Vertrag zur Auftragsverarbeitung für Schaltwerk

nach Art. 28 DSGVO · Stand: 4. November 2026
Auftragsverarbeiter: Taktlotse, Inh. Silvio Wloka, Pappelallee 64, 10437 Berlin

Vertragsparteien und elektronische Form

Dieser Vertrag zur Auftragsverarbeitung („AVV“) wird zwischen dem im Bestellprozess oder in der Auftragsbestätigung bezeichneten Kunden als **Verantwortlichem** und **Taktlotse, Inh. Silvio Wloka**, Pappelallee 64, 10437 Berlin, als **Auftragsverarbeiter** geschlossen.

Der AVV wird elektronisch abgeschlossen und ist Bestandteil des SaaS-Vertrags über Schaltwerk. Die Auftragsbestätigung beziehungsweise das Kundenkonto identifiziert den Verantwortlichen, den Beginn des Hauptvertrags und die angenommene AVV-Version. Eine gesonderte Unterschrift ist nicht erforderlich, soweit keine Partei sie verlangt.

1. Gegenstand, Dauer und Rangfolge

1. Gegenstand ist die Bereitstellung, das Hosting, der Betrieb, die Wartung, Datensicherung und der Support der SaaS-Software Schaltwerk sowie die Ausführung der vom Verantwortlichen genutzten Funktionen. Einzelheiten enthält Anlage 1.
2. Der AVV beginnt mit der ersten Verarbeitung von Kundendaten im Auftrag und gilt für die Dauer des Hauptvertrags. Lösch-, Rückgabe-, Vertraulichkeits- und Nachweispflichten wirken fort, soweit sie ihrer Natur nach über das Vertragsende hinausreichen.
3. Bei Widersprüchen gehen für die Verarbeitung im Auftrag dieser AVV und seine Anlagen dem Hauptvertrag vor.
4. Die tatsächliche Rollenverteilung bleibt maßgeblich. Verarbeitet der Auftragsverarbeiter einzelne Daten für eigene gesetzliche Vertrags-, Abrechnungs- oder Sicherheitszwecke, ist diese Verarbeitung nicht Gegenstand des Auftrags.

2. Umfang, Art und Zweck der Verarbeitung

1. Zweck, Verarbeitungsvorgänge, Datenarten, betroffene Personengruppen und besondere Kategorien personenbezogener Daten ergeben sich aus Anlage 1.
2. Gegenstand und Dauer, Art und Zweck der Verarbeitung dürfen nur durch Hauptvertrag, diesen AVV oder eine dokumentierte Weisung im zulässigen Rahmen geändert werden.
3. Die Funktion „Krankmeldung“ kann Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO umfassen. Diese Daten sind ausdrücklich vom Auftrag erfasst, soweit der Verantwortliche die Funktion rechtmäßig nutzt. Sie unterliegen besonderen Zugriffsbeschränkungen und Schutzmaßnahmen.
4. Daten zu strafrechtlichen Verurteilungen und Straftaten nach Art. 10 DSGVO sind kein regulärer Nutzungszweck. Ihre geplante Verarbeitung erfordert eine vorherige gesonderte Vereinbarung zu Rechtsgrundlage, Personenkreis, Datenarten und Schutzmaßnahmen.

3. Weisungen des Verantwortlichen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich bezüglich einer Übermittlung in ein Drittland, es sei denn, Unionsrecht oder das Recht eines Mitgliedstaats verpflichtet ihn zur Verarbeitung. In diesem Fall informiert er den Verantwortlichen vorab, soweit das Recht dies nicht verbietet.
2. Die erstmalige Weisung ergibt sich aus dem Hauptvertrag, der bestimmungsgemäßen Konfiguration und Nutzung von Schaltwerk, diesem AVV und seinen Anlagen. Einzelweisungen können über die Software oder in Textform an info@schaltwerk-app.de erteilt werden.
3. Weisungen, die den vereinbarten Leistungsumfang wesentlich erweitern, setzen eine Vereinbarung über technische Umsetzbarkeit, Zeitplan und angemessene Vergütung voraus. Zwingende datenschutzrechtliche Pflichten bleiben unberührt.
4. Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtswidrig, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung bis zur Bestätigung, Änderung oder Klärung aussetzen, soweit nicht eine sofortige Ausführung rechtlich geboten ist.
5. Der Verantwortliche benennt weisungsberechtigte Personen und hält deren Kontaktdaten aktuell. Der Auftragsverarbeiter darf die Berechtigung angemessen prüfen.

4. Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und Daten nur im erforderlichen Umfang verarbeiten.
2. Er setzt die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen um und erhält ein dem Risiko angemessenes Schutzniveau nach Art. 32 DSGVO. Änderungen sind zulässig, wenn das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.
3. Er führt ein Verzeichnis der für Verantwortliche durchgeführten Verarbeitungstätigkeiten, soweit gesetzlich erforderlich, und kooperiert mit der zuständigen Aufsichtsbehörde.
4. Kundendaten werden nicht für eigene Werbung, Profilbildung oder allgemeines Training fremder oder eigener KI-Modelle verwendet. KI-Funktionen übermitteln Inhalte an die in Anlage 3 genannten API-Dienste. Die meisten laufen nur, wenn ein berechtigter Nutzer sie im Einzelfall auslöst. Ohne Auslösen im Einzelfall laufen: (a) der Suchindex des Assistenten: Texte des Verantwortlichen, insbesondere Bauakten, Projekte, Aufgaben, Rechnungen, Mängel, Notizen, Nachrichten, Mails, Aufmaße, Angebote und Kundenstammdaten, werden regelmäßig bei OpenAI in Suchwerte umgerechnet; diese Funktion ist für alle aktiven Kundenkonten eingeschaltet; (b) das Einordnen eingehender Mails im Postfach und das Auslesen von Aufträgen, Lieferbestätigungen und Rechnungs-Mails; diese Funktionen sind eingeschaltet, solange der Verantwortliche sie nicht in Textform oder in den Einstellungen abschaltet; (c) Antwort-Entwürfe des Mail-Assistenten, nur für Postfächer, die der Verantwortliche dafür freigibt.

5. Der Auftragsverarbeiter informiert den Verantwortlichen, wenn eine Verarbeitung voraussichtlich ein hohes Risiko verursacht, das von den vereinbarten Maßnahmen nicht angemessen abgedeckt ist.
6. Datenschutzanfragen an den Auftragsverarbeiter können an info@schaltwerk-app.de gerichtet werden.

5. Unterstützung des Verantwortlichen

1. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.
2. Geht ein Antrag einer betroffenen Person unmittelbar beim Auftragsverarbeiter ein und betrifft er erkennbar Kundendaten, leitet er ihn unverzüglich an den Verantwortlichen weiter. Er beantwortet ihn nicht in der Sache, sofern er hierzu nicht angewiesen oder gesetzlich verpflichtet ist.
3. Unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen unterstützt er den Verantwortlichen bei den Pflichten nach Art. 32 bis 36 DSGVO, insbesondere Sicherheitsbewertung, Datenschutz-Folgenabschätzung, vorheriger Konsultation und Meldung von Datenschutzverletzungen.
4. Die im gewöhnlichen Leistungsumfang erforderliche Unterstützung ist mit dem SaaS-Entgelt abgegolten. Außergewöhnlicher Zusatzaufwand kann nach vorheriger Ankündigung und Vereinbarung angemessen vergütet werden, soweit die Ursache nicht in einer Pflichtverletzung des Auftragsverarbeiters liegt.

6. Datenschutzverletzungen

1. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Kundendaten unverzüglich, spätestens binnen 48 Stunden nach Bekanntwerden.
2. Die Erstmeldung enthält, soweit verfügbar: Art des Vorfalls; voraussichtlich betroffene Systeme, Datenarten und Personengruppen; ungefähre Anzahl betroffener Personen und Datensätze; bekannte oder wahrscheinliche Folgen; bereits ergriffene oder vorgeschlagene Maßnahmen; Zeitpunkt der Feststellung sowie eine Kontaktstelle. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.
3. Der Auftragsverarbeiter sichert relevante Beweise und Protokolle, dokumentiert den Vorfall und unterstützt den Verantwortlichen angemessen bei Risikobewertung und Meldungen. Er gibt gegenüber betroffenen Personen oder Behörden keine Erklärung im Namen des Verantwortlichen ab, sofern er nicht angewiesen oder gesetzlich verpflichtet ist.

7. Unterauftragsverarbeiter

1. Der Verantwortliche erteilt eine allgemeine schriftliche Genehmigung für die in Anlage 3 genannten Unterauftragsverarbeiter. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für deren datenschutzrechtliche Pflichten verantwortlich.

2. Der Auftragsverarbeiter informiert den Verantwortlichen grundsätzlich mindestens 30 Tage vor Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform über Name, Leistung, Land und Verarbeitungsort. In einem nachweisbaren Notfall informiert er ohne unangemessene Verzögerung nachträglich.
3. Der Verantwortliche kann innerhalb der Informationsfrist aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Die Parteien suchen eine zumutbare Alternative. Ist keine Lösung möglich, kann der Verantwortliche den betroffenen Leistungsteil zum Wirksamwerden der Änderung außerordentlich kündigen.
4. Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter mindestens zu denselben Datenschutzpflichten, die für dessen Verarbeitung nach diesem AVV gelten, einschließlich Vertraulichkeit, Sicherheit, Unterstützung, Löschung, Kontrollen und Drittlandtransfers.
5. Reine Nebenleistungen ohne Zugriffsmöglichkeit auf personenbezogene Kundendaten sind keine Unterauftragsverarbeitung.

8. Verarbeitungsorte und Drittlandtransfers

1. Verarbeitungsorte und mögliche Fernzugriffe ergeben sich aus Anlage 3. Eine Verarbeitung außerhalb des EWR oder ein Zugriff aus einem Drittland ist nur auf dokumentierte Weisung und bei Einhaltung der Art. 44 ff. DSGVO zulässig.
2. Soweit kein Angemessenheitsbeschluss nach Art. 45 DSGVO greift, stellt der Auftragsverarbeiter vor Beginn des Transfers geeignete Garantien sicher, insbesondere die passenden Standardvertragsklauseln der Europäischen Kommission. Er prüft das Schutzniveau im Empfängerland und setzt erforderliche ergänzende Maßnahmen um.
3. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die für dessen Rechenschaftspflicht erforderlichen Informationen zum Transfermechanismus zur Verfügung, soweit Geschäftsgeheimnisse und Sicherheitsinteressen durch geeignete Schwärzungen geschützt werden können.
4. Eine auf Deutschland oder den EWR beschränkte Speicherung der Kernanwendung schließt mögliche Verarbeitung oder Supportzugriffe eines KI-Dienstes oder eines anderen in Anlage 3 genannten Dienstes außerhalb des EWR nicht aus. Maßgeblich ist die konkrete, vor Aktivierung mitgeteilte Konfiguration.

9. Rückgabe und Löschung

1. Nach Abschluss der Auftragsverarbeitung löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Kundendaten zurück und löscht vorhandene Kopien, sofern Unionsrecht oder das Recht eines Mitgliedstaats keine Speicherung verlangt.
2. Der Verantwortliche übt sein Wahlrecht spätestens bis zum Ende der 30-tägigen Exportfrist aus. Ohne abweichende Weisung stellt der Auftragsverarbeiter die vereinbarten Exportfunktionen bereit und löscht anschließend die Produktivdaten.
3. Die Produktivdaten werden spätestens 90 Tage nach Vertragsende gelöscht.
4. Kopien in Sicherungen werden nicht einzeln gelöscht, sondern laufen nach den in Anlage 2 Nr. 5 genannten Fristen ab. Kopien ohne festen Ablauf (Datei-Spiegel und gegen Löschen gesperrtes Archiv im zweiten Rechenzentrum) löscht der

Auftragsverarbeiter gezielt, spätestens 14 Monate nach Löschung der Produktivdaten. Alle Kopien bleiben bis zu ihrer Löschung gesperrt und werden nur zur Wiederherstellung nach einem Sicherheits- oder Systemvorfall verwendet.

5. Der Auftragsverarbeiter bestätigt die vertragsgemäße Löschung auf Anfrage in Textform. Gesetzlich aufzubewahrende Daten werden getrennt gesperrt.

10. Nachweise und Audits

1. Der Auftragsverarbeiter stellt Informationen bereit, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen. Er kann vorrangig geeignete Nachweise, Prüfberichte, Sicherheitsdokumentationen und beantwortete Kontrollfragebögen vorlegen.
2. Der Verantwortliche oder ein fachkundiger und unabhängiger Prüfer darf einmal im Kalenderjahr ohne besonderen Anlass sowie darüber hinaus bei begründetem Bedarf Audits einschließlich Inspektionen durchführen. Audits sind grundsätzlich mindestens 14 Tage vorher anzukündigen, während üblicher Geschäftszeiten durchzuführen und so zu gestalten, dass Sicherheit, Vertraulichkeit, Betrieb und Rechte anderer Kunden nicht beeinträchtigt werden.
3. Bei einem konkreten Sicherheitsvorfall, einer begründeten Verdachtslage oder aufsichtsbehördlichen Vorgabe ist eine kürzere Ankündigung zulässig.
4. Der Verantwortliche trägt die angemessenen Kosten eines von ihm veranlassten Audits, soweit das Audit keinen wesentlichen Verstoß des Auftragsverarbeiters feststellt.
5. Prüfer dürfen keine Wettbewerber des Auftragsverarbeiters sein und müssen sich zur Vertraulichkeit verpflichten.

11. Pflichten des Verantwortlichen

1. Der Verantwortliche ist für Rechtmäßigkeit, Betroffenenrechte, Datenminimierung und Zulässigkeit seiner Weisungen verantwortlich.
2. Er konfiguriert Rollen und Zugriffe so, dass Nutzer nur erforderliche Daten sehen, und prüft Berechtigungen regelmäßig. Bei Krankmeldungen und anderen Gesundheitsdaten beschränkt er den Zugriff auf einen besonders kleinen, fachlich berechtigten Personenkreis.
3. Er informiert den Auftragsverarbeiter unverzüglich über erkannte Fehler, Unregelmäßigkeiten oder datenschutzrechtliche Risiken.
4. Er hält Datenschutzkontakte und weisungsberechtigte Personen aktuell.

12. Haftung und Schlussbestimmungen

1. Für Ansprüche betroffener Personen und den internen Ausgleich gelten Art. 82 DSGVO und sonstiges zwingendes Recht. Im Übrigen gelten die Haftungsregeln des Hauptvertrags, soweit sie zwingende datenschutzrechtliche Ansprüche nicht beschränken.
2. Änderungen dieses AVV einschließlich seiner Anlagen bedürfen der Textform. Die Aktualisierung der Unterauftragnehmerliste nach Ziffer 7 bleibt unberührt.
3. Es gilt deutsches Recht. Die Gerichtsstandsregelung des Hauptvertrags gilt, soweit gesetzlich zulässig.

4. Bei Unwirksamkeit einer Bestimmung gelten die gesetzlichen Vorschriften; die übrigen Regelungen bleiben unberührt.

Anlage 1 – Beschreibung der Verarbeitung

A. Gegenstand und Zweck

Bereitstellung und Betrieb einer webbasierten Betriebsmanagement-Software für Handwerksbetriebe, einschließlich Mandanten- und Nutzerverwaltung, Projekt-/Bauaktenverwaltung, Kunden- und Kontaktverwaltung, Angebote und Rechnungen, Einsatzplanung, Zeiterfassung, Mitarbeiterprozesse, Dokumentation, Datei-/Fotoverarbeitung, Kommunikation, Auswertungen, Exporte, Support, Datensicherung und – soweit aktiviert – assistierende KI-, Sprach-, Scan- und Erkennungsfunktionen.

B. Art der Verarbeitung

Erheben, Erfassen, Ordnen, Strukturieren, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch vom Verantwortlichen ausgelöste Übermittlung oder Bereitstellung, Abgleichen, Verknüpfen, Einschränken, Exportieren, Sichern, Wiederherstellen, Löschen und Vernichten.

C. Dauer

Für die Dauer des Hauptvertrags zuzüglich der vereinbarten Rückgabe-, Export- und Löschfristen.

D. Kategorien betroffener Personen

- Beschäftigte, Auszubildende, freie Mitarbeiter und sonstige Nutzer des Verantwortlichen;
- Kunden, Interessenten und deren Kontaktpersonen;
- Lieferanten, Nachunternehmer, Architekten, Planer, Bauleiter und sonstige Projektbeteiligte;
- Personen, die auf Baustellenfotos, Protokollen, Kommunikationsinhalten oder Dokumenten erkennbar sind;
- gesetzliche Vertreter und Ansprechpartner des Verantwortlichen.

E. Kategorien personenbezogener Daten

- Stamm- und Identifikationsdaten: Name, Firma, Anschrift, interne Kennung, Rolle;
- Kontakt- und Kommunikationsdaten: Telefon, E-Mail, Nachrichten und Vorgangsinhalte;
- Vertrags-, Angebots-, Auftrags-, Projekt- und Abrechnungsdaten;
- Beschäftigtendaten: Zuordnung, Qualifikation, Arbeits- und Einsatzzeiten, Urlaub, Abwesenheiten, Tagesberichte und Lohnvorbereitungsdaten;
- Bau- und Standortbezug: Baustellenadresse, Projektzuordnung, Termin- und Einsatzdaten;
- Dokument- und Mediendaten: Fotos, Pläne, PDFs, Belege, Lieferscheine, Protokolle, Unterschriften und Metadaten;

- Finanz- und Rechnungsdaten: Preise, Forderungen, Zahlungsstatus, Bankverbindung und steuerlich relevante Daten;
- Authentifizierungs-, Rollen-, Nutzungs-, Support-, Protokoll- und Sicherheitsdaten;
- Inhalte von Eingaben und Ausgaben assistierender KI-, Sprach-, Scan- und Erkennungsfunktionen.

F. Besondere Kategorien nach Art. 9 DSGVO

Gesundheitsdaten können insbesondere durch Krankmeldung, Abwesenheitsgrund, hochgeladene Nachweise, Arbeitsschutz- oder Unfallunterlagen sowie Freitexte entstehen. Diagnosen sind für die reguläre Nutzung nicht erforderlich und sollen nicht erfasst werden. Andere besondere Kategorien sind kein regulärer Zweck, können aber in unstrukturierten Uploads oder Freitexten versehentlich enthalten sein. Der Verantwortliche bleibt zu Datenminimierung und einer tragfähigen Rechtsgrundlage verpflichtet.

G. Frequenz und Empfänger

Fortlaufende Verarbeitung entsprechend der Nutzung. Empfänger sind autorisierte Nutzer des Verantwortlichen, der Auftragsverarbeiter und die in Anlage 3 genehmigten Unterauftragsverarbeiter; weitere Empfänger nur auf Weisung oder aufgrund gesetzlicher Pflicht.

Anlage 2 – Technische und organisatorische Maßnahmen (TOM)

1. Organisation und Vertraulichkeit

- dokumentierte Zuständigkeiten für Betrieb, Informationssicherheit, Datenschutz und Vorfallbearbeitung;
- Verpflichtung berechtigter Personen auf Vertraulichkeit;
- geregelte Vergabe und Entziehung interner Berechtigungen;
- dokumentierte Weisungs-, Auskunfts-, Export- und Löschprozesse.

2. Physische Zutrittskontrolle

- Betrieb der Produktivsysteme in professionell gesicherten Rechenzentren des in Anlage 3 genannten Hosters;
- Zutrittskontrollen, Strom- und Klimaabsicherung sowie Brandschutz durch den Hoster;
- kein regulärer Betrieb personenbezogener Produktivdaten auf frei zugänglichen lokalen Systemen.

3. Zugang, Authentifizierung und Zugriff

- individuelle administrative Zugänge und gesicherte Nutzerkonten;
- Passwort- beziehungsweise PIN-Schutz und rollenbasierte Rechte;
- zeitnahe Sperrung nicht mehr berechtigter Konten;
- administrative Zugriffe auf Kundendaten nur bei betrieblicher Erforderlichkeit, insbesondere Support, Wartung oder Vorfallbearbeitung;

- besonders restriktive Zugriffsrollen für Krankmeldungen und andere Gesundheitsdaten;
- logische Trennung der Kundenmandanten in Anwendung und Datenhaltung.

4. Übertragung und Integrität

- verschlüsselte Übertragung über HTTPS/TLS für Web- und App-Zugriffe (TLS 1.2 und 1.3, Weiterleitung von HTTP auf HTTPS, HSTS);
- dokumentierte Empfänger und geschützte Schnittstellen für ausgelöste Exporte oder Übermittlungen;
- Schutz vor unbefugter Veränderung sowie Protokollierung sicherheitsrelevanter administrativer Vorgänge, soweit technisch angemessen;
- Drittlandtransfers ausschließlich nach Ziffer 8 und Anlage 3.

5. Verfügbarkeit, Sicherung und Wiederherstellung

- regelmäßige automatisierte Sicherung der für die Wiederherstellung erforderlichen Produktivdaten;
- logisch getrennte Aufbewahrung von Produktivsystem und Sicherungen;
- Überwachung wesentlicher Systemkomponenten und Eskalation bei Ausfällen;
- dokumentiertes Verfahren für Wiederanlauf und Wiederherstellung;
- Sicherungen der Datenbank und der Dateien in einem getrennten Rechenzentrum in Deutschland; Datenbank-Sicherungen und Exporte sind verschlüsselt (AES-256);
- wöchentlicher automatisierter Wiederherstellungstest aus der Sicherung, mit Protokoll;
- Aufbewahrung: tägliche Stände 15 Tage, Wochenstände 60 Tage, jeweils überschriebene Fassungen weitere 30 Tage; Vollsicherungen der Datenbank für die Wiederherstellung auf einen Zeitpunkt bis zu vier Wochen; monatlicher Export je Kunde 400 Tage; Monatsstände auf dem Server 12 Monate;
- zusätzlich ein laufend fortgeschriebener Datei-Spiegel und ein gegen Löschen gesperrtes Archiv (Sperrfrist 35 Tage) in einem zweiten Rechenzentrum in Deutschland sowie ein Ersatzsystem mit laufender Datenbank-Spiegelung; Löschung dort nach Ziffer 9 Abs. 4.

6. Sichere Entwicklung und Vorfälle

- Trennung von Entwicklungs-, Test- und Produktivumgebung nach Risiko und keine reguläre Nutzung realer Kundendaten für Tests;
- geregelte Änderungen und Freigaben vor Produktiveinsatz;
- zeitnahe Installation sicherheitsrelevanter Aktualisierungen nach Risikobewertung;
- Verfahren zur Erkennung, Bewertung, Eindämmung, Beweissicherung, Meldung und Nachbereitung von Sicherheits- und Datenschutzvorfällen.

7. Datenminimierung und Löschung

- standardmäßig rollenbasierte, möglichst sparsame Sichtbarkeit von Daten;
- besondere Beschränkung für Krankmeldungen und Gesundheitsdaten;
- keine Verwendung von Kundendaten für allgemeines KI-Training;
- Lösch- und Exportprozess nach Ziffer 9;

- temporäre Dateien und Supportkopien werden nach Zweckerfüllung gelöscht.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Die mit „optional“ bezeichneten Dienste werden nur eingesetzt, wenn die zugehörige Funktion genutzt wird (Ziffer 4 Abs. 4 für KI-Funktionen). Vor dem erstmaligen produktiven Einsatz erhält der Verantwortliche die für seine konkrete Konfiguration maßgebliche Liste in Textform.

Unterauftragsverarbeiter	**Leistung**	**Sitz / Verarbeitungsorte**	**Transfermechanismus**
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Hosting von Anwendung, Datenbank und Backups	Deutschland / EWR	Verarbeitung innerhalb des EWR
mail.de GmbH, Friedrich-Ebert-Straße 70, 33330 Gütersloh	E-Mail-Postfach und E-Mail-Übermittlung	Deutschland / EWR	Verarbeitung innerhalb des EWR
OpenAI Ireland Ltd. und deren im DPA ausgewiesene Unterauftragnehmer	Suchwerte für den Assistenten (für alle aktiven Kundenkonten, Ziffer 4 Abs. 4 a); API-Verarbeitung von KI-Eingaben und Ausgaben aus ausgelösten oder eingeschalteten KI-Funktionen, einschließlich Umwandlung von Sprachaufnahmen in Text	EWR und weitere im DPA ausgewiesene Länder	Angemessenheitsbeschluss, soweit anwendbar; andernfalls EU-Standardvertragsklauseln und ergänzende Maßnahmen
Anthropic PBC und deren im DPA ausgewiesene Unterauftragnehmer	API-Verarbeitung von KI-Eingaben und Ausgaben aus ausgelösten oder eingeschalteten KI-Funktionen, insbesondere Einordnen und Auslesen eingehender Mails (Ziffer 4 Abs. 4 b, c)	USA und weitere im DPA ausgewiesene Länder	Angemessenheitsbeschluss, soweit anwendbar; andernfalls EU-Standardvertragsklauseln und ergänzende Maßnahmen
Functional Software, Inc. (Sentry)	Fehlerüberwachung des Servers: technische Fehlermeldungen mit Fehlertext, Programmablauf,	Speicherung in der EU-Region des Anbieters (Deutschland); Sitz des Anbieters USA	Angemessenheitsbeschluss, soweit anwendbar; andernfalls EU-Standardvertragsklauseln und ergänzende Maßnahmen

Unterauftragsverarbeiter	Leistung	Sitz / Verarbeitungsorte	Transfermechanismus
	aufgerufener Adresse sowie interner Nutzer- und Kundenkennung; ohne Inhalte von Anfragen, ohne Cookies, Namen, E-Mail-Adressen und IP-Adressen. Fehlertexte können im Einzelfall einzelne Datenwerte enthalten.		
Push-Dienste der Gerätehersteller: Apple, Google (für die Android-App: Google Firebase Cloud Messaging), Mozilla, Microsoft	Zustellung von Benachrichtigungen an Endgeräte. Inhalte von Web-Push-Nachrichten sind für den Push-Dienst verschlüsselt; Benachrichtigungen der iPhone-App enthalten nur einen neutralen Text; an Firebase gehen für die Android-App nur Geräte-Kennung, eine interne technische Kennung und eine Ablaufzeit, kein Inhalt.	USA und weitere Länder der jeweiligen Anbieter	Angemessenheitsbeschluss, soweit anwendbar; andernfalls EU-Standardvertragsklauseln und ergänzende Maßnahmen
OpenStreetMap Foundation	Kartenausschnitte (im Büro direkt aus dem Browser, in der Mitarbeiter-App über den Server des Auftragsverarbeiters) und Umrechnung der Baustellenadresse in Koordinaten (ohne Namen)	Vereinigtes Königreich	Angemessenheitsbeschluss
FOSSGIS e.V. (Overpass-API)	Suche des nächstgelegenen Krankenhauses anhand der Koordinaten einer Baustelle	Deutschland	Verarbeitung innerhalb des EWR
Bright Sky (Wetterdaten des Deutschen Wetterdienstes)	Wetterdaten für das Gebiet von Baustellen;	vom Anbieter nicht ausgewiesen	nicht erforderlich, da keine personenbezogenen Daten übermittelt werden

Unterauftragsverarbeiter	Leistung	Sitz / Verarbeitungsorte	Transfermechanismus
	übermittelt werden nur grobe Koordinaten (auf etwa 10 km gerundet), keine Adressen und keine personenbezogenen Daten		

Änderungen werden nach Ziffer 7 mitgeteilt. Die jeweils aktuelle öffentliche Vorabinformation ist online abrufbar; maßgeblich bleibt die dem Kunden in Textform mitgeteilte Vertragsfassung.