

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

FacilityDesk · Version 1.7 · Stand 23.10.2026

Vertrag nach Art. 28 DSGVO. Er wird vor der ersten Eingabe personenbezogener Daten mit jedem Kunden abgeschlossen – auch in der Testphase. Für den Abschluss schreiben Sie an kontakt@facility-desk.de.

Dieser Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO wird vor der ersten Eingabe personenbezogener Daten zwischen dem Kunden (Verantwortlicher) und dem Anbieter (Auftragsverarbeiter) abgeschlossen. Anlagen 2 und 3 beschreiben den tatsächlichen technischen Stand einschließlich bestehender Einschränkungen.

zwischen

Kunde (Name, Anschrift laut Auftragsbestätigung oder Registrierung) – nachfolgend „Verantwortlicher“ –

und

Eduard Wiebe (FacilityDesk), Achenbacher Straße 5, 35236 Breidenbach (Ortsteil Oberdieten), Deutschland, kontakt@facility-desk.de – nachfolgend „Auftragsverarbeiter“.

1. Gegenstand, Dauer und Verhältnis zum Hauptvertrag

1.1 Der Auftragsverarbeiter stellt dem Verantwortlichen die Software FacilityDesk als Online-Dienst bereit (Hauptvertrag: AGB, Leistungsbeschreibung, Auftragsbestätigung). Dabei verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Gegenstand, Art und Zweck der Verarbeitung, Datenarten und betroffene Personen beschreibt Anlage 1.

1.2 Dieser Vertrag gilt ab Unterzeichnung bzw. elektronischer Annahme, auch für kostenlose Testzugänge, und endet, wenn alle Daten nach Ziffer 11 zurückgegeben und gelöscht sind.

1.3 Bei Widersprüchen geht dieser Vertrag in Datenschutzfragen dem Hauptvertrag vor.

2. Weisungen

2.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch bei Übermittlungen in Drittländer –, es sei denn, er ist durch Unionsrecht oder deutsches Recht zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

2.2 Die Weisungen sind mit diesem Vertrag und dem Hauptvertrag sowie durch die Nutzung und Konfiguration der Anwendung durch berechtigte Nutzer des Verantwortlichen erteilt (zum Beispiel Anlegen, Ändern, Exportieren und Löschen von Daten). Weitere Weisungen erteilt der Verantwortliche in Textform an kontakt@facility-desk.de.

2.3 Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

2.4 Handelt der Verantwortliche seinerseits als Auftragsverarbeiter eines Dritten (zum Beispiel eines Eigentümers oder einer Wohnungseigentümergeinschaft), sichert er zu, dass die Beauftragung des Auftragsverarbeiters von den Weisungen und der Genehmigung dieses Dritten gedeckt ist (Art. 28 Abs. 2 und 4 DSGVO). Weisungen erteilt ausschließlich der Verantwortliche; der Auftragsverarbeiter nimmt Weisungen Dritter nicht entgegen und leitet sie an den Verantwortlichen weiter. Auf Anfrage weist der Verantwortliche die Genehmigung nach.

2.5 Meldungen, die über die Meldeseite oder an ticket@facility-desk.de eingehen, verarbeitet der Auftragsverarbeiter ausschließlich im Auftrag des Verantwortlichen, dem die Meldung anhand des QR-Codes, der Objektkennung oder der Adresse zugeordnet ist. Nicht zuordenbare Meldungen werden ohne inhaltliche Auswertung spätestens nach 14 Tagen gelöscht. Der Verantwortliche stellt die Informationen nach Art. 13 DSGVO gegenüber Meldern bereit; der Auftragsverarbeiter blendet auf der Meldeseite einen vom Verantwortlichen hinterlegten Datenschutzhinweis sowie die Hinweise ein, dass Gesundheitsdaten nur anzugeben sind, soweit erforderlich, und dass die Meldeseite kein Notruf ist.

2.6 Zugriff über Vertragsgrenzen hinweg. Der Auftragsverarbeiter gewährt Benutzerkonten eines anderen Kunden Zugriff auf Daten des Verantwortlichen nur, wenn der Verantwortliche dies nach Ziffer 5.10 der AGB in der Anwendung ausdrücklich freigegeben hat und der andere Kunde bestätigt hat. Die Freigabe ist eine dokumentierte Weisung im Sinne des Art. 28 Abs. 3 lit. a DSGVO und auf das freigegebene Benutzerkonto, die freigegebenen Objekte und den freigegebenen Rechteumfang beschränkt. Mit Widerruf oder Ende eines der beiden Verträge endet der Zugriff. Der Verantwortliche bleibt für seine Daten verantwortlich und prüft die Rechtsgrundlage der Offenlegung gegenüber dem anderen Kunden. Erteilung, Änderung und Widerruf werden protokolliert; das Protokoll ist für den Verantwortlichen einsehbar und Teil der Nachweise nach Ziffer 10.

2.7 ERP-Schnittstelle. Die Erzeugung eines API-Schlüssels und das Hinterlegen einer Benachrichtigungsadresse durch einen Administrator gelten als Weisung des Verantwortlichen, die betreffenden Daten an die so bestimmten Systeme zu übermitteln (Ziffer 6a.8 der AGB). Die vom Verantwortlichen bestimmten Systeme sind Empfänger auf seine Weisung, keine Unterauftragsverarbeiter des Auftragsverarbeiters. Das Zugriffsprotokoll führt der Auftragsverarbeiter auf Weisung des Verantwortlichen; die gekürzte IP-Adresse wird nach 90 Tagen entfernt, die übrigen Angaben werden nach 365 Tagen gelöscht.

3. Pflichten des Verantwortlichen

3.1 Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für Rechtsgrundlagen, Informationspflichten gegenüber Betroffenen (zum Beispiel Beschäftigte, Bewohner, Melder, Dienstleister), die Beteiligung von Betriebs- oder Personalrat und eine gegebenenfalls erforderliche Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

3.2 Für Beschäftigtendaten (zum Beispiel Zeiterfassung, optionale Standortprüfung) wählt der Verantwortliche eine tragfähige Rechtsgrundlage. Hinweis: Nach dem Urteil des EuGH vom 30.03.2023 (C-34/21) kann eine nationale Vorschrift wie § 26 Abs. 1 Satz 1 BDSG nur dann eigenständig herangezogen werden, wenn sie die Anforderungen des Art. 88 DSGVO erfüllt; in Betracht kommen daneben insbesondere Art. 6 Abs. 1 lit. b und c DSGVO sowie Kollektivvereinbarungen. Eine Einwilligung ist im Beschäftigungsverhältnis nur ausnahmsweise geeignet.

3.3 Besondere Kategorien personenbezogener Daten. Gesundheitsdaten und andere Daten nach Art. 9 DSGVO (zum Beispiel Pflege- oder Diagnoseangaben in Tickets, Fahrdienst-Notizen oder Fotos) darf der Verantwortliche nur eingeben oder eingeben lassen, wenn eine Ausnahme nach Art. 9 Abs. 2 DSGVO (gegebenenfalls in Verbindung mit § 22 BDSG) besteht und die Angabe für den Zweck erforderlich ist. Der Verantwortliche weist seine Nutzer an, solche Angaben nicht in Freitexte aufzunehmen, soweit dies vermeidbar ist – zum Beispiel „Fahrt zur Arztpraxis“ statt Diagnose oder Behandlungsgrund. Ergänzende Schutzmaßnahmen nennt Anlage 2 Abschnitt 6.

3.4 Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt, und benennt eine Kontaktperson für Datenschutzfragen.

4. Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3

lit. b, Art. 29, Art. 32 Abs. 4 DSGVO). Derzeit verarbeitet ausschließlich der Auftragsverarbeiter selbst die Daten; werden Personen hinzugezogen, werden sie vorab schriftlich verpflichtet.

5. Sicherheit der Verarbeitung

5.1 Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 lit. c DSGVO).

5.2 Er darf die Maßnahmen weiterentwickeln, wenn das Schutzniveau nicht unterschritten wird, und dokumentiert wesentliche Änderungen. Auf Anfrage erhält der Verantwortliche die aktuelle Fassung von Anlage 2.

6. Unterauftragsverarbeiter

6.1 Der Verantwortliche erteilt eine allgemeine Genehmigung für den Einsatz weiterer Auftragsverarbeiter (Unterauftragsverarbeiter). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter nennt Anlage 3.

6.2 Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vorher in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eigener Unterauftragsverarbeiter. Änderungen bei weiteren Auftragsverarbeitern eines Unterauftragsverarbeiters (zum Beispiel des Hosters), die dem Auftragsverarbeiter mit kürzerem Vorlauf mitgeteilt werden, gibt er unverzüglich nach Kenntnis weiter. Der Verantwortliche kann innerhalb von 14 Tagen nach Zugang aus datenschutzrechtlich begründetem Anlass widersprechen. Einigen sich die Parteien nicht, kann der Verantwortliche den Hauptvertrag zum Zeitpunkt der Änderung kündigen; vorausbezahlte Entgelte werden anteilig erstattet.

6.3 Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für dessen Pflichterfüllung (Art. 28 Abs. 4 DSGVO). Satz 1 und 2 gelten auch für weitere Auftragsverarbeiter eines Unterauftragsverarbeiters, soweit der Auftragsverarbeiter dies vertraglich durchsetzen kann; die Haftung nach Art. 28 Abs. 4 Satz 2 DSGVO bleibt unberührt.

6.4 Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikations- und Postdienste oder die Zahlungsabwicklung, soweit dabei keine Kundendaten verarbeitet werden.

7. Drittlandübermittlung

Die Daten in der Anwendung werden in Deutschland gespeichert (Rechenzentrum Nürnberg, Deutschland, vom Betreiber bestätigt). Eine Übermittlung in ein Drittland findet nur statt, wenn Anlage 3 sie ausweist oder der Verantwortliche sie anweist und die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (zum Beispiel Angemessenheitsbeschluss oder Standardvertragsklauseln).

8. Unterstützung bei Betroffenenrechten

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte nach Art. 15 bis 22 DSGVO (Art. 28 Abs. 3 lit. e DSGVO). Die Anwendung ermöglicht dem Verantwortlichen insbesondere das Anzeigen, Berichten, Exportieren und Löschen von Daten.

8.2 Wendet sich eine betroffene Person an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst, außer der Verantwortliche weist ihn an.

9. Unterstützung bei Art. 32 bis 36 DSGVO und Meldung von Verletzungen

9.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei der Sicherheit der Verarbeitung, bei Meldungen und Benachrichtigungen nach Art. 33 und 34 DSGVO sowie bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 28 Abs. 3 lit. f DSGVO).

9.2 Meldung von Datenschutzverletzungen. Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten des Verantwortlichen bekannt, meldet er sie dem Verantwortlichen unverzüglich (Art. 33 Abs. 2 DSGVO) per E-Mail an die benannte Kontaktadresse; er strebt eine Erstmeldung innerhalb von 24 Stunden nach Kenntnis an. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO (Art der Verletzung, Kategorien und ungefähre Zahl betroffener Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen, Kontakt). Fehlende Angaben werden ohne unangemessene Verzögerung nachgereicht.

9.3 Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen nimmt der Verantwortliche vor; der Auftragsverarbeiter nimmt sie nur auf Weisung vor.

9.4 Für Unterstützungsleistungen, die nicht auf einer Pflichtverletzung des Auftragsverarbeiters beruhen und über die in der Anwendung verfügbaren Funktionen deutlich hinausgehen, kann eine angemessene Vergütung nach vorheriger Absprache vereinbart werden. Ohne eine solche vorherige Vereinbarung entsteht keine Vergütung.

10. Nachweise und Überprüfungen

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer (Art. 28 Abs. 3 lit. h DSGVO).

10.2 Überprüfungen erfolgen vorrangig durch Vorlage von Nachweisen (zum Beispiel dieser Unterlagen, Auskünfte in Textform, Prüfberichte oder Zertifikate). Eine Vor-Ort-Prüfung findet bei konkretem Anlass nach Terminabsprache statt; ihre Kosten trägt der Verantwortliche, soweit kein Verstoß des Auftragsverarbeiters festgestellt wird. Überprüfungen werden mit angemessenem Vorlauf (in der Regel 14 Tage) angekündigt und so durchgeführt, dass der Betrieb und die Daten anderer Kunden nicht beeinträchtigt werden. Für Rechenzentren von Unterauftragsverarbeitern kann der Nachweis über deren Prüfberichte oder Zertifikate geführt werden.

10.3 Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO).

11. Rückgabe und Löschung nach Vertragsende

11.1 Nach Ende der Leistungen wählt der Verantwortliche zwischen Rückgabe und Löschung (Art. 28 Abs. 3 lit. g DSGVO). Die Rückgabe erfolgt über den Export nach Anlage 1 der AGB, den Administratoren des Verantwortlichen selbst auslösen können.

11.2 Die Daten bleiben nach Vertragsende mindestens 30 Kalendertage abrufbar. Die Frist beginnt mit dem Vertragsende oder, wenn der Auftragsverarbeiter den Abruf erst später ermöglicht, mit der tatsächlichen Bereitstellung.

11.3 Nach Ablauf der Abruffrist löscht der Auftragsverarbeiter die Daten innerhalb von 14 Kalendertagen aus den produktiven Systemen, einschließlich Anhängen (Dokumente, Fotos, Unterschriften), erzeugter Protokolle und noch vorhandener Exportdateien. Eine frühere Löschung erfolgt auf ausdrückliche Weisung.

11.4 Kopien in Datensicherungen werden spätestens 90 Kalendertage nach der tatsächlichen Löschung aus den produktiven Systemen gelöscht oder überschrieben. Bis dahin sind sie gegen Nutzung gesperrt und dienen nur der Wiederherstellung. Nach einer Wiederherstellung prüft der Auftragsverarbeiter anhand einer Löschliste, dass bereits gelöschte Organisationen nicht wieder verfügbar werden, und setzt die Löschung erneut um.

11.5 Eine längere Speicherung erfolgt nur, soweit Unionsrecht oder deutsches Recht den Auftragsverarbeiter dazu verpflichtet. Eigene Vertrags- und Abrechnungsnachweise des Auftragsverarbeiters sind keine Daten des Verantwortlichen im Sinne dieses Vertrags.

11.6 Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung in Textform.

12. Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregeln des Hauptvertrags, soweit Art. 82 DSGVO nicht entgegensteht. Ansprüche des Verantwortlichen wegen Verletzung dieses Vertrags verjähren nach den gesetzlichen Vorschriften; Ziffer 13.6 der AGB findet insoweit keine Anwendung.

13. Schlussbestimmungen

13.1 Änderungen und Ergänzungen bedürfen der Textform. Dieser Vertrag kann elektronisch abgeschlossen werden (Art. 28 Abs. 9 DSGVO); der Auftragsverarbeiter dokumentiert Fassung, Zeitpunkt und annehmende Person.

13.2 Es gilt deutsches Recht. Für den Gerichtsstand gelten die gesetzlichen Vorschriften.

13.3 Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

13.4 Diese Fassung 1.7 gilt für Verträge, die ab dem 23.10.2026 geschlossen werden. Für zuvor geschlossene Verträge gilt sie, sobald der Verantwortliche ihr in Textform zugestimmt hat, auch durch gesondertes Ankreuzen bei der Buchung der ERP-Schnittstelle (Ziffer 6a.8 g der AGB); bis dahin gilt die bisher vereinbarte Fassung.

Für den Verantwortlichen | Für den Auftragsverarbeiter |

Ort, Datum:Name, Funktion:Unterschrift / elektronische Annahme: | Ort, Datum:Eduard WiebeUnterschrift / elektronische Annahme: |

Anlage 1 – Gegenstand, Art und Zweck, Datenarten, Betroffene

Zweck: Bereitstellung von FacilityDesk zur Organisation, Dokumentation und Verwaltung des Gebäudebetriebs des Verantwortlichen.

Art der Verarbeitung: Erheben und Speichern durch Nutzer des Verantwortlichen, Hosting, Anzeigen, Ordnen, Auswerten, Erzeugen von PDF-Dokumenten, Versand von Benachrichtigungen, Abruf eingehender Ticket-E-Mails, Datensicherung, Export, Löschung.

Datenkategorie | Beispiele | Betroffene |

Nutzerkonten | Name, geschäftliche E-Mail, Rolle, Standortzuordnung, Abteilung, Arbeitszeitmodell, Passwort-Hash, Änderungsprotokoll (Aktion, Nutzerkennung, Zeitpunkt) | Beschäftigte, externe Nutzer |

Tickets und Meldungen | Beschreibungen, Kommentare, Zuweisungen, Status, Zeitstempel, Fotos; Meldungen per E-Mail und QR-Formular (Name, optional E-Mail) | Beschäftigte, Melder, ggf. abgebildete Personen |

Aufgaben, Routinen, Rundgänge | Zuständigkeiten, Checklisten, Prüfergebnisse, Zeitpunkte | Beschäftigte |

Spül-, Wartungs- und Leistungsnachweise | Protokolle, ausführende Person, Unterschrift, PDF | Beschäftigte, Dienstleister, Unterzeichner |

Kontakte und Dienstleister | Name, Firma, Telefon, E-Mail, Zuständigkeit, Notizen | Ansprechpartner, Dienstleister, Bewohner |

Schlüsselverwaltung | Schlüssel, Empfänger, Ausgabe und Rückgabe, Übergabeprotokoll, Unterschrift | Beschäftigte, Empfänger |

Unterschriften | Unterschriftsbild, Name, Zeitpunkt, Prüfsumme | Unterzeichner |

Zeiterfassung | Kommen/Gehen/Pausen, Korrekturen, Urlaub, Abwesenheiten mit Typ (z. B. „krank“, ohne Diagnose) und Notizen; optional Arbeitsbereich und Ergebnis der Standortprüfung (innerhalb/außerhalb, Entfernung, Zeitpunkt) | Beschäftigte |

Fuhrpark (Zusatzmodul) | Kennzeichen, Hersteller/Modell, Kilometerstände, Fahrzeugfotos, Notizen, verantwortliche Person, Termine (Inspektion, HU/TÜV, Reifenwechsel), Pflege- und Terminprotokolle mit Checkliste, Datum, Uhrzeit, Name und Unterschrift | Beschäftigte (Fahrer, Verantwortliche, Unterzeichner) |

ERP-Schnittstelle (Zusatzmodul) | Lesende Übermittlung von Tickets, Aufgaben, Leistungsnachweisen, Zeiterfassung (mit Benutzerkennung und Personalnummer), Objekten und Abrechnungsbereichen an vom Verantwortlichen festgelegte Systeme (API-Abruf, signierte Benachrichtigungen an eine hinterlegte Adresse); API-Schlüssel nur als Prüfwert; Zugriffsprotokoll (Zeitpunkt, Vorgang, Schlüsselkennung bzw. handelnde Person, Ergebnis, gekürzte IP-Adresse), Entfernung der IP-Adresse nach 90 Tagen, Löschung nach 365 Tagen | Beschäftigte, Melder, Dienstleister, Ansprechpartner (je nach abgerufenen Daten) |

Kalender, Projekte, Fahrdienste | Termine, Fahrten (z. B. Arzt- oder Bewohnerfahrten) mit Start, Ziel, Zeit, Notizen | Beschäftigte, Bewohner/Fahrgäste |

Dokumente | hochgeladene Dateien (PDF, JPEG, PNG) | je nach Inhalt |

Vertrag | Organisation, Firmenname, Laufzeit, Vertragsnachweis (bestellende Person, Fassungen, Preis) | Ansprechpartner des Verantwortlichen |

Besondere Kategorien (Art. 9 DSGVO): Die Angabe des Abwesenheitstyps „krank“ ist auch ohne Diagnose als Gesundheitsdatum einzuordnen; ihre Verarbeitung stützt der Verantwortliche auf seine arbeitsrechtliche Grundlage (Art. 9 Abs. 2 lit. b DSGVO, § 26 Abs. 3 BDSG; zur Anwendbarkeit siehe Ziffer 3.2). Im Übrigen sind besondere Kategorien nicht vorgesehen und nicht erforderlich, können aber in Freitextfeldern (Ticket-Beschreibung und -Notizen, Aufgaben-Notizen, Fahrt-Start/-Ziel/-Notizen, Abwesenheits- und Urlaubsnotizen, QR-Meldungen, eingehende E-Mails, Prüfungs- und Kontrollgang-Bemerkungen), Fotos und Dokumenten anfallen. Eine technische Filterung findet nicht statt. Es gilt Ziffer 3.3 und Anlage 2 Abschnitt 6.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand 09.10.2026. Beschrieben ist der tatsächliche Stand laut technischer Faktenliste vom 09.10.2026, 17:10 Uhr (Live-System und Code); Einschränkungen sind offen benannt.

1. Vertraulichkeit

- Zutritt: Betrieb auf einem gemieteten virtuellen Server der netcup GmbH im Rechenzentrum Nürnberg, Deutschland (vom Betreiber bestätigt). Die physische Sicherheit verantwortet netcup nach dem Vertrag zur Auftragsverarbeitung vom 10.10.2026 (netcup „Auftragsverarbeitung für Kunden“, Version 7, Stand

2026/07), Anhang 1. Für den Standort Nürnberg sind dort unter anderem genannt: Alarmanlage, Chipkarten-/Transpondersysteme, Klingelanlage mit Kamera, Videoüberwachung, Schlüsselregelung, Ausweise und begleitete Besucher; für die Verfügbarkeit Brand- und Rauchmeldeanlagen, Klimatisierung, USV und Notstrom-Dieselaggregate, RAID/Festplattenspiegelung. netcup gibt dort Zertifizierungen nach ISO 9001, ISO/IEC 27001 und ISO/IEC 27701 an (Angabe von netcup; Zertifikate selbst nicht eingesehen).

- Zugang zum Server: nur per SSH-Schlüssel, kein Root-Login, ein einziger Benutzer (Auftragsverarbeiter); Firewall nur Ports 22, 80, 443; Datenbank und API nicht von außen erreichbar; fail2ban; automatische Sicherheitsupdates mit kontrollierten Neustarts.
- Gemeinsamer Server: Auf demselben virtuellen Server betreibt der Auftragsverarbeiter weitere eigene Anwendungen; diese sind technisch getrennt (eigene Webserver-Konfigurationen und Dienste, interne Ports nur lokal erreichbar).
- Zugang zur Anwendung: Passwörter nur als Argon2-Hash, Mindestlänge 10 Zeichen; Sitzungen höchstens 12 Stunden, Ablauf nach 8 Stunden Inaktivität; Cookies HttpOnly, Secure, SameSite; CSRF-Schutz; E-Mail-Bestätigung und Zugriffsbegrenzungen (Rate-Limits) bei Anmeldung, Einladung, Passwort-Zurücksetzen und öffentlichen Formularen; Begrenzung von Anmeldeversuchen auf drei Ebenen (Webserver höchstens 10 Anfragen pro Minute, Anwendung je Konto, fail2ban-Sperre der IP für 15 Minuten). Optionale Zwei-Faktor-Anmeldung mit Authenticator-App (TOTP, RFC 6238) für Administratoren; jeder Code ist nur einmal gültig.
- Zugriff: Rollen- und Rechtekonzept; Beschränkung von Nutzern auf Standorte; serverseitige Prüfung jeder Anfrage.
- Mandantentrennung: Zugriffe über Organisationsgrenzen nur auf Grundlage protokollierter, widerruflicher Freigaben nach Ziffer 2.6, beschränkt auf freigegebene Benutzerkonten, Objekte und Rechte und serverseitig bei jeder Anfrage geprüft; logische Trennung in gemeinsamer Datenbank und gemeinsamem Dateiverzeichnis; alle Abfragen auf die Organisation des angemeldeten Nutzers beschränkt; Dateien nur über die Anwendung mit Berechtigungsprüfung; automatisierte Tests mit zwei Mandanten, auch für den Export; täglicher Prüflauf auf einer Datenbankkopie auf mandantenfremde Verweise.
- Endgeräte: Beim Abmelden und beim Organisationswechsel löscht die App automatisch die lokal gespeicherten Inhaltsdaten (IndexedDB-Offline-Daten, Unterschriftsbilder und Zwischenstände im localStorage, Daten-Caches, organisationsbezogene Speicher). Nicht übertragene Offline-Einträge werden nicht unbemerkt verworfen (Warnung, Angebot zur Übertragung, Verwerfen nur nach gesonderter Bestätigung). Der Service-Worker-Cache enthält nur App-Dateien, keine Inhaltsdaten. Diese Löschung ist seit dem 09.10.2026 in Betrieb (App-Stand 1c6cee0). Die Offline-Arbeit für alle Arbeitsfunktionen mit automatischer Synchronisierung ist seit dem 10.10.2026 in Betrieb.
- Minimierung: Entfernen von Foto-Metadaten (EXIF) bei öffentlichen Meldungen; Tokens nur als Hash; Standortkoordinaten der Standortprüfung werden nicht gespeichert.
- ERP-Schnittstelle (Zusatzmodul): nur lesender Zugriff auf Daten der eigenen Organisation, keine freigegebenen Fremddaten; API-Schlüssel nur als Hash gespeichert, einmalige Anzeige, Widerruf jederzeit; höchstens 600 Abrufe je Minute und Schlüssel; signierte Benachrichtigungen; nur ergänzbares Zugriffsprotokoll, IP-Adressen gekürzt (IPv4 /24, IPv6 /48) und nach 90 Tagen entfernt, automatische Löschung nach 365 Tagen.

2. Integrität

- Übertragung: ausschließlich verschlüsselt (TLS 1.2/1.3, HSTS); E-Mail-Versand mit Transportverschlüsselung; Absenderdomain mit SPF, DKIM und DMARC.
- Eingabekontrolle: Änderungsprotokoll (Anmeldung, Änderungen, Exporte) mit Nutzerkennung und Zeitpunkt; E-Mail-Adressen darin gekürzt. Einschränkung: noch keine automatische Löschfrist; vorgesehen sind 24 Monate.
- Ausgehende E-Mails: Versand über den Mailserver von netcup; Bestätigungs-, Passwort- und Begrüßungsmails nur mit festen Texten an die angegebene Adresse (höchstens 5 je Empfänger und Stunde), alle übrigen Mails nur an freigegebene Empfänger; insgesamt höchstens 60 Mails pro Stunde.
- Vertragsnachweis: nur ergänzbares Protokoll mit Hash-Kette; Änderungen und Löschungen werden von der Datenbank abgewiesen; tägliche Prüfung.
- Uploads: nur PDF, JPEG, PNG bis 10 MB; Prüfung der Dateisignatur; Schutz vor Pfadmanipulation.
- Unterschriften und Exporte: Prüfsummen (SHA-256) zur Erkennung nachträglicher Veränderung.
- Härtung: Sicherheits-Header, API-Dokumentation im Produktivbetrieb abgeschaltet, Dienst mit eingeschränkten Rechten (systemd-Sandboxing).

3. Verfügbarkeit und Belastbarkeit

- Datensicherung: täglich (Datenbank, Dateien, Konfiguration) mit Integritätsprüfung; alle drei werden mit GPG verschlüsselt, der private Schlüssel liegt nur beim Auftragsverarbeiter, nicht auf dem Server; Rotation 14 tägliche und 8 wöchentliche Stände (ältester Stand etwa 62 Tage).
- Einschränkungen (Stand 11.10.2026): Die Datenbank auf dem Server selbst ist nicht verschlüsselt (Schutz über Dateirechte und Zugangsbeschränkung); Sicherungen liegen bei netcup, eine Kopie an einem zweiten, räumlich getrennten Ort besteht derzeit nicht; 88 ältere manuelle und 6 automatische Datenbankkopien liegen unverschlüsselt im Sicherungsverzeichnis (nur Zugriff des Auftragsverarbeiters); die automatischen laufen mit der Rotation aus, die manuellen werden nach erfolgreichem Wiederherstellungstest bereinigt; Export-Archive liegen bis zu 7 Tage auf dem Server und werden dann automatisch entfernt; Ein-Server-Betrieb ohne Ausfallredundanz; keine zugesagte Wiederherstellungszeit.
- Überwachung: Watchdog mit automatischem Neustart; tägliche Sicherheitsprüfung mit Ampel-Bericht per E-Mail, Alarm bei kritischem Ergebnis und bei Sicherheitsfehlern; tägliche Schwachstellenprüfung der eingesetzten Softwarepakete.
- Externe Verfügbarkeitsüberwachung: stündliche Prüfung der Erreichbarkeit von außerhalb des Servers (Website, Health-Adresse, Gültigkeit des Zertifikats), ausschließlich über öffentliche Adressen und ohne personenbezogene Daten; Alarm an den Auftragsverarbeiter bei zwei aufeinanderfolgenden Fehlschlägen (seit 09.10.2026).
- Notfall: Wartungsmodus und Beweissicherung vorbereitet; Wiederherstellung nur über ein Freigabeverfahren, das bereits gelöschte Mandanten nicht wiederherstellt (Löschliste).
- Protokolle: Webzugriffe und Systemprotokolle 30 Tage (Systemprotokoll höchstens 500 MB).

4. Verfahren zur regelmäßigen Überprüfung

- Automatisierte Tests (unter anderem Mandantentrennung, Export, Fristberechnung), versionierte Änderungen, Sicherung vor Eingriffen.

- Tägliche automatisierte Prüfung der Sicherung (Vollständigkeit, Integrität, Empfängerschlüssel, Prüfsummen). Ein vollständiger Wiederherstellungstest auf einem getrennten Gerät ist vorgesehen; sein Ergebnis wird dokumentiert.
- Jährliche Überprüfung dieser Anlage und der Unterauftragsverarbeiter.

5. Organisation

- Verfahren für Datenschutz- und Sicherheitsvorfälle mit Meldewegen und Vorlagen.
- Lösch- und Aufbewahrungskonzept (30/14/90 Tage, Löschliste nach Wiederherstellung). Einschränkung: Die produktive Löschung ist technisch vorbereitet, aber noch nicht aktiviert; bis dahin wird manuell nach dem Konzept gelöscht.
- Zugriff auf Kundeninhalte zu Supportzwecken nur im erforderlichen Umfang und dokumentiert.

6. Zusätzliche Maßnahmen für besondere Kategorien (Art. 9 DSGVO)

- Hinweis an Nutzer, keine Gesundheitsangaben in Freitexte und Meldungen aufzunehmen (derzeit im öffentlichen Meldeformular; Hinweise an weiteren Freitextfeldern sind vorgesehen).
- Zugriff über Rollen und Standortbeschränkung auf erforderliche Personen begrenzen (Konfiguration durch den Verantwortlichen).
- Kein Einsatz von Analyse- oder Werbediensten; keine Verwendung von Kundeninhalten zum KI-Training.
- Empfehlung an den Verantwortlichen: Fahrdienste ohne Diagnose oder Behandlungsgrund erfassen; regelmäßige Löschung nicht mehr benötigter Fahrdienst- und Ticketinhalte.
- Zwei-Faktor-Anmeldung ist verfügbar. Der Verantwortliche aktiviert sie für Konten mit der Rolle Administrator (AGB Ziffer 9.1); für übrige Nutzer entscheidet er über die Aktivierung (Art. 32 DSGVO).

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter | Leistung | Ort der Verarbeitung | Grundlage / Status |

netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Deutschland | Hosting (virtueller Server): Speicherung aller Anwendungsdaten und Sicherungen | Rechenzentrum Nürnberg, Deutschland (vom Betreiber bestätigt) | Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO geschlossen am 10.10.2026 (Vertragsfassung von netcup, Version 7, Stand 2026/07), Gesundheitsdaten als besondere Kategorie angegeben. Weitere Auftragsverarbeiter von netcup: Anexia Holding GmbH (Klagenfurt, Österreich; Unterstützungsleistungen, z. B. Abrechnung, regulatorische Anfragen) und Anexia Cloud Solutions GmbH (Klagenfurt, Österreich, und Karlsruhe, Deutschland; Infrastrukturleistungen im Rechenzentrumsumfeld, Personal). Kein Drittland. Colocation-Rechenzentrumsbetreiber werden von netcup als bloße Infrastruktur-Nebenleistung und nicht als weitere Auftragsverarbeiter eingeordnet. |

netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Deutschland | E-Mail: Mailserver (Webhosting) für den Versand aller System-E-Mails (SMTP, Absender noreply@facility-desk.de) und für die Postfächer unter facility-desk.de einschließlich des Ticket-Postfachs ticket@facility-desk.de (IMAP-Abruf) | Deutschland | Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO vom 10.10.2026 (gilt für alle bestehenden und künftigen Verträge mit netcup) |

OpenStreetMap Foundation, St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, Vereinigtes Königreich | Geokodierung (Dienst Nominatim): Umrechnung der Adresse eines Objekts oder Dienstleisters in Koordinaten; Abfrage durch den Server, ohne IP-Adresse oder weitere Angaben zu Nutzern; Ergebnisse werden auf dem Server zwischengespeichert | Vereinigtes Königreich | Angemessenheitsbeschluss der EU-Kommission für das Vereinigte Königreich (Art. 45 DSGVO); Nutzung nach den Nutzungsbedingungen der OpenStreetMap Foundation |

Keine Unterauftragsverarbeiter für Kundeninhalte: Stripe Payments Europe, Ltd. (Dublin) wickelt nur Zahlungen des Kunden ab und erhält keine Inhalte aus der Anwendung; dafür ist Stripe teilweise eigener Verantwortlicher (siehe Datenschutzerklärung). Anfragen über das Kontaktformular der Website verarbeitet der Anbieter in eigener Verantwortung. Let's Encrypt (Zertifikat, nur Domainname) und die Paketverzeichnisse für die Schwachstellenprüfung (nur Paketnamen und -versionen) erhalten keine Kundeninhalte.

Version 1.7 · Stand 23.10.2026 · Eduard Wiebe, FacilityDesk