

WERK & WANDEL · BAUDOKU

# Auftragsverarbeitungsvertrag

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO

Version 0.1 · Stand: **04.09.2026**

Werk & Wandel · Andre Rehermann · Leonardstraße 2 · 33098 Paderborn

# Auftragsverarbeitungsvertrag

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 Abs. 3 DSGVO

zwischen

**Firmenname des Auftraggebers**

**Straße und Hausnummer**

**PLZ und Ort**

vertreten durch **Name der vertretungsberechtigten Person**

– nachfolgend „Verantwortlicher“ –

und

**Andre Rehermann, Einzelunternehmer, handelnd unter „Werk & Wandel“**

Leonardstraße 2

33098 Paderborn

– nachfolgend „Auftragsverarbeiter“ –

– gemeinsam die „Parteien“ –

## Präambel

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich der digitalen Baustellendokumentation unter der Bezeichnung „Baudoku“ auf Grundlage des zwischen den Parteien geschlossenen Haupt- bzw. Nutzungsvertrags (nachfolgend „Hauptvertrag“).

Im Rahmen dieser Leistungserbringung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien nach Art. 28 DSGVO. Er gilt ergänzend zum Hauptvertrag; im Fall von Widersprüchen in datenschutzrechtlichen Fragen gehen die Regelungen dieses Vertrags vor.

## § 1 Gegenstand, Dauer und Beendigung

(1) Gegenstand des Auftrags ist die Erbringung der im Hauptvertrag vereinbarten Leistungen, soweit dabei personenbezogene Daten verarbeitet werden. Art, Umfang und Zweck der Verarbeitung, die Kategorien personenbezogener Daten sowie die Kategorien betroffener Personen ergeben sich abschließend aus Anlage 1.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er endet automatisch mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf.

(3) Der Verantwortliche kann den Hauptvertrag jederzeit fristlos kündigen, wenn der Auftragsverarbeiter in schwerwiegender Weise gegen datenschutzrechtliche Vorschriften oder gegen wesentliche Pflichten aus diesem Vertrag verstößt, eine Weisung des Verantwortlichen nicht ausführt oder Kontrollrechte des Verantwortlichen vertragswidrig verweigert.

## § 2 Konkretisierung des Auftragsinhalts

(1) Die Einzelheiten der Verarbeitung sind in Anlage 1 beschrieben. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zu den dort genannten Zwecken.

(2) Die Verarbeitung findet ausschließlich innerhalb des Europäischen Wirtschaftsraums statt, soweit sich aus Anlage 3 nichts anderes ergibt. Für Verarbeitungen außerhalb des EWR gilt § 12.

(3) Eine über den Auftrag hinausgehende Verarbeitung, insbesondere die Nutzung der Daten zu eigenen Zwecken des Auftragsverarbeiters, ist ausgeschlossen. Dies gilt ausdrücklich auch für die Nutzung der Daten zum Training, zur Verbesserung oder zur Evaluierung von Modellen künstlicher Intelligenz.

### **§ 3 Weisungsbindung**

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- (2) Weisungen bedürfen der Textform. Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen. Der Hauptvertrag und dieser Vertrag stellen die ursprüngliche vollständige Weisung dar.
- (3) Weisungsberechtigt auf Seiten des Verantwortlichen ist die Person, die diesem Vertrag zustimmt.. Weisungsempfänger auf Seiten des Auftragsverarbeiters ist Andre Reherrmann, info@werkundwandel.digital.
- (4) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Verantwortlichen unverzüglich. Er ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.
- (5) Der Auftragsverarbeiter dokumentiert erteilte Weisungen und bewahrt die Dokumentation für die Dauer des Vertrags sowie 1 Jahr darüber hinaus auf.

### **§ 4 Pflichten des Auftragsverarbeiters**

- (1) Der Auftragsverarbeiter verpflichtet alle mit der Verarbeitung befassten Personen schriftlich zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.
- (2) Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 2 und hält sie während der Vertragslaufzeit aufrecht. Er ist berechtigt, die Maßnahmen weiterzuentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt er dem Verantwortlichen in Textform mit.
- (3) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen nach Kapitel III DSGVO.
- (4) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten und bei einer etwaigen Datenschutz-Folgenabschätzung.
- (5) Ein Datenschutzbeauftragter ist beim Auftragsverarbeiter derzeit nicht bestellt, da die Voraussetzungen des Art. 37 DSGVO in Verbindung mit § 38 BDSG nicht vorliegen. Ansprechpartner in Datenschutzfragen ist Andre Reherrmann, info@werkundwandel.digital. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, sobald ein Datenschutzbeauftragter bestellt wird.
- (6) Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt es dem Verantwortlichen auf Anforderung zur Verfügung.
- (7) Der Auftragsverarbeiter arbeitet auf Anfrage mit der zuständigen Aufsichtsbehörde zusammen und informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen von Aufsichtsbehörden, soweit sie sich auf diesen Auftrag beziehen.
- (8) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn Dritte, insbesondere Ermittlungs- oder Sicherheitsbehörden, Zugriff auf Daten des Verantwortlichen verlangen, soweit dies rechtlich zulässig ist.

### **§ 5 Technische und organisatorische Maßnahmen**

- (1) Die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO ergeben sich aus Anlage 2. Sie sind Vertragsbestandteil.
- (2) Der Auftragsverarbeiter überprüft die Wirksamkeit der Maßnahmen mindestens einmal jährlich sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitung und dokumentiert das Ergebnis.

## **§ 6 Unterauftragsverhältnisse**

- (1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und werden hiermit ausdrücklich genehmigt.
- (2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier Wochen vor der Beauftragung eines weiteren oder dem Austausch eines bestehenden Unterauftragsverarbeiters in Textform. Der Verantwortliche kann der Änderung innerhalb von zwei Wochen nach Zugang der Information aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Widerspricht er, sind die Parteien zu einer einvernehmlichen Lösung verpflichtet; kommt eine solche nicht zustande, steht dem Verantwortlichen ein außerordentliches Kündigungsrecht bezogen auf die betroffene Leistung zu.
- (3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Datenschutzniveau, das den Anforderungen dieses Vertrags und des Art. 28 DSGVO entspricht. Er bleibt gegenüber dem Verantwortlichen für die Einhaltung der Pflichten durch den Unterauftragsverarbeiter verantwortlich.
- (4) Keine Unterauftragsverarbeitung im Sinne dieser Regelung sind Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt und die die Verarbeitung personenbezogener Daten lediglich als unvermeidliche Begleiterscheinung mit sich bringen, etwa Telekommunikationsdienste, Post- und Transportdienste, Wartung oder Reinigung. Der Auftragsverarbeiter ist verpflichtet, auch insoweit angemessene Schutzmaßnahmen zu treffen.

## **§ 7 Rechte der betroffenen Personen**

- (1) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst.
- (2) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung von Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie bei Widersprüchen, soweit dies mit angemessenem Aufwand möglich ist.
- (3) Die Berichtigung, Löschung oder Einschränkung von Daten nimmt der Auftragsverarbeiter nur auf Weisung des Verantwortlichen vor.

## **§ 8 Nachweise und Kontrollrechte**

- (1) Der Auftragsverarbeiter weist die Einhaltung der Pflichten aus diesem Vertrag gegenüber dem Verantwortlichen in geeigneter Weise nach, insbesondere durch Vorlage der Dokumentation der technischen und organisatorischen Maßnahmen, durch Selbstauskünfte oder, sofern vorhanden, durch Zertifikate oder Prüfberichte unabhängiger Stellen.
- (2) Der Verantwortliche ist berechtigt, die Einhaltung dieses Vertrags durch Überprüfungen in den Geschäftsräumen des Auftragsverarbeiters zu kontrollieren oder durch einen zur Verschwiegenheit verpflichteten Prüfer kontrollieren zu lassen. Kontrollen sind mit einer Frist von mindestens 14 Tagen anzukündigen, während der üblichen Geschäftszeiten durchzuführen und so zu gestalten, dass der Betriebsablauf nicht unangemessen gestört wird. Sie finden ohne besonderen Anlass höchstens einmal jährlich statt.
- (3) Für Kontrollen, die über den in Absatz 2 genannten Umfang hinausgehen, kann der Auftragsverarbeiter eine angemessene Aufwandsentschädigung verlangen, sofern die Kontrolle nicht durch einen von ihm zu vertretenden Verstoß veranlasst ist.

## **§ 9 Verletzungen des Schutzes personenbezogener Daten**

- (1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten, die die im Auftrag verarbeiteten Daten betrifft.

(2) Die Mitteilung enthält, soweit verfügbar, eine Beschreibung der Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl betroffener Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO und ergreift unverzüglich geeignete Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen.

(4) Meldungen an eine Aufsichtsbehörde oder an betroffene Personen nimmt der Auftragsverarbeiter nicht ohne vorherige Abstimmung mit dem Verantwortlichen vor, es sei denn, er ist selbst gesetzlich dazu verpflichtet.

## **§ 10 Pflichten des Verantwortlichen**

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich. Er stellt insbesondere sicher, dass für die Verarbeitung eine Rechtsgrundlage nach Art. 6 DSGVO besteht und dass die Informationspflichten nach Art. 13 und 14 DSGVO gegenüber seinen Beschäftigten und gegenüber seinen eigenen Kunden erfüllt sind.

(2) Der Verantwortliche stellt durch geeignete Anweisungen an seine Beschäftigten sicher, dass keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO, insbesondere keine Gesundheitsdaten, in das System eingegeben werden. Das System ist für die Verarbeitung solcher Daten nicht ausgelegt.

(3) Der Verantwortliche verwaltet die Zugänge seiner Nutzer, schützt Zugangsdaten vor unbefugtem Zugriff und meldet dem Auftragsverarbeiter unverzüglich das Ausscheiden von Nutzern sowie den Verdacht eines unbefugten Zugriffs.

(4) Der Verantwortliche benennt die nach § 3 Abs. 3 weisungsberechtigte Person und teilt Änderungen unverzüglich mit.

## **§ 11 Löschung und Rückgabe**

(1) Nach Beendigung der Verarbeitungsleistungen löscht der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie zurück, je nach Wahl des Verantwortlichen. Der Verantwortliche teilt seine Wahl spätestens 360 Tage nach Vertragsende in Textform mit; erfolgt keine Mitteilung, werden die Daten gelöscht.

(2) Die Löschung erfolgt aus den produktiven Systemen innerhalb von 1 Jahr. Daten in verschlüsselten Sicherungskopien werden im Rahmen der regulären Rotationszyklen überschrieben, spätestens jedoch nach 1 Jahr.

(3) Bestehen gesetzliche Aufbewahrungspflichten, bleibt die Speicherung insoweit unberührt. Die betreffenden Daten werden für alle anderen Zwecke gesperrt.

(4) Der Auftragsverarbeiter weist die Löschung auf Verlangen in Textform nach.

## **§ 12 Verarbeitung außerhalb des Europäischen Wirtschaftsraums**

(1) Eine Verarbeitung personenbezogener Daten außerhalb des EWR findet nur statt, soweit dies in Anlage 3 ausgewiesen ist.

(2) Für solche Verarbeitungen stellt der Auftragsverarbeiter sicher, dass die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind, insbesondere durch einen Angemessenheitsbeschluss der Europäischen Kommission oder durch Standardvertragsklauseln nebst erforderlicher zusätzlicher Maßnahmen.

(3) Der Auftragsverarbeiter legt dem Verantwortlichen die jeweils einschlägigen Garantien auf Anforderung offen.

## § 13 Vertraulichkeit

(1) Die Parteien behandeln alle im Rahmen dieses Vertrags erlangten Informationen der jeweils anderen Partei vertraulich. Die Verpflichtung besteht über das Ende dieses Vertrags hinaus fort.

## § 14 Haftung

(1) Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Innenverhältnis gelten ergänzend die Haftungsregelungen des Hauptvertrags.

## § 15 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags einschließlich seiner Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.

(3) Es gilt das Recht der Bundesrepublik Deutschland.

(4) Gerichtsstand ist, soweit gesetzlich zulässig, Paderborn.

Anlagen: Anlage 1 – Beschreibung der Verarbeitung · Anlage 2 – Technische und organisatorische Maßnahmen · Anlage 3 – Unterauftragsverarbeiter

---

Ort, Datum – Verantwortlicher

---

Ort, Datum – Auftragsverarbeiter

## ANLAGE 1 ZUM AUFTRAGSVERARBEITUNGSVERTRAG

# Beschreibung der Verarbeitung

## Gegenstand und Zweck

Erstellung strukturierter Baustellendokumentation im Auftrag des Verantwortlichen. Beschäftigte des Verantwortlichen übermitteln über einen Messenger-Kanal Sprachnachrichten, Textnachrichten und Fotos zu einer zuvor ausgewählten Baustelle. Der Auftragsverarbeiter transkribiert die Sprachnachrichten, strukturiert die Inhalte automatisiert zu einem Tagesbericht und stellt diesen dem Verantwortlichen als PDF-Dokument sowie in der Weboberfläche bereit.

## Art der Verarbeitung

Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln an den Verantwortlichen, Einschränken, Löschen und Vernichten.

## Kategorien betroffener Personen

- Beschäftigte des Verantwortlichen, die das System nutzen (gewerbliche Mitarbeitende, Büropersonal, Leitung)
- Auftraggeber und Bauherren des Verantwortlichen sowie deren Ansprechpartner
- Dritte, die auf übermittelten Fotos oder in Freitextangaben zufällig erscheinen

## Kategorien personenbezogener Daten

| BETROFFENENGRUPPE                        | DATENKATEGORIEN                                                                                                                                                                                                                              |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschäftigte des Verantwortlichen</b> | Name, Mobilfunknummer, Messenger-Profilangaben, Zeitpunkt und Inhalt der übermittelten Nachrichten, Sprachaufnahmen und daraus erzeugte Transkripte, übermittelte Fotos, Freitextangaben zur ausgeführten Tätigkeit, Zuordnung zur Baustelle |
| <b>Auftraggeber des Verantwortlichen</b> | Bezeichnung des Bauvorhabens, Anschrift der Baustelle, gegebenenfalls Name und Kontaktdaten eines Ansprechpartners                                                                                                                           |
| <b>Nutzerkonten der Weboberfläche</b>    | Name, E-Mail-Adresse, Rolle, Zeitpunkt der Anmeldung, technische Protokolldaten                                                                                                                                                              |
| <b>Dritte</b>                            | Bild- und Textdaten, soweit sie unvermeidbar mit übermittelt werden                                                                                                                                                                          |

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Auftrags. Das System ist für deren Verarbeitung nicht ausgelegt; der Verantwortliche stellt deren Eingabe durch geeignete Anweisungen ab (§ 10 Abs. 2).

## Dauer der Verarbeitung

Für die Dauer des Hauptvertrags. Dokumentationsdaten werden für 1 Jahr gespeichert, sofern der Verantwortliche keine kürzere Frist weist. Rohdaten der Sprachnachrichten werden nach erfolgreicher Transkription nach 1 Jahr gelöscht. Nach Vertragsende gilt § 11.

## Ort der Verarbeitung

Europäischer Wirtschaftsraum, im Übrigen nach Maßgabe von Anlage 3.

## ANLAGE 2 ZUM AUFTRAGSVERARBEITUNGSVERTRAG

# Technische und organisatorische Maßnahmen

Maßnahmen nach Art. 32 DSGVO. Stand: 04.09.2026. Der Auftragsverarbeiter überprüft die Maßnahmen mindestens jährlich und dokumentiert das Ergebnis.

## 1. Vertraulichkeit

### Zutrittskontrolle

Es werden keine eigenen Serverräume betrieben. Die Verarbeitung erfolgt in Rechenzentren der in Anlage 3 genannten Anbieter, die über zertifizierte physische Zutrittssicherung verfügen. Arbeitsplatzgeräte des Auftragsverarbeiters befinden sich in abschließbaren Räumlichkeiten.

### Zugangskontrolle

Individuelle Benutzerkonten, keine Sammelkonten. Zwei-Faktor-Authentifizierung für alle administrativen Zugänge zu Infrastruktur, Datenbank und Messenger-Plattform. Passwortverwaltung über einen Passwortmanager. Festplattenverschlüsselung auf allen Endgeräten. Automatische Bildschirmsperre.

### Zugriffskontrolle

Rollen- und rechtebasiertes Berechtigungskonzept nach dem Prinzip der geringsten Rechte. Getrennte Schlüssel für Anwendungs- und Administrationszugriffe; Schlüssel mit erweiterten Rechten werden ausschließlich serverseitig verwendet und nicht im Frontend ausgeliefert. Regelmäßige Rotation von Zugangsschlüsseln, Deaktivierung nicht mehr benötigter Schlüssel.

### Trennungskontrolle

Mandantenfähige Datenhaltung mit eindeutiger Mandanten-Kennung je Verantwortlichem. Durchsetzung der Mandantentrennung auf Datenbankebene über zeilenbasierte Zugriffsregeln. Getrennte Systeme für Test- und Produktivbetrieb.

### Pseudonymisierung

Eine Pseudonymisierung gegenüber dem eingesetzten Sprachmodell findet nicht statt und ist zweckbedingt nicht möglich: Der erzeugte Tagesbericht muss die anwesenden Mitarbeiter namentlich ausweisen, da er als Nachweis der Arbeitszeit und Leistungserbringung dient. An das Sprachmodell (Anthropic Claude) werden übergeben: Baustellenbezeichnung, Kundenname, Datum, Namen der anwesenden Mitarbeiter mit den jeweils erfassten Stunden sowie die von den Mitarbeitern erfassten Notizen, Transkripte von Sprachnachrichten und Bildbeschreibungen. Nicht übergeben werden: Telefonnummern, E-Mail-Adressen, Adressdaten, Stundensätze, Vertrags- und Abrechnungsdaten sowie sämtliche internen Kennungen. Die Datenminimierung erfolgt stattdessen an anderer Stelle: Über den Messengerdienst werden ausschließlich Kurzbezeichnungen der Baustellen übertragen, vollständige Adressdaten verbleiben in der Datenbank innerhalb der EU. Gegenüber Anthropic besteht ein Auftragsverarbeitungsvertrag; die übermittelten Daten werden nicht zum Training von Modellen verwendet.

## 2. Integrität

### Weitergabekontrolle

Transportverschlüsselung nach dem Stand der Technik (TLS) für sämtliche Verbindungen, automatisierte Zertifikatsverwaltung. Verschlüsselte Speicherung ruhender Daten bei den eingesetzten Anbietern. Sicherungskopien werden vor der Übertragung an den Speicherort clientseitig verschlüsselt, sodass der Speicheranbieter keinen Zugriff auf die Inhalte hat.

**Eingabekontrolle**

Protokollierung von Erstellung, Änderung und Löschung von Datensätzen mit Zeitstempel und auslösendem Konto. Nachvollziehbarkeit administrativer Eingriffe über Systemprotokolle.

**3. Verfügbarkeit und Belastbarkeit****Datensicherung**

Automatisierte tägliche Sicherung der Datenbank durch den Datenbankanbieter sowie zusätzliche, davon unabhängige verschlüsselte Sicherung auf einem getrennten Speicherort. Die Wiederherstellbarkeit wurde getestet und wird halbjährlich erneut geprüft.

**Verfügbarkeit**

Betrieb auf Infrastruktur mit Redundanz auf Anbieterseite. Automatisierte Verfügbarkeitsüberwachung mit Benachrichtigung bei Ausfällen. Getrennte Ausführung von Anwendungs- und Verarbeitungskomponenten.

**Wiederherstellbarkeit**

Dokumentiertes Wiederstellungsverfahren. Wiederstellungszeit im Regelfall unter 24 Stunden.

**4. Verfahren zur regelmäßigen Überprüfung****Datenschutzmanagement**

Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO wird geführt und gepflegt. Verpflichtung auf Vertraulichkeit für alle beteiligten Personen. Überprüfung der Maßnahmen mindestens jährlich sowie anlassbezogen.

**Vorfallreaktion**

Definierter Meldeweg bei Verletzungen des Schutzes personenbezogener Daten mit Benachrichtigung des Verantwortlichen innerhalb der in § 9 vereinbarten Frist. Dokumentation aller Vorfälle.

**Datenschutzfreundliche Voreinstellungen**

Datensparsame Gestaltung der Verarbeitungsprozesse. Übermittlung nur der für den jeweiligen Verarbeitungsschritt erforderlichen Datenfelder. Keine Nutzung der Daten zu eigenen Zwecken oder zum Training von Modellen.

**Auftragskontrolle**

Schriftliche Vereinbarungen mit allen Unterauftragsverarbeitern. Prüfung der Anbieter vor Beauftragung. Führung und Pflege der Liste nach Anlage 3.

## ANLAGE 3 ZUM AUFTRAGSVERARBEITUNGSVERTRAG

# Unterauftragsverarbeiter

Stand: 04.09.2026. Der Verantwortliche genehmigt mit Abschluss dieses Vertrags die nachfolgend aufgeführten Unterauftragsverarbeiter. Änderungen richten sich nach § 6.

| Dienstleister                   | Zweck                                                             | Ort der Verarbeitung |
|---------------------------------|-------------------------------------------------------------------|----------------------|
| Netcup GmbH                     | Betrieb der Anwendung und der Automatisierungsprozesse            | Deutschland          |
| Supabase Pte. Ltd               | Speicherung der Konto- und Anwendungsdaten                        | Deutschland          |
| IONOS SE                        | Bereitstellung und Absicherung der Oberfläche                     | Deutschland          |
| Stripe Payments Europe Ltd.     | Abwicklung von Zahlungen und Abonnements                          | USA/Europa           |
| Plus Five Five, Inc.            | Versand von System- und Servicenachrichten                        | EU/Irland            |
| WhatsApp Ireland Limited        | Übermittlung der Nachrichten zwischen Beschäftigten und Anwendung | EU und Drittländer   |
| OpenAI Ireland Ltd              | Umwandlung von Sprachnachrichten in Text                          | USA                  |
| Anthropic Ireland Limited       | Automatisierte Strukturierung der Berichtstexte                   | USA                  |
| Microsoft Professional Services | Aufbewahrung verschlüsselter Sicherungskopien                     | Deutschland          |
| Haufe Service Center GmbH       | Rechnungsstellung und Buchführung                                 | Deutschland          |
| HubSpot, Inc                    | Betreuung von Interessenten und Kunden                            | Deutschland          |