Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Version: 1.1

Stand: 12. Juni 2026

Gültig ab: 12. Juni 2026

Vertragsbestandteil: Dieser Auftragsverarbeitungsvertrag (AVV) ist Bestandteil des Hauptvertrags und der Allgemeinen Geschäftsbedingungen über die Nutzung von Shiftdesk. Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieses AVV für die Auftragsverarbeitung vor.

PDF-Fassung: Diese Fassung als PDF herunterladen (Version 1.1) — z. B. für Ihr Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO).

Dieser Auftragsverarbeitungsvertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien für die Verarbeitung personenbezogener Daten im Auftrag des Kunden gemäß Art. 28 DSGVO.

§ 1 Parteien

Auftragnehmerin ist Valerie Koch, handelnd unter „Shiftdesk", Herforder Str. 176, 33609 Bielefeld, Deutschland, E-Mail: support@shiftdesk.app (nachfolgend „Auftragnehmerin").

Auftraggeber ist der jeweilige Kunde, der den Dienst Shiftdesk als Arbeitgeber oder Unternehmen nutzt (nachfolgend „Auftraggeber"). Die Identität des Auftraggebers ergibt sich aus dem Hauptvertrag.

§ 2 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand der Verarbeitung ist die Bereitstellung des Software-as-a-Service-Dienstes Shiftdesk zur Dienstplanung, Arbeitszeiterfassung, Abwesenheitsverwaltung, Teamkommunikation, arbeitszeitrechtlichen Plausibilitätsprüfung und Lohnvorbereitung.

(2) Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Sie endet mit dessen Beendigung; nachvertragliche Pflichten zur Löschung und Rückgabe (§ 12) bleiben unberührt.

§ 3 Art und Zweck der Verarbeitung

(1) Die Verarbeitung umfasst insbesondere das Erheben, Speichern, Strukturieren, Anzeigen, Ändern, Übermitteln, Exportieren, das Einschränken sowie das Löschen personenbezogener Daten im Rahmen der vom Auftraggeber konfigurierten Nutzung von Shiftdesk.

(2) Zwecke sind insbesondere Personalverwaltung, Dienstplanung, Arbeitszeiterfassung, Abwesenheitsverwaltung, Teamkommunikation, Auditierung, Reporting, Datenexport und die technische Vorbereitung der Lohnabrechnung durch den Auftraggeber.

§ 4 Kategorien betroffener Personen

Betroffene Personen sind insbesondere:

- Beschäftigte des Auftraggebers (unbefristet, befristet, Teilzeit, Minijob, Werkstudierende, Aushilfen)
- Bewerberinnen und Bewerber, soweit vom Auftraggeber im Dienst geführt
- Freie Mitarbeitende und Subunternehmende, soweit vom Auftraggeber im Dienst geführt
- Ansprechpartner des Auftraggebers
- Administratoren, Planerinnen und Planer, Teamleitungen sowie sonstige vom Auftraggeber angelegte Nutzerinnen und Nutzer

§ 5 Kategorien personenbezogener Daten

Verarbeitet werden je nach Konfiguration und Nutzung des Auftraggebers insbesondere folgende Datenkategorien:

- **Stammdaten:** Name, Kontaktdaten, Anschrift, Personalnummer, Eintrittsdatum
- **Beschäftigungsdaten:** Vertragsart, Arbeitszeitmodell, Rolle und Berechtigungen, Qualifikationen, Standort, Abteilung, Team
- **Arbeitszeitdaten:** Dienstpläne, Zeitbuchungen, Pausen, Korrekturen, Geräte-IP zum Zeitpunkt der Buchung
- **Optionale Standortdaten:** GPS-Position zum Zeitpunkt des Stempelvorgangs, sofern vom Auftraggeber pro Standort aktiviert
- **Abwesenheitsdaten:** Urlaub, Krankheit (ausschließlich Typ-Information ohne Diagnose), Mutterschutz, Elternzeit, sonstige Abwesenheiten
- **Kommunikationsdaten:** Chat-Nachrichten, Benachrichtigungen
- **Dokumente und Uploads:** Personaldokumente, Abwesenheits-Anhänge — nur sofern vom Auftraggeber aktiviert
- **Audit-Logs und technische Protokolle**
- **Exportdaten** für Lohnvorbereitung und DATEV-Schnittstellen

§ 6 Besondere Kategorien personenbezogener Daten

(1) Je nach Konfiguration des Auftraggebers können besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO verarbeitet werden. Dies betrifft insbesondere krankheitsbezogene Abwesenheitstypen, mutterschutz- und elternzeitbezogene Angaben sowie hochgeladene Nachweise.

(2) Die Auftragnehmerin verarbeitet diese Datenkategorien ausschließlich nach Weisung des Auftraggebers. Der Auftraggeber ist für die Rechtmäßigkeit, Erforderlichkeit, Verhältnismäßigkeit sowie die Zugriffsbeschränkung im eigenen Verantwortungsbereich zuständig. Shiftdesk sieht produktseitig vor, dass Krankheits-Notizen und -Anhänge nur Owner- und HR-Rollen ausgespielt werden; der Auftraggeber ist für die organisatorische Umsetzung dieser Beschränkung in seiner Organisation verantwortlich.

§ 7 Weisungen

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit sie nicht durch das Recht der Union oder der Mitgliedstaaten zu einer abweichenden Verarbeitung verpflichtet ist; in diesem Fall teilt die Auftragnehmerin dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht ausschließt.

(2) Weisungen ergeben sich insbesondere aus dem Hauptvertrag, den AGB, diesem AVV sowie aus den Konfigurationen des Auftraggebers innerhalb der Anwendung (z. B. Aktivierung der GPS-Erfassung pro Standort, Aktivierung von Dokument-Uploads, Rollen- und Berechtigungsvergabe).

(3) Einzelweisungen können in Textform an support@shiftdesk.app erteilt werden. Erscheint eine Weisung der Auftragnehmerin als rechtswidrig, hat sie den Auftraggeber unverzüglich darauf hinzuweisen.

§ 8 Pflichten des Auftraggebers

Der Auftraggeber bleibt Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Er ist insbesondere verantwortlich für:

- Rechtmäßigkeit der Verarbeitung im Beschäftigungsverhältnis
- Information der betroffenen Personen nach Art. 13 / 14 DSGVO
- Rechtsgrundlagen für sensible Verarbeitungen (Art. 9 DSGVO, § 26 BDSG)
- Beteiligung eines Betriebsrats bzw. Personalrats, soweit nach BetrVG, BPersVG oder Landespersonalvertretungsrecht erforderlich (insbesondere § 87 Abs. 1 Nr. 6 BetrVG bei Standorterfassung)
- Rollen- und Berechtigungskonzept innerhalb seiner Organisation
- Prüfung der Erforderlichkeit und Verhältnismäßigkeit der GPS-Erfassung, der Dokument-Uploads und sonstiger sensibler Funktionen, bevor diese aktiviert werden

- Lösch- und Aufbewahrungsentscheidungen unter Berücksichtigung gesetzlicher Aufbewahrungsfristen

§ 9 Pflichten der Auftragnehmerin

Die Auftragnehmerin verpflichtet sich insbesondere:

- Daten nur nach dokumentierter Weisung des Auftraggebers zu verarbeiten (§ 7)
- Mitarbeitende, die Zugriff auf personenbezogene Daten haben, auf Vertraulichkeit zu verpflichten (Art. 28 Abs. 3 lit. b DSGVO)
- Angemessene technische und organisatorische Maßnahmen zu ergreifen (siehe Anlage 2)
- Den Auftraggeber bei der Beantwortung von Anträgen betroffener Personen, bei Datenschutz-Folgenabschätzungen und bei der Bearbeitung von Datenschutzverletzungen zu unterstützen
- Subprozessoren ausschließlich nach Maßgabe von § 10 einzusetzen
- Datenschutzverletzungen unverzüglich zu melden (§ 13)

§ 10 Subprozessoren und Änderungs-Logik

(1) Die Auftragnehmerin darf zur Erbringung der vertraglich geschuldeten Leistungen Subprozessoren einsetzen. Eine abschließende Aufstellung der eingesetzten Subprozessoren findet sich in Anlage 3.

(2) Mit jedem Subprozessor wird ein Vertrag geschlossen, der den Anforderungen von Art. 28 DSGVO entspricht oder — bei Anbietern, die als eigene Verantwortliche oder ausschließlich technische Drittanbieter (siehe Anlage 3) handeln — ein gleichwertiges Schutzniveau gewährleistet.

(3) **Geplante Änderungen** (Hinzufügen oder Austausch eines Subprozessors, Änderung des Verarbeitungs-Sitzes oder der Rolle) werden dem Auftraggeber spätestens **30 Tage** vor Wirksamwerden in Textform mitgeteilt. Die Mitteilung erfolgt per E-Mail an die im Account hinterlegte primäre Kontaktadresse sowie zusätzlich als Banner im Administrations-Dashboard.

(4) **Widerspruchsrecht.** Der Auftraggeber kann der geplanten Änderung innerhalb von **14 Tagen** nach Zugang der Mitteilung aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Bei wirksamem Widerspruch wird der Vertrag mit dem bisherigen Subprozessor fortgeführt, soweit dies technisch und wirtschaftlich zumutbar ist. Andernfalls steht dem Auftraggeber ein Sonderkündigungsrecht zum geplanten Zeitpunkt des Wirksamwerdens der Änderung zu.

(5) **Notfall-Wechsel.** Bei einem Sicherheitsvorfall beim bisherigen Subprozessor, dessen Insolvenz oder einem anderen objektiv zwingenden Grund kann die Auftragnehmerin den Subprozessor ohne Einhaltung der 30-Tage-Frist wechseln. Die Information des Auftraggebers erfolgt in diesem Fall unverzüglich, spätestens jedoch innerhalb von 7 Tagen.

§ 11 Drittlandtransfers

Drittlandtransfers erfolgen nur, wenn die Anforderungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere durch Angemessenheitsbeschluss (Art. 45 DSGVO) — etwa unter dem EU-US Data Privacy Framework — oder durch geeignete Garantien (Art. 46 DSGVO), insbesondere Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914. Die konkreten Grundlagen je Subprozessor sind in Anlage 3 ausgewiesen.

§ 12 Löschung und Rückgabe nach Vertragsende

(1) Nach Beendigung des Hauptvertrags stellt die Auftragnehmerin dem Auftraggeber für die Dauer von **30 Tagen** eine Exportmöglichkeit zur Verfügung, über die der Auftraggeber alle eigenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format herunterladen kann.

(2) Nach Ablauf dieser Frist löscht die Auftragnehmerin sämtliche personenbezogenen Daten des Auftraggebers, einschließlich der Daten in Backups spätestens 35 Tage nach Ablauf der Exportfrist. Ausgenommen sind ausschließlich Daten, deren Aufbewahrung einer eigenen gesetzlichen Pflicht der Auftragnehmerin unterliegt (insbesondere Rechnungs- und Buchungsbelege nach § 257 HGB, § 147 AO sowie Nachweise über die Bearbeitung von Löschanfragen); diese Daten werden für jede weitere Verarbeitung gesperrt.

(3) Der Auftraggeber ist verpflichtet, Daten, die er aufgrund eigener gesetzlicher Pflichten aufbewahren muss (z. B. § 16 Abs. 2 ArbZG, § 41 Abs. 1 EStG, § 28f SGB IV), vor Ablauf der Exportfrist über die bereitgestellten Exportfunktionen zu sichern. Auf gesonderte, dokumentierte Weisung des Auftraggebers in Textform kann die Auftragnehmerin Daten über die Exportfrist hinaus für einen vereinbarten Zeitraum gesperrt aufbewahren; in diesem Fall gilt die Weisung als Verarbeitungsgrundlage im Sinne von Art. 28 Abs. 3 lit. a DSGVO.

§ 13 Datenschutzverletzungen

Die Auftragnehmerin meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Kenntnis, spätestens jedoch innerhalb von 24 Stunden. Die Meldung enthält — soweit verfügbar — die Art der Verletzung, die betroffenen Datenkategorien, die ungefähre Anzahl betroffener Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen zur Eindämmung.

§ 14 Nachweise und Audit

(1) Die Auftragnehmerin stellt dem Auftraggeber auf Anfrage angemessene Informationen zum Nachweis der Einhaltung dieses AVV zur Verfügung. Geeignete Nachweise sind insbesondere Selbstauskünfte, anerkannte Zertifizierungen sowie Berichte über Sicherheits-Audits.

(2) Vor-Ort-Audits erfolgen in der Regel bei berechtigtem Anlass, mit angemessener Vorankündigung von in der Regel mindestens 30 Tagen und unter Wahrung von Betriebs- und Sicherheitsinteressen

sowie der Vertraulichkeit gegenüber anderen Kunden. Die Auftragnehmerin kann verlangen, dass das Audit durch einen zur Verschwiegenheit verpflichteten Dritten durchgeführt wird.

(3) Für Audits und Unterstützungsleistungen, die über das zur Erfüllung der gesetzlichen Pflichten der Auftragnehmerin erforderliche Maß hinausgehen, kann die Auftragnehmerin einen angemessenen Aufwandsersatz verlangen.

§ 15 Haftung, Schlussbestimmungen

(1) Für die Haftung der Parteien gilt § 10 der AGB. Im Innenverhältnis haften die Parteien einander nach Art. 82 Abs. 5 DSGVO entsprechend ihrem Anteil an der Verantwortung für den Schaden; die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

(2) Im Übrigen gelten der Hauptvertrag und die AGB. Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieses AVV für die Auftragsverarbeitung vor.

(3) Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden anstelle der unwirksamen Bestimmung eine wirksame Regelung vereinbaren, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung möglichst nahekommt.

(4) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts. Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist Bielefeld, soweit gesetzlich zulässig.

Anlage 1: Verarbeitungskategorien

Die nachfolgende Tabelle ordnet die im Dienst angelegten Funktionen den Verarbeitungs- und Zweckkategorien zu.

Funktion	Verarbeitungskategorie	Zweck
Dienstplanung	Erheben, Speichern, Strukturieren, Anzeigen, Ändern	Personalplanung, Schichtorganisation
Zeiterfassung (Web + Mobile)	Erheben, Speichern, Auswerten	Erfüllung der arbeitszeitrechtlichen Aufzeichnungspflicht (BAG 1 ABR 22/21)
Standorterfassung (optional, pro Standort aktivierbar)	Punktuelle Erhebung beim Stempelvorgang, keine Hintergrundortung	Plausibilisierung des Stempelorts
Abwesenheitsverwaltung	Erheben, Speichern, Genehmigung	Urlaubs- und Abwesenheitsverwaltung; krankheitsbezogene Abwesenheiten als Art. 9 DSGVO
Teamkommunikation (Chat, Push)	Übermittlung, Speichern	Operative Kommunikation
Dokumenten-Uploads (optional)	Speichern, Anzeigen, Löschen	Personaldokumente, Abwesenheits-Nachweise
Audit-Logs	Speichern, Anzeigen	Nachvollziehbarkeit, Fälschungssicherheit

Funktion	Verarbeitungskategorie	Zweck
Lohnvorbereitung / DATEV-Export	Erheben, Aggregieren, Exportieren	Technische Vorbereitung der Lohnabrechnung durch den Auftraggeber, Steuerberater oder das Lohnbüro
Support	Erheben, Speichern, Anzeigen	Bearbeitung von Support-Anfragen

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

Die Auftragnehmerin trifft die nachfolgenden technischen und organisatorischen Maßnahmen zur Sicherstellung eines dem Risiko angemessenen Schutzniveaus (Art. 32 DSGVO).

Zutrittskontrolle

Die produktive Verarbeitung personenbezogener Daten erfolgt in Rechenzentren der eingesetzten Subprozessoren (siehe Anlage 3). Diese gewährleisten Standard-Zutrittskontrollen (Vereinzelung, Schließanlagen, Videoüberwachung, Sicherheitspersonal).

Zugangskontrolle

Authentifizierung über Supabase Auth mit Passwort-Hashing (bcrypt), optional Mehr-Faktor-Authentisierung (TOTP). Service-Role-Zugänge werden über umgebungsspezifische Secrets verwaltet und nicht im Quellcode gehalten.

Zugriffskontrolle

Rollenbasiertes Berechtigungskonzept (Owner, HR, Standortleitung, Teamleitung, Beschäftigte) mit serverseitigen Permissionprüfungen für geschützte Funktionen und Datenzugriffe. Mandantentrennung erfolgt auf Tenant-ID-Ebene und wird in produktiven Datenzugriffen umgesetzt.

Weitergabekontrolle

Datenübertragungen erfolgen verschlüsselt über TLS 1.2 oder höher. Datenübergaben an Subprozessoren auf Grundlage dokumentierter AVV bzw. gleichwertiger Vereinbarungen (siehe Anlage 3). Exporte (z. B. DATEV) werden auf Anforderung des Auftraggebers erzeugt und vom autorisierten Nutzer heruntergeladen.

Eingabekontrolle

Alle sicherheitsrelevanten Vorgänge (Login, Änderungen an Zeitbuchungen, Genehmigungen, Exporte, Konfigurationsänderungen, Aktivierung der GPS-Erfassung) werden im Audit-Log mit Zeitstempel und Nutzerreferenz erfasst.

Auftragskontrolle

Subprozessoren werden ausschließlich auf Grundlage dokumentierter Verträge eingesetzt; siehe § 10 und Anlage 3.

Verfügbarkeitskontrolle

Tägliche automatisierte Backups durch den Datenbank- Subprozessor mit definiertem Recovery Point Objective. Wiederherstellungsverfahren werden mindestens jährlich getestet.

Trennungskontrolle

Logische Mandantentrennung über Tenant-ID-Filter, der in produktiven Datenzugriffen angewendet wird. Materielle Trennung von Produktiv-, Staging- und Entwicklungsumgebung.

Verschlüsselung

Verschlüsselung in Transit (TLS 1.2+) sowie at rest (AES-256 für Datenbank, Storage und Backups durch die eingesetzten Subprozessoren). Auf den mobilen Endgeräten werden Authentifizierungs-Tokens im plattformeigenen verschlüsselten Schlüsselspeicher (iOS Keychain bzw. Android EncryptedSharedPreferences) abgelegt.

Backup und Wiederherstellung

Tägliche Snapshots, Point-in-Time-Recovery durch den Datenbank-Subprozessor, getrennte Aufbewahrung der Backups.

Rollen- und Berechtigungskonzept

Fünf vordefinierte Rollen (Owner, HR, Standortleitung, Teamleitung, Beschäftigte) mit dokumentiertem Permission-Mapping. Zugriff auf krankheitsbezogene Notizen, Abwesenheits-Anhänge und Personaldokumente ist auf Owner und HR beschränkt.

Logging und Monitoring

Anwendungs- und Sicherheits-Logs mit angemessener Aufbewahrungsfrist; Anomalie-Monitoring.

Incident Response

Definierte Ablauforganisation für Sicherheitsvorfälle inklusive 24-Stunden-Meldepflicht an den Auftraggeber gemäß § 13.

Patch- und Vulnerability-Management

Regelmäßige Aktualisierung der eingesetzten Komponenten einschließlich automatisierter Dependency-Scans und Reaktion auf bekannte Sicherheitslücken nach risikobasiertem Schweregrad.

Löschkonzept

Differenzierte Löschfristen je Datenkategorie (siehe Datenschutzerklärung Abschnitt 8). Nutzer- und Organisationslöschungen werden über einen geprüften Löschanforderungs-Prozess durchgeführt (siehe `/account-loeschung`).

Subprozessorenmanagement

Verwaltung der Subprozessoren-Liste (Anlage 3) mit regelmäßiger Risiko-Bewertung und Vertragsmonitoring.

Mobile-App-Sicherheit

Verschlüsselte lokale Token-Speicherung (Keychain / EncryptedSharedPreferences). Keine Hintergrund-Standorterfassung. Native Permissions ausschließlich „when-in-use". Keine Drittanbieter-Analytics-SDKs in den mobilen Apps.

Anlage 3: Subprozessoren

Die nachfolgende Aufstellung enthält alle Anbieter, die Daten des Auftraggebers verarbeiten oder technisch übermitteln. Sie wird aus derselben technischen Quelle generiert wie die vollständige Dienstleister-Liste in Abschnitt 6 der Datenschutzerklärung; dort sind zusätzlich Dienste aufgeführt, die ausschließlich eigene Verarbeitungen der Auftragnehmerin betreffen (z. B. Abonnement-Abrechnung, Newsletter, Website-Reichweitenmessung) und daher keine Subprozessoren dieses AVV sind. Änderungen werden gemäß § 10 vorab kommuniziert.

Abgrenzung: Subprozessoren im Sinne von § 10 dieses AVV sind die mit der Rolle „Auftragsverarbeiter (Art. 28 DSGVO)" gekennzeichneten Anbieter. Anbieter mit der Rolle „Technischer Drittanbieter" übermitteln Daten lediglich als Teil der Plattform-Infrastruktur (z. B. Push-Token-Routing, einmaliges Adress-Geocoding); sie sind aus Transparenzgründen mit aufgeführt.

Dienst	Anbieter	Rolle	Sitz / Region	Zweck und Datenkategorien	Übern
Hosting (Frontend, Edge, Web Analytics)	Vercel Inc.	Auftragsverarbeiter (Art. 28 DSGVO)	USA (Unternehmenssitz); Hosting Frankfurt (Region fra1)	Bereitstellung der Website und Webanwendung; einwilligungsbasierte Reichweitenmessung via Vercel Web Analytics *Daten: IP-Adresse, User-Agent, Request-Pfad, Performance-Metriken; bei Analytics zusätzlich Aggregate-Statistiken*	EU-US Frame DPF-z

Dienst	Anbieter	Rolle	Sitz / Region	Zweck und Datenkategorien	Übern
Datenbank, Auth und Storage	Supabase Inc.	Auftragsverarbeiter (Art. 28 DSGVO)	USA (Unternehmenssitz); Hosting EU (Frankfurt)	Persistenz aller Anwendungsdaten, Authentifizierung, Storage für Personaldokumente und Chat-Anhänge *Daten: Sämtliche im Dienst erfassten personenbezogenen Daten gemäß Abschnitt 5*	Stand gemäl DSGV Modul Adder und S Regio
Transaktions-E-Mail	Resend, Inc.	Auftragsverarbeiter (Art. 28 DSGVO)	USA	Versand transaktionaler E-Mails (Account-Verifikation, Stripe-Belege, Schicht-Benachrichtigungen, Lösch-Bestätigungen) *Daten: E-Mail-Adresse, Anrede, transaktionsspezifischer Inhalt*	Stand gemäl DSGV
CDN, WAF und DDoS-Schutz	Cloudflare, Inc.	Auftragsverarbeiter (Art. 28 DSGVO)	USA (Unternehmenssitz); Edge-Server weltweit	Performance-Beschleunigung, Web Application Firewall, DDoS-Schutz *Daten: IP-Adresse, User-Agent, Request-Metadaten*	EU-US Frame ist DP
Push-Benachrichtigungs-Relay (Mobile)	Expo Application Services, Inc.	Auftragsverarbeiter (Art. 28 DSGVO)	USA	Routing der Push-Benachrichtigungen von der Shiftdesk-Anwendung zu den Plattform-Push-Diensten APNs (iOS) und FCM (Android) *Daten: Geräte-Token, Push-Inhalt (operative Schicht-/Nachrichten-Hinweise, ohne Gesundheitsdaten)*	Stand gemäl DSGV
Error-Tracking	Sentry GmbH (EU-Region) / Functional Software, Inc.	Auftragsverarbeiter (Art. 28 DSGVO)	EU (Frankfurt) bei aktivierter EU-Region	Fehlerdiagnose und Stacktrace-Sammlung zur Stabilisierung der Anwendung. Erfasst werden Fehler-Stacktraces, anonymisierte Browser-/Geräte-Daten und eine pseudonyme User-ID (keine Mail-Adresse, kein Name). IP-Adressen werden vor der Speicherung anonymisiert; Auth-Tokens und Mail-Adressen in Stacktraces	EU-Re EU-Wi Konze USA v Privac Stand gemäl DSGV Art. 6 (berec Anwe

Dienst	Anbieter	Rolle	Sitz / Region	Zweck und Datenkategorien	Übern
				werden serverseitig redactiert. Kein Session-Replay aktiv. *Daten: Fehler-Stacktraces, anonymisierte technische Geräte-/Browser-Daten, pseudonyme User-ID, Tenant-ID, Rolle*	
Push-Notification-Service iOS	Apple Inc.	Technischer Drittanbieter	USA	Apple stellt die plattformseitige Push-Infrastruktur (Apple Push Notification service) bereit und verarbeitet hierfür insbesondere Geräte-Token und technische Zustellinformationen. Die Push-Inhalte werden durch Shiftdesk so gestaltet, dass keine Gesundheitsdaten oder sonstigen besonders sensiblen Inhalte enthalten sind. *Daten: APNs-Device-Token, Push-Payload (operative Hinweise) Funktion: Push-Token-Routing*	EU-US Frame DPF-z
Push-Notification-Service Android	Google LLC (Firebase Cloud Messaging)	Technischer Drittanbieter	USA	Google stellt die plattformseitige Push-Infrastruktur (Firebase Cloud Messaging) bereit und verarbeitet hierfür insbesondere Geräte-Token, eine Installations-ID und technische Zustellinformationen. Die Push-Inhalte werden durch Shiftdesk so gestaltet, dass keine Gesundheitsdaten oder sonstigen besonders sensiblen Inhalte enthalten sind. *Daten: FCM-Token, Firebase Installation ID, Push-Payload (operative Hinweise) Funktion: Push-Token-Routing*	EU-US Frame DPF-z
Adress-Geocoding (Standort-Aktivierung	OpenStreetMap Foundation	Technischer Drittanbieter	Vereinigtes Königreich	Wenn der Kunde beim Aktivieren der Standortprüfung das	Anger der EU

Dienst	Anbieter	Rolle	Sitz / Region	Zweck und Datenkategorien	Übern
Compliance-Modal)	(Nominatim-Dienst)			automatische Geocoding nutzt, wird die Stamm-Adresse einer Filiale (Straße, Postleitzahl, Stadt, Land) einmalig an Nominatim übermittelt, um daraus geographische Koordinaten (Breiten- / Längengrad) zu ermitteln. Es werden keine Personendaten von Beschäftigten übermittelt; die Adresse selbst ist nicht personenbezogen. Das Ergebnis wird im Datenbestand des Kunden gespeichert und nicht erneut übertragen. *Daten: Adresse einer Filiale (Straße, PLZ, Stadt, Land)* *Funktion: einmaliges Adress-Geocoding (kein Token-Routing)*	28.06. Verein

Zuletzt aktualisiert: 12. Juni 2026