

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

Auftraggeber (Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO)

[Firma / Name des Betriebs]
[Straße und Hausnummer]
[PLZ, Ort]
vertreten durch: [vertretungsberechtigte Person]
E-Mail: [E-Mail-Adresse]

– nachfolgend „Auftraggeber“ –

und

Auftragnehmer (Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO)

Andre Reherrmann – Werk & Wandel
Leonardstraße 2
33098 Paderborn
E-Mail: info@werkundwandel.digital
Telefon: +49 152 24296100

– nachfolgend „Auftragnehmer“ –

Auftraggeber und Auftragnehmer nachfolgend einzeln auch „Partei“ und gemeinsam „Parteien“ genannt.

Präambel

Der Auftragnehmer stellt dem Auftraggeber die Anwendung „Werk & Wandel Baudoku“ zur Verfügung. Mit dieser können Mitarbeiter des Auftraggebers Baustellendokumentation per WhatsApp (Text, Sprachnachricht, Foto) erfassen; der Dienst erstellt daraus automatisiert PDF-Tagesberichte und versendet diese per E-Mail. Im Rahmen dieser Leistungserbringung verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gemäß Art. 28 DSGVO und ist Bestandteil des zwischen den Parteien geschlossenen Hauptvertrags (Nutzungs-/Leistungsvertrag, nachfolgend „Hauptvertrag“).

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Bereitstellung und des Betriebs der Anwendung „Werk & Wandel Baudoku“. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen ergeben sich aus Anlage 1.

(2) Die Dauer dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrags. Der Vertrag endet automatisch mit Beendigung des Hauptvertrags, ohne dass es einer gesonderten Kündigung bedarf, unbeschadet der nachwirkenden Pflichten aus diesem Vertrag (insbesondere § 10).

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Umfang und zu den Zwecken, die zur Erbringung der vertraglich vereinbarten Leistungen erforderlich sind. Eine Verarbeitung der Daten zu eigenen Zwecken des Auftragnehmers findet nicht statt.

(2) Die Verarbeitung erfolgt ausschließlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums, soweit in Anlage 3 nicht ausdrücklich etwas anderes (Drittlandtransfer mit geeigneten Garantien nach § 9) geregelt ist.

§ 3 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, einschließlich in Bezug auf die Übermittlung in Drittländer, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist.

(2) Die Nutzung der Anwendung gemäß ihrer Zweckbestimmung und im Rahmen der vom Auftraggeber vorgenommenen Konfiguration gilt als Weisung. Weitergehende Einzelweisungen sind in Textform (z.B. per E-Mail an info@werkundwandel.digital) zu erteilen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber unverzüglich. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wird.

§ 4 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich insbesondere:

- a) die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers zu verarbeiten (siehe § 3);
- b) zu gewährleisten, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- c) alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen (siehe § 5 und Anlage 2);
- d) die Bedingungen für die Inanspruchnahme weiterer Auftragsverarbeiter gemäß Art. 28 Abs. 2 und 4 DSGVO einzuhalten (siehe § 6 und Anlage 3);
- e) den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO) zu unterstützen (siehe § 7);
- f) den Auftraggeber bei der Einhaltung der Pflichten gemäß Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen zu unterstützen;
- g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Aufbewahrungspflicht besteht (siehe § 10);

- h) dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung zu stellen und Überprüfungen zu ermöglichen und dazu beizutragen (siehe § 11).

Der Auftragnehmer hat eine zuständige Ansprechperson für den Datenschutz benannt; diese ist unter info@werkundwandel.digital erreichbar.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus gemäß Art. 32 DSGVO. Maßgeblich ist der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer ist berechtigt, alternative angemessene Maßnahmen umzusetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und gelten als genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern (Textform genügt) und räumt dem Auftraggeber die Möglichkeit ein, gegen derartige Änderungen innerhalb von vierzehn (14) Tagen Einspruch zu erheben.

(3) Der Auftragnehmer stellt durch vertragliche Vereinbarung sicher, dass den Unterauftragsverarbeitern dieselben Datenschutzpflichten auferlegt werden, wie sie in diesem Vertrag festgelegt sind. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten.

(4) Als Unterauftragsverhältnis im Sinne dieser Regelung gelten nicht Nebenleistungen, die der Auftragnehmer als reine Annexleistung in Anspruch nimmt (z.B. Telekommunikationsleistungen, Wartung), sofern hierbei kein wesentlicher Zugriff auf personenbezogene Daten erfolgt.

§ 7 Unterstützungspflichten

(1) Wendet sich eine betroffene Person mit Anträgen zur Berichtigung, Löschung, Auskunft oder sonstigen Betroffenenrechten unmittelbar an den Auftragnehmer, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter, sofern eine Zuordnung zum Auftraggeber möglich ist.

(2) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen sowie bei der Einhaltung der Pflichten zur Datensicherheit, zur Meldung von Datenschutzverletzungen, zur Datenschutz-Folgenabschätzung und zur vorherigen Konsultation (Art. 32 bis 36 DSGVO).

(3) Über einen über die vereinbarte Leistung hinausgehenden Unterstützungsaufwand kann der Auftragnehmer eine angemessene Vergütung verlangen, sofern der Aufwand nicht auf einem Verschulden des Auftragnehmers beruht.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten, die im Zusammenhang mit dem Auftrag steht, unverzüglich nach Bekanntwerden.

(2) Die Meldung enthält nach Möglichkeit eine Beschreibung der Art der Verletzung, der betroffenen Datenkategorien und -personen, der wahrscheinlichen Folgen sowie der ergriffenen oder vorgeschlagenen Maßnahmen. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Melde- und Benachrichtigungspflichten gemäß Art. 33 und 34 DSGVO.

§ 9 Datenübermittlung in Drittländer

Eine Übermittlung personenbezogener Daten in ein Drittland erfolgt nur, soweit dies in Anlage 3 ausgewiesen ist oder der Auftraggeber dies anweist und die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Soweit Unterauftragsverarbeiter mit Sitz bzw.

Datenverarbeitung außerhalb der EU/des EWR eingesetzt werden, ist ein angemessenes Datenschutzniveau durch geeignete Garantien sicherzustellen, insbesondere durch EU-Standardvertragsklauseln (SCC) und/oder eine Zertifizierung nach dem EU-US Data Privacy Framework.

§ 10 Löschung und Rückgabe nach Beendigung

(1) Nach Abschluss der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers sämtliche personenbezogenen Daten oder gibt diese in einem gängigen Format zurück und löscht anschließend vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der Daten besteht.

(2) Sprachaufnahmen und Transkripte werden bereits während der Vertragslaufzeit nach Erstellung des jeweiligen Berichts, spätestens jedoch nach 30 Tagen, automatisiert gelöscht. Dokumentation und Nachweis der Löschung erfolgen auf Anforderung des Auftraggebers.

§ 11 Nachweis- und Kontrollrechte

(1) Der Auftragnehmer weist dem Auftraggeber auf Anforderung die Einhaltung der in diesem Vertrag festgelegten Pflichten in geeigneter Weise nach, insbesondere durch Vorlage einer Dokumentation der technischen und organisatorischen Maßnahmen oder durch geeignete Zertifikate bzw. Berichte unabhängiger Stellen, soweit vorhanden.

(2) Der Auftraggeber ist berechtigt, sich von der Einhaltung der Pflichten zu überzeugen, im erforderlichen Umfang auch durch Kontrollen vor Ort. Solche Kontrollen sind mit angemessener Vorankündigung, während der üblichen Geschäftszeiten und ohne unzumutbare Betriebsstörung durchzuführen. Der Auftragnehmer kann die Kontrolle vom Abschluss einer Vertraulichkeitsvereinbarung abhängig machen.

§ 12 Haftung

Für die Haftung der Parteien gelten die Regelungen des Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags entsprechend, soweit dieser Vertrag keine

abweichenden Regelungen enthält. Der Auftraggeber bleibt im Außenverhältnis für die Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen verantwortlich.

§ 13 Laufzeit und Kündigung

Dieser Vertrag ist untrennbar mit dem Hauptvertrag verbunden und teilt dessen Laufzeit. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen. Das Recht zur außerordentlichen Kündigung des Hauptvertrags aus wichtigem Grund, insbesondere bei schwerwiegenden Verstößen gegen datenschutzrechtliche Bestimmungen, bleibt unberührt.

§ 14 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieses Vertrags sowie seiner Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.
- (2) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen hinsichtlich datenschutzrechtlicher Regelungen die Bestimmungen dieses Vertrags vor.
- (3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, eine unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.
- (4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Unterschriften

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer (Werk & Wandel)

Anlage 1 – Gegenstand und Einzelheiten der Verarbeitung

Gegenstand und Zweck der Verarbeitung

Bereitstellung und Betrieb der Anwendung „Werk & Wandel Baudoku“: Erfassung von Baustellendokumentation per WhatsApp (Text, Sprachnachricht, Foto), automatisierte Transkription von Sprachnachrichten, KI-gestützte Erstellung von PDF-Tagesberichten sowie deren Versand per E-Mail; Verwaltung von Nutzerkonten und Mitarbeitern des Auftraggebers.

Art der Verarbeitung

Erheben, Erfassen, Speichern, Auslesen, Verwenden, Transkribieren, Auswerten, Aufbereiten, Übermitteln (Versand) und Löschen personenbezogener Daten.

Kategorien betroffener Personen

- Mitarbeiter des Auftraggebers (Nutzer der WhatsApp-Erfassung)
- Ansprechpartner / Kontoinhaber des Auftraggebers
- Ggf. in der Baustellendokumentation genannte Dritte (z.B. Kunden, Auftraggeber des Betriebs, weitere am Bau Beteiligte)

Kategorien personenbezogener Daten

- Stammdaten der Mitarbeiter (Name, Telefon-/WhatsApp-Nummer)
- Konto- und Kontaktdaten des Auftraggebers (Name, E-Mail, Unternehmensname)
- Kommunikations- und Inhaltsdaten (Textnachrichten, Sprachaufnahmen, Transkripte, Fotos)
- Aus den Inhalten erzeugte Berichte (PDF-Tagesberichte)
- Nutzungs- und Metadaten (Zeitstempel, Zuordnung zu Baustellen)

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand des Auftrags und sollen vom Auftraggeber nicht über den Dienst verarbeitet werden.

Dauer der Verarbeitung

Für die Laufzeit des Hauptvertrags. Sprachaufnahmen und Transkripte werden nach Berichtserstellung, spätestens nach 30 Tagen, gelöscht. Im Übrigen gilt § 10.

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

Der Auftragnehmer hat insbesondere die nachfolgenden Maßnahmen umgesetzt. Die Maßnahmen sind regelmäßig zu überprüfen und an den Stand der Technik anzupassen.

Vertraulichkeit

- Zutrittskontrolle: Datenverarbeitung erfolgt ausschließlich bei zertifizierten Hosting-Anbietern mit gesicherten Rechenzentren (Zutrittsschutz durch die Betreiber).
- Zugangskontrolle: Authentifizierung der Nutzer über individuelle Konten mit Passwortschutz; verschlüsselte Speicherung der Passwörter; Schutz administrativer Zugänge.
- Zugriffskontrolle: Rollen- und Rechtekonzept; mandantengetrennter Datenzugriff auf Datenbankebene (Row-Level-Security); Zugriff nur für berechtigte Personen im erforderlichen Umfang.
- Verschlüsselung: Transportverschlüsselung (TLS/HTTPS) bei allen Datenübertragungen; Verschlüsselung gespeicherter Daten beim Hosting-Anbieter.

Integrität

- Weitergabekontrolle: Übertragung personenbezogener Daten ausschließlich über verschlüsselte Verbindungen; dokumentierte Schnittstellen zu Unterauftragsverarbeitern.
- Eingabekontrolle: Protokollierung wesentlicher Verarbeitungsvorgänge; Nachvollziehbarkeit von Eingaben und Änderungen über System-Logs.

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Regelmäßige Datensicherungen durch den Hosting-/Datenbankanbieter; Schutzmaßnahmen gegen Datenverlust.
- Rasche Wiederherstellbarkeit: Möglichkeit der Wiederherstellung von Daten nach einem physischen oder technischen Zwischenfall.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Trennungskontrolle: Logische Trennung der Daten verschiedener Auftraggeber (Mandantentrennung).
- Auftragskontrolle: Auswahl der Unterauftragsverarbeiter nach Eignung; vertragliche Verpflichtung gemäß Art. 28 DSGVO; regelmäßige Überprüfung.
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO); Datenminimierung und definierte Löschfristen.

Hinweis: Diese Maßnahmen sind anhand der tatsächlichen Implementierung zu prüfen und zu konkretisieren.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Die folgenden Unterauftragsverarbeiter sind zum Zeitpunkt des Vertragsschlusses genehmigt:

Unterauftragsverarbeiter	Zweck / Leistung	Sitz / Verarbeitung	Garantie bei Drittland
Lovable / GoStudent Holding GmbH (inkl. Cloudflare)	Hosting und Auslieferung der Anwendung	EU / ggf. global (CDN)	SCC / DPF
Supabase, Inc.	Datenbank, Authentifizierung, Datei-Speicher	EU (Frankfurt)	EU-Hosting
Meta Platforms Ireland Ltd.	WhatsApp Business Plattform (Nachrichtenein-/ausgang)	Irland / USA	SCC / DPF
OpenAI (Whisper) – Anbieter prüfen	Transkription von Sprachnachrichten	USA	SCC / DPF
Anthropic PBC	KI-Modell (Claude) zur Berichtserstellung	USA	SCC / DPF
PDFShift – Anbieter/Sitz prüfen	Erzeugung der PDF-Berichte	EU/USA (prüfen)	SCC / DPF
Resend, Inc.	Versand von Berichten und System-E-Mails	USA	SCC / DPF
Stripe Payments Europe, Ltd. / Stripe, Inc.	Zahlungsabwicklung (Abonnements)	Irland / USA	SCC / DPF
n8n GmbH (n8n Cloud)	Workflow-Automatisierung	EU	EU-Hosting

Hinweis: Die Liste ist anhand der tatsächlich eingesetzten Dienste, der genauen Rechtsträger und der jeweils geschlossenen Auftragsverarbeitungsverträge zu verifizieren und aktuell zu halten.

Dieses Dokument ist eine Vorlage und ersetzt keine Rechtsberatung. Vor dem Einsatz sollte es durch eine fachkundige Person (Datenschutz-/IT-Recht) geprüft und an die tatsächlichen Verhältnisse angepasst werden.