich, personenbezogene Daten nach Abschluss der Leistung gemäß § 10 zu löschen oder zurückzugeben;

(7) TimeShift verpflichtet sich, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO zur Verfügung zu stellen;

(8) TimeShift verpflichtet sich, Unterstützung bei der Meldung von Datenschutzverletzungen (§ 8) zu leisten.

§ 7 Vertraulichkeit

(1) TimeShift behandelt alle im Rahmen dieses Vertrages bekannt gewordenen personenbezogenen Daten und Geschäftsinformationen vertraulich.

(2) Die Vertraulichkeitspflicht besteht über das Vertragsende hinaus fort.

§ 8 Meldung von Datenschutzverletzungen

(1) TimeShift informiert den Verantwortlichen **unverzüglich**, spätestens innerhalb von **48 Stunden**, nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten.

(2) Die Meldung enthält mindestens: Art der Verletzung, betroffene Datenkategorien und ungefähre Zahl betroffener Personen, wahrscheinliche Folgen sowie ergriffene Abhilfemaßnahmen.

(3) TimeShift unterstützt den Verantwortlichen bei dessen Meldepflichten gegenüber Aufsichtsbehörde und betroffenen Personen, soweit zumutbar.

§ 9 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich durch geeignete Maßnahmen (z. B. Fragebogen, Einsicht in aktuelle TOMs, Zertifikate) vom ordnungsgemäßen Datenschutz überzeugen.

(2) Audits vor Ort sind nach **vorheriger Terminvereinbarung** (mindestens 14 Tage Vorlauf) zulässig, höchstens **einmal jährlich**, sofern kein konkreter Anlass besteht.

(3) TimeShift kann Nachweise auch durch aktuelle Zertifizierungen oder Prüfberichte Dritter (z. B. SOC-Berichte der Cloud-Anbieter) erbringen.

§ 10 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Hauptvertrages löscht TimeShift alle personenbezogenen Daten des Verantwortlichen aus produktiven Systemen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(2) Der Verantwortliche kann vor Löschung einen **Export** seiner Daten anfordern (soweit technisch verfügbar).

(3) Backups werden im Rahmen üblicher Rotationsfristen (max. **90 Tage**) überschrieben.

(4) Aggregierte, anonymisierte Statistiken ohne Personenbezug können gespeichert bleiben.

§ 11 Unterauftragsverarbeiter

(1) Der Verantwortliche **erteilt die allgemeine Genehmigung**, TimeShift weitere Unterauftragsverarbeiter einzusetzen.

(2) Aktuell eingesetzte Unterauftragsverarbeiter sind in **Anlage 2** aufgeführt.

(3) TimeShift informiert den Verantwortlichen über beabsichtigte Änderungen mit mindestens **30 Tagen** Vorlauf. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen und den Hauptvertrag kündigen.

(4) TimeShift stellt sicher, dass mit Unterauftragsverarbeitern Verträge gemäß Art. 28 Abs. 4 DSGVO bestehen.

§ 12 Drittlandübermittlungen

(1) Die **Hauptverarbeitung** erfolgt in der **EU** (Rechenzentrum **europe-west3**, Frankfurt am Main - Google Cloud / Firebase).

(2) Einzelne Unterauftragsverarbeiter (z. B. Apple Inc., RevenueCat, Inc.) können Daten in Drittländern (insb. USA) verarbeiten, auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission und/oder der EU-Standardvertragsklauseln (SCC).

(3) Eine aktuelle Übersicht ergibt sich aus Anlage 2.

§ 13 Haftung

Die Haftung richtet sich nach den Regelungen des **Hauptvertrages (AGB)** und den gesetzlichen Vorschriften, insbesondere Art. 82 DSGVO.

§ 14 Laufzeit und Änderungen

(1) Dieser AVV tritt mit Unterzeichnung / Akzeptanz durch den Verantwortlichen in Kraft und läuft parallel zum Hauptvertrag.

(2) TimeShift kann diesen AVV bei relevanten Rechtsänderungen anpassen. Der Verantwortliche wird mindestens **30 Tage** vorher informiert. Ohne Widerspruch gilt die Fortführung als Zustimmung.

§ 15 Schlussbestimmungen

(1) Es gilt das Recht der **Bundesrepublik Deutschland** unter Ausschluss des UN-Kaufrechts.

(2) Gerichtsstand ist, soweit zulässig, der Sitz des Auftragsverarbeiters (**Höxter**).

(3) Salvatorische Klausel: Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

(4) Anlagen sind Bestandteil dieses Vertrages: **Anlage 1** (TOMs), **Anlage 2** (Unterauftragsverarbeiter).

Unterschriften

Verantwortlicher (Auftraggeber)	Auftragsverarbeiter (TimeShift)
Ort, Datum: _____	Ort, Datum: _____
Unterschrift: _____	Unterschrift: Robin Stenzel
Name: _____	TimeShift (Einzelunternehmen)

Alternative Akzeptanz (digital): Der Verantwortliche akzeptiert diesen AVV durch Aktivierung eines Kontrollkästchens bei Registrierung / im Konto-Bereich mit dem Text: *Ich schliesse den Auftragsverarbeitungsvertrag (AVV) mit TimeShift ab.*

Anlage 1 - Technische und organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO · Stand: Juni 2026

1. Vertraulichkeit

Maßnahme	Umsetzung bei TimeShift
Zugangskontrolle	Firebase Authentication; rollenbasierte Zugriffe (Admin/Mitarbeiter); Firestore Security Rules
Weitergabekontrolle	TLS-Verschlüsselung (HTTPS); verschlüsselte Verbindungen zu APIs
Eingabekontrolle	Protokollierung von Admin-Aktionen; Mandantentrennung (Arbeitgeber-IDs)
Verfügbarkeitskontrolle	Cloud-Infrastruktur Google Firebase; regionale Deployment-Zone EU
Trennungskontrolle	Logische Mandantentrennung in Firestore (arbeitgeber/{id}/…); getrennte Nutzerkonten

2. Integrität

Maßnahme	Umsetzung bei TimeShift
Datenintegrität	Firestore-Transaktionen wo erforderlich; serverseitige Validierung (Cloud Functions)
Schutz vor Manipulation	Security Rules; keine direkte Client-Schreibberechtigung auf fremde Mandanten

3. Verfügbarkeit und Belastbarkeit

Maßnahme	Umsetzung bei TimeShift
Hosting	Google Cloud / Firebase (SLA des Anbieters)
Region	europe-west3 (Frankfurt) für Firestore, Cloud Functions, Hosting
Backups	Firebase/Google Cloud Backup-Mechanismen; Wiederherstellung nach Anbieter-Standards
Monitoring	Firebase / Cloud Logging; interne Fehlerprotokolle

4. Wiederherstellbarkeit

Maßnahme	Umsetzung bei TimeShift
Disaster Recovery	Wiederherstellung über Cloud-Anbieter; Export-Funktionen für Kunden auf Anfrage
Backup-Rotation	Max. 90 Tage in Backups, danach Überschreibung

5. Pseudonymisierung / Verschlüsselung

Maßnahme	Umsetzung bei TimeShift
Transport	TLS 1.2+ für alle Verbindungen
Speicherung	Verschlüsselung at rest durch Google Cloud (Firebase Standard)
Passwörter	Hashing durch Firebase Authentication (kein Klartext-Speicher)

6. Organisatorische Maßnahmen

Maßnahme	Umsetzung bei TimeShift
Zugriffsrechte	Zugriff auf Produktivdaten nur für autorisierte Personen (Robin Stenzel)
Vertraulichkeit	Vertraulichkeitsverpflichtung für alle mit Zugriff

Datensparsamkeit	Minimierung der verarbeiteten Daten
Dokumentation	Datenschutzerklärung und dieser AVV

Anlage 2 - Unterauftragsverarbeiter

Nr.	Anbieter	Leistung	Daten	Region	Schutz
1	Google Ireland Ltd.	Firebase (Auth, Firestore, Functions, Hosting)	Nutzerkonten, App-Daten, Logs	EU-West3 Frankfurt	SCC
2	Stripe Payments Europe Ltd.	Zahlungsabwicklung Web	Name, E-Mail, Abo	EU Irland	SCC
3	Apple Inc.	App Store, IAP iOS	Apple-ID, Kauf-Ref.	EU/USA	SCC
4	Google LLC	Google Play Store	Store-Metadaten	EU/USA	SCC
5	RevenueCat Inc.	Abo-Sync iOS	UID, Abo-Status	USA	SCC
6	Google Ireland Ltd.	Google Sign-In	E-Mail, Name	EU/USA	SCC
7	Apple Inc.	Sign in with Apple	Apple-ID, E-Mail	EU/USA	SCC
8	Google Ireland Ltd.	Cloud Vision API OCR	Schichtplan-Bilder	EU-West3	SCC
9	Resend Inc.	Transaktions-E-Mails	E-Mail, Name	USA	SCC
10	OpenStreetMap Nominatim	Geocoding	Koordinaten	variabel	ggf. SCC

Die aktuelle Liste kann jederzeit unter **trytimeshift.com/datenschutz** eingesehen werden. Die Liste wird bei neuen Dienstleistern gemäß § 11 AVV ergänzt.

Anlage 3 - Kurzinformation für den Verantwortlichen (Checkliste)

■ Datenschutzerklärung für die eigenen Mitarbeiter (als Arbeitgeber)

■ Rechtsgrundlage für Schicht- und Zeiterfassung (Arbeitsvertrag, Betriebsvereinbarung)

■ Information der Mitarbeiter über TimeShift als Auftragsverarbeiter

■ Ggf. Betriebsrat / Mitarbeitervertretung einbinden

■ Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) aktualisieren

■ AVV mit TimeShift abgeschlossen (dieses Dokument)