Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Fassung 2026-11-23 · Prüfsumme SHA-256: 7875be0144c21c9674c5edd40bc2897226df4b20fe6b671071fc5ce5fb431475

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Fassung 2026-11-23 · gültig ab 23. November 2026

Dieser Vertrag zur Auftragsverarbeitung (nachfolgend "Vertrag") konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus dem zwischen ihnen bestehenden Vertrag über die Nutzung der Software HeWo (nachfolgend "Hauptvertrag").

Zwischen

dem Kunden, der die Software HeWo nutzt und dessen Betriebsdaten in der Anwendung hinterlegt sind (nachfolgend "Verantwortlicher"),

und

HeWo Systems GbR, vertreten durch Bo Herzog und Lios Wolters, Elbchaussee 17, 22765 Hamburg, Deutschland, E-Mail kontakt@hewosystems.com (nachfolgend "Auftragsverarbeiter").

1. Gegenstand, Art und Zweck der Verarbeitung

1.1 Der Auftragsverarbeiter stellt dem Verantwortlichen die Software HeWo als über das Internet nutzbare Anwendung (Software as a Service) einschließlich der zugehörigen mobilen Anwendung bereit. Die Software unterstützt Handwerksbetriebe bei Planung, Disposition, Durchführung, Dokumentation und Abrechnung ihrer Aufträge.

1.2 Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Verantwortlichen ausschließlich zu dem Zweck, diese Leistung zu erbringen. Eine Verarbeitung dieser Daten zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt. Insbesondere werden die Daten nicht zu Werbezwecken genutzt, nicht an Dritte verkauft und nicht zum Training von Systemen künstlicher Intelligenz verwendet.
Ausgenommen sind die Sicherheits- und Protokolldaten und die Nutzungsereignisse nach Anlage 1 Abschnitt B, die bei der Nutzung der Software selbst entstehen. Diese verarbeitet der Auftragsverarbeiter als eigener Verantwortlicher, um den Dienst gegen Angriffe und Missbrauch zu schützen, den Betrieb zu überwachen und die Software weiterzuentwickeln (Art. 6 Abs. 1 lit. f, Art. 32 DSGVO). Er verwendet dafür keine Inhalte wie Texte, Fotos, Dokumente oder Sprachaufnahmen, löscht Sicherheits- und Protokolldaten nach 90 Tagen und Nutzungsereignisse nach 180 Tagen und informiert die betroffenen Personen in seiner Datenschutzerklärung.

1.3 Art der Verarbeitung sind das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln, Einschränken, Löschen und Vernichten der in Anlage 1 genannten Daten mittels automatisierter Verfahren.

1.4 Die Datenbank, der Dateispeicher und die Authentifizierungsdaten werden in der Europäischen Union gespeichert. Für die übrigen in Anlage 3 genannten Dienste gilt der dort angegebene Verarbeitungsort. Ein Zugriff durch den Auftragsverarbeiter oder seine Unterauftragsverarbeiter aus Drittländern ist nur nach Maßgabe der Ziffern 3.2 und 9.6 und der Anlage 3 zulässig.

2. Dauer

Der Vertrag beginnt mit seiner Annahme durch den Verantwortlichen und läuft auf unbestimmte Zeit. Er endet automatisch mit der Beendigung des Hauptvertrags. Die Pflichten aus Ziffer 11 (Löschung und Rückgabe) sowie aus Ziffer 5 (Vertraulichkeit) bestehen über das Vertragsende hinaus fort.

3. Weisungsrecht

3.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Als dokumentierte Weisung gelten dieser Vertrag, der Hauptvertrag sowie die Nutzung der Funktionen der Software durch den Verantwortlichen und die von ihm berechtigten Personen. Einzelweisungen sind in Textform an kontakt@hewosystems.com zu richten.

3.2 Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgt nur im Rahmen der Ziffer 9.6 und der Anlage 3, die der Verantwortliche damit als Weisung erteilt, oder wenn der Auftragsverarbeiter hierzu nach dem Unionsrecht oder dem Recht der Mitgliedstaaten verpflichtet ist. Im zweiten Fall teilt der Auftragsverarbeiter dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.3 Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die Datenschutz-Grundverordnung oder andere Datenschutzbestimmungen verstößt, teilt er dies dem Verantwortlichen unverzüglich mit. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis der Verantwortliche sie bestätigt oder ändert.

3.4 Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen verantwortlich. Er stellt insbesondere sicher, dass für den Einsatz der Software eine Rechtsgrundlage besteht und dass etwaige Beteiligungsrechte betrieblicher Interessenvertretungen gewahrt sind.

4. Datenschutz-Hinweis zu besonderen Funktionen

4.1 Die Software enthält Funktionen, die Daten von Beschäftigten des Verantwortlichen verarbeiten, insbesondere die Erfassung von Arbeits- und Fahrtzeiten sowie eine auf ausdrückliche Nutzerhandlung ausgelöste Prüfung des Standorts am Einsatzort. Eine Hintergrundortung findet nicht statt.

4.2 Der Verantwortliche entscheidet als Arbeitgeber eigenständig über den Einsatz dieser Funktionen, über die dafür maßgebliche Rechtsgrundlage und über die Einhaltung der Vorschriften des Beschäftigtendatenschutzes einschließlich etwaiger Mitbestimmungsrechte. Der Auftragsverarbeiter stellt hierzu die technische Beschreibung der verarbeiteten Daten in Anlage 1 zur Verfügung.

4.3 Die Sprachfunktion ist optional. Wird sie genutzt, werden die Sprachaufnahme, das daraus erzeugte Transkript und der zur Zuordnung erforderliche Ausschnitt des Materialkatalogs an den in Anlage 3 genannten Unterauftragsverarbeiter für die Sprach- und Textauswertung übermittelt. Sämtliche Angaben lassen sich alternativ manuell erfassen.

5. Vertraulichkeit

5.1 Der Auftragsverarbeiter setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung wirkt über die Beendigung der Tätigkeit hinaus fort.

5.2 Der Auftragsverarbeiter macht die eingesetzten Personen vor Aufnahme der Tätigkeit mit den für sie geltenden Datenschutzbestimmungen vertraut und unterweist sie in angemessenen Abständen.

5.3 Der Zugriff auf Produktivdaten des Verantwortlichen ist auf die Fälle beschränkt, in denen dies zur Störungsbeseitigung, zur Erfüllung einer Support-Anfrage des Verantwortlichen oder zur Abwehr eines Sicherheitsvorfalls erforderlich ist.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Der zum Zeitpunkt des Vertragsschlusses geltende Stand ist in Anlage 2 beschrieben.

6.2 Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie anpassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dem Verantwortlichen in Textform mitgeteilt.

6.3 Der Auftragsverarbeiter überprüft die Wirksamkeit der Maßnahmen regelmäßig und dokumentiert die Überprüfung.

7. Unterstützung des Verantwortlichen

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen mit angemessenen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch. Soweit die Software dem Verantwortlichen entsprechende Funktionen bereitstellt, nutzt dieser vorrangig diese Funktionen.

7.2 Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht eigenständig, soweit es Daten betrifft, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet. Für Daten, die er nach Ziffer 1.2 (zweiter Absatz) als eigener Verantwortlicher verarbeitet, beantwortet er das Anliegen selbst.

7.3 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgenabschätzung und der vorherigen Konsultation. Dabei werden die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt.

7.4 Unterstützungsleistungen, die über den vertraglich geschuldeten Umfang hinausgehen und nicht auf einem vom Auftragsverarbeiter zu vertretenden Umstand beruhen, kann der Auftragsverarbeiter nach Ankündigung nach Aufwand abrechnen.

8. Verletzungen des Schutzes personenbezogener Daten

8.1 Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten, die dessen Daten betrifft, unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, in Textform an die vom Verantwortlichen hinterlegte Kontaktadresse.

8.2 Die Meldung enthält, soweit verfügbar, eine Beschreibung der Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Abhilfemaßnahmen sowie eine Kontaktstelle für Rückfragen. Sind die Informationen noch nicht vollständig verfügbar, werden sie unverzüglich nachgereicht.

8.3 Die Meldung an die Aufsichtsbehörde und gegebenenfalls an die betroffenen Personen obliegt dem Verantwortlichen. Der Auftragsverarbeiter unterstützt ihn dabei mit den ihm vorliegenden Informationen.

9. Unterauftragsverarbeiter

9.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine schriftliche Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter im Sinne des Art. 28 Abs. 4 DSGVO. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage 3.

9.2 Beabsichtigt der Auftragsverarbeiter, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert er den Verantwortlichen mindestens 30 Tage vorher in Textform. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus einem wichtigen datenschutzrechtlichen Grund widersprechen.

9.3 Widerspricht der Verantwortliche, bemühen sich die Parteien um eine einvernehmliche Lösung. Kommt eine solche nicht zustande und kann der Auftragsverarbeiter die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht mit zumutbarem Aufwand erbringen, ist jede Partei berechtigt, den Hauptvertrag mit einer Frist von einem Monat zu kündigen.

9.4 Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten aus diesem Vertrag im Wesentlichen entsprechen. Er haftet dem Verantwortlichen gegenüber für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.

9.5 Nicht als Unterauftragsverarbeitung im Sinne dieser Ziffer gelten Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt, ohne dass diese bestimmungsgemäß auf personenbezogene Daten des Verantwortlichen zugreifen, etwa Telekommunikations- oder Reinigungsleistungen.

9.6 Soweit ein Unterauftragsverarbeiter personenbezogene Daten außerhalb der Europäischen Union verarbeitet, stellt der Auftragsverarbeiter sicher, dass ein zulässiges Übermittlungsinstrument nach Kapitel V DSGVO besteht, insbesondere ein Angemessenheitsbeschluss oder die Standardvertragsklauseln der Europäischen Kommission nebst erforderlichen ergänzenden Maßnahmen. Anlage 3 weist für jeden Unterauftragsverarbeiter den Verarbeitungsort und das jeweils genutzte Instrument aus.

9.7 Verbindet der Verantwortliche die Software mit Diensten Dritter, die er selbst ausgewählt hat (etwa ein eigenes Microsoft-Konto, ein eigenes Buchhaltungssystem oder die Bestell- und Katalogzugänge eigener Lieferanten), und weist er die Software dadurch an, Daten dorthin zu übermitteln, ist der

Dritte kein Unterauftragsverarbeiter des Auftragsverarbeiters. Die Übermittlung erfolgt auf dokumentierte Weisung nach Ziffer 3.1. Für die Rechtmäßigkeit der Übermittlung und die Beziehung zum Dritten ist der Verantwortliche verantwortlich. Zugangsdaten zu solchen Diensten speichert der Auftragsverarbeiter verschlüsselt und nutzt sie nur für die vom Verantwortlichen veranlasste Verbindung.

10. Nachweise und Überprüfung

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anforderung alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind.

10.2 Der Nachweis kann durch aktuelle Selbstauskünfte, durch die Beschreibung der Maßnahmen nach Anlage 2 oder durch Testate, Berichte oder Zertifikate unabhängiger Stellen erfolgen, auch soweit diese die eingesetzten Unterauftragsverarbeiter betreffen.

10.3 Genügen diese Nachweise im Einzelfall nicht, ermöglicht der Auftragsverarbeiter dem Verantwortlichen oder einem von diesem beauftragten, zur Verschwiegenheit verpflichteten und nicht mit dem Auftragsverarbeiter im Wettbewerb stehenden Prüfer Überprüfungen. Diese sind mit angemessener Vorlauffrist von mindestens 30 Tagen, während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und in der Regel höchstens einmal jährlich durchzuführen. Bei einem konkreten Anlass, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten, entfällt die Beschränkung auf eine jährliche Prüfung.

10.4 Der Auftragsverarbeiter kann den durch eine Überprüfung nach Ziffer 10.3 entstehenden Aufwand nach Ankündigung angemessen vergüten lassen, sofern die Überprüfung keinen vom Auftragsverarbeiter zu vertretenden Mangel aufdeckt.

11. Löschung und Rückgabe

11.1 Der Verantwortliche kann während der Vertragslaufzeit jederzeit die von ihm eingestellten Daten über die dafür vorgesehenen Exportfunktionen der Software abrufen. Dazu gehören die Sicherheits- und Protokolldaten nach Anlage 1 Abschnitt B, soweit sie noch gespeichert sind.

11.2 Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter die personenbezogenen Daten des Verantwortlichen nach dessen Wahl oder gibt sie zurück. Dabei gilt:
a) Der Verantwortliche kann bis zur Löschung jederzeit einen Export in einem gängigen, maschinenlesbaren Format abrufen (Ziffer 11.1). Nach Vertragsende stellt der Auftragsverarbeiter den Export auf Anforderung in Textform unverzüglich, spätestens innerhalb von 14 Tagen nach Zugang der Anforderung, bereit. Die Löschung ist bis dahin ausgesetzt.
b) Der Auftragsverarbeiter kündigt die Löschung spätestens am 70. Tag nach Vertragsende in Textform an die hinterlegten Adressen der Administratoren und an die Firmenadresse an. Die Ankündigung nennt den Löschtermin, den Umfang, die Möglichkeit zum Export, die Möglichkeit einer abweichenden Wahl (Rückgabe, spätere Löschung auf Weisung) und den Hinweis nach Ziffer 11.3.
c) Der Löschtermin liegt mindestens 14 Tage nach der Ankündigung und, vorbehaltlich einer Aussetzung nach Buchstabe a und Ziffer 11.3, spätestens am 90. Tag nach Vertragsende. Trifft der Verantwortliche bis dahin keine abweichende Wahl, gilt die Löschung als gewählt.
d) Für Betriebe, deren Hauptvertrag vor Inkrafttreten dieser Fassung endete,

liegt der Löschtermin mindestens 14 Tage nach der Ankündigung.
e) Der Auftragsverarbeiter bestätigt die Löschung nach Ziffer 11.5.

11.3 Gesetzliche Aufbewahrungspflichten für Unterlagen des Verantwortlichen, etwa nach § 147 der Abgabenordnung, § 257 des Handelsgesetzbuchs und § 14b des Umsatzsteuergesetzes, treffen den Verantwortlichen. Sie begründen für den Auftragsverarbeiter keine Pflicht, die Daten über den Löschtermin hinaus zu speichern (Art. 28 Abs. 3 Buchst. g DSGVO). Der Verantwortliche hat dafür zu sorgen, dass er seine aufbewahrungspflichtigen Unterlagen vor dem Löschtermin aus dem Export übernimmt und während der Frist lesbar und maschinell auswertbar vorhält. Will er, dass der Auftragsverarbeiter bestimmte Daten über das Vertragsende hinaus speichert, kann er dies vor dem Löschtermin in Textform anweisen; Umfang, Dauer und Vergütung regeln die Parteien dann gesondert. Befinden sich Daten des Verantwortlichen im Rahmen einer Außenprüfung nach § 147 Abs. 6 der Abgabenordnung beim Auftragsverarbeiter, teilt der Verantwortliche dies unverzüglich in Textform mit; die Löschung wird dann ausgesetzt, bis er sie freigibt. Unberührt bleiben Unterlagen, die der Auftragsverarbeiter in eigener Verantwortung zu seinem Vertrag mit dem Verantwortlichen aufbewahren muss: Abonnement-, Rechnungs- und Zahlungsbelege, der Nachweis der Zustimmung zu diesem Vertrag (Art. 5 Abs. 2 DSGVO) und ein Löschprotokoll ohne Inhalte. Diese Verarbeitung ist nicht Gegenstand dieses Vertrags.

11.4 Sicherungskopien werden nach den regulären Aufbewahrungszyklen der Sicherungssysteme überschrieben. Bis dahin bleiben sie gegen weitere Verarbeitung gesperrt.

11.5 Der Auftragsverarbeiter bestätigt die Löschung in Textform an die Adressen nach Ziffer 11.2 b).

12. Haftung

12.1 Für das Verhältnis der Parteien untereinander gelten die Haftungsregelungen des Hauptvertrags, soweit dieser Vertrag nichts Abweichendes bestimmt.

12.2 Art. 82 DSGVO bleibt unberührt.

13. Schlussbestimmungen

13.1 Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Das gilt auch für die Abbedingung dieses Formerfordernisses.

13.2 Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit es um die Verarbeitung personenbezogener Daten geht.

13.3 Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

13.4 Es gilt das Recht der Bundesrepublik Deutschland.

13.5 Mit seiner Annahme ersetzt dieser Vertrag mit Wirkung für die Zukunft die bisherige Fassung (2026-08-01) einschließlich ihrer Anlagen. Für die Zeit vor der Annahme bleibt die bisherige Fassung maßgeblich.

Anlagen

Anlage 1 — Gegenstand der Verarbeitung
Anlage 2 — Technische und organisatorische Maßnahmen (abrufbar unter /tom)
Anlage 3 — Unterauftragsverarbeiter (abrufbar unter /subprozessoren)

ANLAGE 1 — GEGENSTAND DER VERARBEITUNG

A. Kategorien betroffener Personen

- Beschäftigte des Verantwortlichen sowie für ihn tätige Personen, die die Software nutzen oder in ihr erfasst sind
- Kunden und Auftraggeber des Verantwortlichen sowie deren Ansprechpartner
- Lieferanten des Verantwortlichen sowie deren Ansprechpartner
- Inhaber und vertretungsberechtigte Personen des Verantwortlichen, soweit dessen Angaben, insbesondere die Bankverbindung, einen Personenbezug haben (etwa bei Einzelunternehmern)
- Interessenten und Anfragende des Verantwortlichen
- Sonstige Dritte, die auf Baustellenfotos abgebildet oder in Notizen, Aufträgen oder Sprachaufnahmen erwähnt sind

B. Kategorien personenbezogener Daten

- Konto- und Zugangsdaten: Name, E-Mail-Adresse, Rolle, Mitarbeiterkennung, Zeitpunkt der letzten Anmeldung, Angaben zur Zwei-Faktor-Authentifizierung
- Stammdaten der Kunden des Verantwortlichen: Anrede, Name, Firmierung, Anschriften, Telefonnummern, E-Mail-Adressen
- Auftrags- und Projektdaten: Beschreibungen, Termine, Zuweisungen, Status, Notizen, Aufgaben
- Arbeitszeitdaten: Beginn und Ende von Einsätzen, Pausen, Fahrtzeiten, Korrekturen
- Revisionsprotokoll der Arbeitszeiten: Änderungen an Beginn, Ende und Pause mit vorherigem und neuem Wert, Zeitpunkt, handelndem Konto und Begründung; keine automatische Löschfrist
- Abwesenheits- und Planungsdaten: Zeitraum und Art von Abwesenheiten der Beschäftigten (Urlaub, Schulung, sonstige Abwesenheit ohne Angabe eines Grundes) mit optionaler Kurznotiz; Tagesplanung mit geschätzten Fahrzeiten zwischen Einsatzadressen. Gesundheitsangaben sind nicht vorgesehen; an der Eingabe steht der Hinweis „Keine Gesundheitsangaben eintragen.“
- Standortdaten: einzelne, durch ausdrückliche Nutzerhandlung ausgelöste Koordinaten nebst Genauigkeitsangabe zur Präsenzprüfung am Einsatzort; keine fortlaufende Bewegungshistorie und keine Hintergrundortung
- Dokumentationsdaten: Fotos vom Einsatzort, Unterschriften auf Arbeitsnachweisen, Materialverbrauch
- Sprachdaten: bei aktiver Nutzung der Sprachfunktion die Aufnahme sowie das daraus erzeugte Transkript und die daraus abgeleiteten Vorschläge
- Sprachnachweise: auf Wunsch des Verantwortlichen gespeicherte Aufnahme, Rohtranskript und übernommene Angaben zu einem Einsatz (nur nach Freischaltung für den Betrieb); Aufbewahrungsdauer bestimmt der Verantwortliche, die Löschung einzelner Nachweise ist über die Software möglich
- Abrechnungsdaten: Angebote, Rechnungen, Positionen, Zahlungsstatus
- Zahlungs- und Mahndaten: Zahlungseingänge zu Rechnungen mit Betrag, Datum, Zahlungsart, freiwilliger Notiz und Kennung der erfassenden Person; Mahnstufe, Mahntag, Zahlungsfrist, Forderungsaufstellung (offener Betrag, Verzugszinsen, Pauschale), Mahntext und Versandstand. Bankverbindungen der Kunden werden nicht verarbeitet.
- Bankverbindung des Verantwortlichen: Kontoinhaber, IBAN und BIC, die auf Rechnungen, Mahnschreiben und E-Rechnungen ausgegeben werden; bei Einzelunternehmern personenbezogen

- Lieferanten- und Bestelldaten: Name des Lieferanten und Kundennummer bei diesem, E-Mail-Adresse für Bestellungen (in der Regel eine Geschäftsadresse), Text und Positionen der Bestellung sowie Versandstand
- Zugangsdaten des Verantwortlichen zu Shops, Katalogen und Schnittstellen seiner Lieferanten, die der Auftragsverarbeiter verschlüsselt speichert und nur für die vom Verantwortlichen veranlasste Verbindung nutzt
- Geräte- und Zustelldaten: Gerätekennung, Plattform, App-Version, Push-Token
- Versandprotokoll der E-Mails: Empfängeradresse, Zeitpunkt, Art des versendeten Dokuments (zum Beispiel Angebot, Rechnung, Arbeitsnachweis, Bestellung beim Lieferanten, Sicherheitshinweis), Nachrichtenkennung des Versanddienstes und Zustellstand (zugestellt, verzögert, unzustellbar, Beschwerde); keine automatische Löschfrist
- Sicherheits- und Protokolldaten: Anmeldungen, Abmeldungen und fehlgeschlagene Anmeldeversuche an Konten des Verantwortlichen, Änderungen von Passwort und E-Mail-Adresse, Bestätigung der E-Mail-Adresse, Zustellprobleme von Konto-E-Mails, vom Verantwortlichen ausgelöste Datenexporte sowie Änderungen der Bankverbindung (dabei nur die letzten vier Zeichen der IBAN und ein Fingerabdruck), jeweils mit Zeitpunkt, Konto, IP-Adresse und Browser- beziehungsweise Gerätekennung; Speicherdauer 90 Tage (Verarbeitung als eigener Verantwortlicher nach Ziffer 1.2; Bereitstellung an den Verantwortlichen nach Ziffer 11.1)
- Nutzungsereignisse: Ereignistyp, Modul, Kennung des betroffenen Datensatzes, handelndes Konto, Zeitpunkt, ohne Inhalte; Speicherdauer 180 Tage (Verarbeitung als eigener Verantwortlicher nach Ziffer 1.2; Bereitstellung an den Verantwortlichen nach Ziffer 11.1)

C. Besondere Kategorien personenbezogener Daten

Eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO ist nicht Gegenstand dieses Vertrags und von der Software nicht vorgesehen. Der Verantwortliche stellt sicher, dass solche Daten nicht in Freitextfeldern, Fotos oder Sprachaufnahmen erfasst werden.

D. Ort der Verarbeitung

Datenbank, Dateispeicher und Authentifizierungsdaten werden in der Europäischen Union gespeichert. Ein Zugriff durch den Auftragsverarbeiter oder seine Unterauftragsverarbeiter aus Drittländern ist nur nach Maßgabe der Ziffern 3.2 und 9.6 zulässig. Der Ort der Verarbeitung je Unterauftragsverarbeiter ergibt sich aus Anlage 3.

Anlage 2 — Technische und organisatorische Maßnahmen

Fassung 2026-11-23 · Prüfsumme SHA-256: fcc24bee3bd2d577c42374be0aa6f29a3be189d0f91a12ba66f1e0045e3f8db1

Anlage 2 zum Auftragsverarbeitungsvertrag
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Fassung 2026-11-23 · gültig ab 23. November 2026

Auftragsverarbeiter: HeWo Systems GbR, Elbchaussee 17, 22765 Hamburg

Vorbemerkung

HeWo wird als Software as a Service betrieben. Der Auftragsverarbeiter unterhält keine eigenen Rechenzentren. Datenbank, Authentifizierung und Dateispeicher werden bei Supabase betrieben, die Anwendung selbst bei Vercel. Die Maßnahmen zur physischen Sicherheit werden daher von diesen Unterauftragsverarbeitern erbracht und durch deren Zertifizierungen nachgewiesen; die Maßnahmen des Auftragsverarbeiters setzen auf dieser Ebene auf.

1. VERTRAULICHKEIT

1.1 Zutrittskontrolle

Der Auftragsverarbeiter betreibt keine eigenen Serverräume. Der physische Zutritt zu den verarbeitenden Systemen wird durch die in Anlage 3 genannten Infrastrukturdienstleister sichergestellt, die hierfür anerkannte Sicherheitsstandards einhalten und entsprechende Testate vorhalten.

1.2 Zugangskontrolle

- Jede nutzende Person besitzt ein eigenes, personenbezogenes Konto. Sammelkonten sind nicht vorgesehen.
- Kennwörter werden ausschließlich als Hashwert gespeichert; der Authentifizierungsdienst gibt Kennwörter zu keinem Zeitpunkt im Klartext aus.
- Bei der Vergabe von Kennwörtern wird serverseitig eine Mindestlänge von zwölf Zeichen erzwungen. Die Prüfung erfolgt bei Registrierung und bei jeder Kennwortvergabe über eine Einladung.
- Für Konten mit administrativen Rechten steht eine Zwei-Faktor-Authentifizierung per zeitbasiertem Einmalkennwort bereit. Administratoren, die sie nicht aktiviert haben, werden in der Anwendung dauerhaft darauf hingewiesen.
- Anmeldeversuche sind mengenmäßig begrenzt. Die Begrenzung wird serverseitig in der Datenbank geführt und lässt sich clientseitig nicht umgehen.
- Sitzungen werden über signierte, kurzlebige Token geführt, die serverseitig erneuert werden. Beim Abmelden werden lokale Daten des Geräts entfernt.
- Einladungen neuer Beschäftigter und Kennwort-Rücksetzungen erfolgen über einmalig verwendbare, zeitlich befristete Verweise.

1.3 Zugriffskontrolle

- Die Anwendung kennt ein abgestuftes Rollenmodell mit den Rollen Administrator, Büro und Monteur. Die Rolle bestimmt den Funktions- und Datenumfang.
- Der Zugriff auf Datensätze wird zusätzlich unmittelbar in der Datenbank durch zeilenbasierte Zugriffsregeln (Row Level Security) durchgesetzt. Diese wirken unabhängig von der Anwendungsschicht: Ein Zugriff, der die Anwendung umgeht, erhält dieselben Einschränkungen.
- Monteure sehen ausschließlich die ihnen zugewiesenen Aufträge sowie die eigenen Zeit- und Stammdaten.

- Dateien wie Fotos, Dokumente und Belege liegen in nicht öffentlich lesbaren Speicherbereichen. Der Abruf erfolgt über kurzlebige, signierte Verweise.
- Administrative Datenbankzugänge mit erweiterten Rechten sind auf eine abgegrenzte, im Quelltext nachvollziehbare Menge serverseitiger Endpunkte beschränkt und werden nie an Endgeräte ausgeliefert. Die Einhaltung wird vor jeder Übernahme einer Änderung in die Hauptlinie automatisiert geprüft.
- Zugangsschlüssel der Anwendung sind als Umgebungsvariablen der Betriebsumgebung hinterlegt und nicht Bestandteil des Quelltexts. Zugangsdaten für Wartungszugriffe auf die Produktivdatenbank liegen ausschließlich auf Arbeitsplatzrechnern der Gesellschafter.

1.4 Trennungskontrolle

- Die Anwendung ist mandantenfähig. Jeder Datensatz ist einem Betrieb zugeordnet; die Zuordnung wird durch die genannten zeilenbasierten Zugriffsregeln erzwungen.
- Automatisierte Tests laufen gegen lokale Testdatenbanken mit synthetischen Daten und eigenen Zugangsdaten. Zugriffe auf die Produktivumgebung erfolgen nur zu Betriebs- und Wartungszwecken.
- Für die Mandantentrennung bestehen automatisierte Tests, die vor jeder Übernahme einer Änderung in die Hauptlinie ausgeführt werden (Ziffer 4.2).

1.5 Pseudonymisierung und Datensparsamkeit

- Standortdaten werden ausschließlich als Einzelmessung nach ausdrücklicher Nutzerhandlung erhoben. Eine Hintergrundortung und eine fortlaufende Bewegungshistorie finden nicht statt.
- Sprachaufnahmen werden zur Auswertung an den in Anlage 3 genannten Dienst übertragen und nicht zum Training von Modellen verwendet. Eine dauerhafte Speicherung der Aufnahme beim Auftragsverarbeiter findet nur statt, wenn der Verantwortliche die Funktion „Sprachnachweis“ für seinen Betrieb ausdrücklich freigeschaltet hat. Sie ist standardmäßig ausgeschaltet.
- Das Sicherheitsprotokoll enthält Netzwerkadresse und Gerätekennung, weil beide zur Beweissicherung und zur Abwehr von Missbrauch benötigt werden. Es wird nach 90 Tagen automatisiert gelöscht und ist damit zeitlich eng begrenzt.
- Beim Nachweis der Vertragsannahme werden Netzwerkadresse und Gerätekennung ausschließlich als Hashwert gespeichert, da hier die Zuordnung zur Person bereits über das handelnde Konto gesichert ist.
- Technische Betriebsprotokolle sind so gestaltet, dass sie nach Möglichkeit keine Inhaltsdaten wie Kundentexte oder Transkripte enthalten.

2. INTEGRITÄT

2.1 Weitergabekontrolle

- Sämtliche Verbindungen zwischen Endgerät und Anwendung sowie zwischen Anwendung und Datenbank sind transportverschlüsselt nach dem Stand der Technik.
- Daten ruhen im Dateispeicher und in der Datenbank verschlüsselt.
- Die mobile Anwendung verschlüsselt Daten, die zur Offline-Nutzung auf dem Gerät vorgehalten werden, zusätzlich mit einem im gesicherten Schlüsselspeicher des Betriebssystems abgelegten Schlüssel.
- Zugangsdaten des Verantwortlichen zu Drittsystemen (Shops und Katalogschnittstellen seiner Lieferanten) werden ausschließlich verschlüsselt gespeichert (AES-256-GCM; der Schlüssel liegt in der Betriebsumgebung und nicht in der Datenbank). Sie sind nicht Bestandteil des Datenexports und werden mit den übrigen Daten des Verantwortlichen gelöscht.
- Ein Versand personenbezogener Daten auf Datenträgern findet nicht statt.

2.2 Eingabekontrolle

- Anlage, Änderung und Löschung fachlicher Datensätze werden dem handelnden Konto und dem Zeitpunkt nach nachvollziehbar gehalten, soweit die jeweilige Tabelle Zeitstempel und Akteurskennung führt. Änderungen an festgeschriebenen Rechnungen, Zahlungen und Mahnungen sind nur durch Gegenbuchung oder neue Version möglich und bleiben in der Historie sichtbar.
- Sicherheitsrelevante Ereignisse — Anmeldung, Abmeldung, fehlgeschlagene Anmeldung, Registrierung — werden mit Zeitpunkt, Konto, Netzwerkadresse und Gerätekennung protokolliert und nach 90 Tagen automatisiert gelöscht.
- Administrative Eingriffe über die Plattformverwaltung werden in einem gesonderten Protokoll erfasst, auf das ausschließlich der Betreiber Zugriff hat.
- Aufträge, Angebotsentwürfe und Rechnungsentwürfe, die der Verantwortliche löscht, werden zunächst in einen Papierkorb überführt und lassen sich von dort wiederherstellen, sodass irrtümliche Löschungen erkennbar und umkehrbar bleiben. Der Papierkorb hat keine automatische Frist; die Einträge bleiben dort, bis sie wiederhergestellt oder nach Ziffer 4.5 gelöscht werden. Das endgültige Entfernen einzelner Einträge erfolgt auf Einzelweisung nach Ziffer 3.1 des Vertrags.

2.3 Auftragskontrolle

- Unterauftragsverarbeiter werden nur nach vorheriger Prüfung eingesetzt und vertraglich auf entsprechende Pflichten verpflichtet. Die eingesetzten Stellen sind in Anlage 3 abschließend aufgeführt.
- Weisungen des Verantwortlichen werden in Textform entgegengenommen und dokumentiert.
- Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt; ausgenommen sind die Sicherheits- und Protokolldaten nach Ziffer 1.5 und 2.2 und die Nutzungsereignisse (Ziffer 1.2 des Vertrags).

3. VERFÜGBARKEIT UND BELASTBARKEIT

- Die Webanwendung wird auf einer mehrfach ausgelegten Infrastruktur des Anbieters betrieben. Die Datenbank wird durch den Infrastrukturdienstleister täglich automatisiert gesichert; eine Wiederherstellung ist auf den Stand der letzten Sicherung möglich.
- Die Sicherungen werden verschlüsselt und getrennt von den Produktivdaten aufbewahrt.
- Der Datenbankstand ist vollständig durch versionierte, im Versionsverwaltungs-system nachvollziehbare Migrationsskripte beschrieben und dadurch reproduzierbar.
- Die mobile Anwendung ist offlinefähig. Erfasste Daten verbleiben verschlüsselt auf dem Gerät, bis sie übertragen werden konnten; offene Übertragungen werden nicht allein wegen Zeitablaufs verworfen.
- Übertragungen sind gegen Doppelverarbeitung abgesichert, sodass ein Verbindungsabbruch nicht zu doppelten oder verlorenen Datensätzen führt.

4. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG

4.1 Datenschutz-Management

- Es besteht ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO.
- Es besteht ein dokumentierter Prozess zur Behandlung von Verletzungen des Schutzes personenbezogener Daten.
- Welche Daten automatisch, welche nur auf Weisung oder nach Vertragsende und welche nicht vorzeitig gelöscht werden, ist in Ziffer 4.5 beschrieben.

4.2 Sichere Softwareentwicklung

- Änderungen am Quelltext werden versionsverwaltet und vor Übernahme in die Produktivumgebung überprüft.
- Für die Mandantentrennung, die Rechteprüfung und den Zugriffsschutz der Schnittstellen bestehen automatisierte Tests. Vor jeder Übernahme einer Änderung in die Hauptlinie werden diese Tests sowie Prüfungen auf statische Sicherheitsmängel, versehentlich eingecheckte Zugangsdaten und bekannte Schwachstellen der Abhängigkeiten durch die Entwickler ausgeführt. Die Auslieferung an die Produktivumgebung erfolgt erst nach manueller Freigabe.
- Sicherheitsaktualisierungen der eingesetzten Bibliotheken werden zeitnah eingespielt.

4.3 Vorfallserkennung

- Auffällige Muster, insbesondere eine ungewöhnliche Häufung fehlgeschlagener Anmeldeversuche, lösen eine automatische Benachrichtigung der Betreiber aus.
- Meldungen über Sicherheitsmängel können jederzeit an kontakt@hewosystems.com gerichtet werden und werden vorrangig bearbeitet.

4.4 Überprüfung dieser Anlage

Diese Anlage wird mindestens jährlich sowie anlassbezogen bei wesentlichen Änderungen an der Verarbeitung überprüft und fortgeschrieben. Die jeweils geltende Fassung ist unter der in Anlage 3 genannten Adresse abrufbar.

4.5 Löschung und Aufbewahrung

Diese Ziffer beschreibt, was die Software von sich aus löscht, was nur auf Weisung oder nach Vertragsende gelöscht wird und was nicht vorzeitig gelöscht wird. Eine Löschung von Daten, die der Auftragsverarbeiter für den Verantwortlichen verarbeitet und die hier nicht aufgeführt ist, findet nicht automatisch statt.

a) Automatisch gelöscht werden

Ein täglicher Wartungslauf der Datenbank löscht ohne Zutun des Verantwortlichen:

- Ergebnisse der Standortprüfung am Einsatzort: 90 Tage nach der Prüfung
- Benachrichtigungen in der Anwendung: 90 Tage nach Erstellung
- das Sicherheitsprotokoll nach Ziffer 1.5 und 2.2: 90 Tage
- Zwischenstände von Aufträgen, die der Wiederherstellung dienen: 90 Tage
- Übertragungsbelege der mobilen Anwendung, sobald die Verarbeitung abgeschlossen ist: 90 Tage
- Protokoll versendeter Push-Erinnerungen: 90 Tage
- Nutzungsereignisse der Anwendung (Ereignistyp, Modul, Kennung des betroffenen Datensatzes, handelndes Konto, ohne Inhalte): 180 Tage
- Abwesenheiten der Beschäftigten in der Plantafel: 24 Monate nach dem letzten Tag der Abwesenheit, je Datensatz und in jedem Betrieb
- technische Zähler der Anfragebegrenzung: 1 Tag

Im selben Lauf werden außerdem gelöscht: Standortangaben an Baustellen-Nachweisen nach der vom Verantwortlichen gewählten Dauer (12, 24, 48 oder 60 Monate), das Begründungsprotokoll des Kalenderimports nach 30 Tagen und Dateien im Dateispeicher, zu denen kein Datensatz mehr besteht, nach 24 Stunden.

b) Nur auf Weisung oder nach Vertragsende gelöscht werden

- Daten, die der Verantwortliche über die Funktionen der Software selbst entfernt, etwa Materialeinträge, Abwesenheiten, Zuweisungen oder Beschäftigtenkonten ohne Vorgänge: sofort mit der Handlung. Beschäftigtenkonten mit Vorgängen werden deaktiviert, nicht gelöscht; der Name bleibt an den Vorgängen, solange eine Aufbewahrungspflicht des Verantwortlichen besteht. Nach Ablauf der Frist anonymisiert der Auftragsverarbeiter den Namen an den Vorgängen auf Einzelweisung des Verantwortlichen nach Ziffer 3.1 des Vertrags, und zwar innerhalb von 30 Tagen nach Zugang der Weisung.
- Aufträge, Angebotsentwürfe und Rechnungsentwürfe im Papierkorb: Der Papierkorb wird nicht automatisch geleert, und die Oberfläche der Software bietet keine Funktion, einzelne Einträge endgültig zu entfernen. Das endgültige Entfernen einzelner Einträge erfolgt auf Einzelweisung nach Ziffer 3.1 des Vertrags; im Übrigen werden die Einträge mit allen übrigen Daten nach Vertragsende gelöscht (vierter Spiegelstrich).
- Sonstige Daten, mit Ausnahme der unter c) genannten, auf dokumentierte Einzelweisung in Textform nach Ziffer 3.1 des Vertrags.
- Sämtliche Daten des Verantwortlichen, einschließlich der Dateien und der Anmeldekonten seiner Beschäftigten, nach Vertragsende: Der Auftragsverarbeiter löscht sie nach dem in Ziffer 11.2 des Vertrags beschriebenen Ablauf. Er bietet den Export an, kündigt die Löschung in Textform an und führt sie zu dem angekündigten Termin durch, spätestens am 90. Tag nach Vertragsende, vorbehaltlich einer Aussetzung nach Ziffer 11.2 a) und 11.3 des Vertrags.
- Sicherungskopien des Infrastrukturdienstleisters werden nach dessen regulären Zyklen überschrieben (Ziffer 11.4 des Vertrags).

c) Nicht vorzeitig gelöscht werden

- Finalisierte Rechnungen und Stornorechnungen sowie die dazugehörigen Belege: das ausgegebene Rechnungsdokument, die E-Rechnungs-Dateien, das Zahlungsjournal und versendete Mahnungen. Sie lassen sich in der Software nicht löschen und unterliegen keiner automatischen Löschfrist. Sie werden erst nach Vertragsende gelöscht, und zwar nach dem Ablauf unter b), vierter Spiegelstrich.

Die gesetzlichen Aufbewahrungspflichten für diese Unterlagen treffen den Verantwortlichen (Ziffer 11.3 des Vertrags). Der Auftragsverarbeiter führt für ihn keine Aufbewahrung durch, bietet ihm aber vor der Löschung den Export an.

Anlage 3 — Unterauftragsverarbeiter

Fassung 2026-11-23 · Prüfsumme SHA-256: 060aa20cb66e6637d793fab748d746e8078d61d6a59eed56786415c5562785b1

Anlage 3 zum Auftragsverarbeitungsvertrag
Verzeichnis der Unterauftragsverarbeiter

Fassung 2026-11-23 · gültig ab 23. November 2026

Auftragsverarbeiter: HeWo Systems GbR, Elbchaussee 17, 22765 Hamburg

Der Verantwortliche erteilt nach Ziffer 9.1 des Auftragsverarbeitungsvertrags die allgemeine Genehmigung zum Einsatz der nachfolgend aufgeführten Stellen. Vor der Hinzuziehung einer weiteren Stelle oder dem Austausch einer bestehenden wird der Verantwortliche mindestens 30 Tage vorher in Textform informiert und kann widersprechen.

1. INFRASTRUKTUR (IMMER EINGESETZT)

1.1 Supabase Pte. Ltd.
65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513
Leistung: Datenbank, Benutzerverwaltung und Authentifizierung, Dateispeicher für Fotos, Dokumente und Belege
Verarbeitete Daten: sämtliche in Anlage 1 genannten Kategorien
Verarbeitungsort: Speicherung in der Europäischen Union (Frankfurt am Main); Zugriff durch den Anbieter und seine Unterauftragsverarbeiter aus Drittländern möglich
Übermittlungsinstrument: Auftragsverarbeitungsvertrag des Anbieters (Teil der Nutzungsbedingungen) einschließlich der Standardvertragsklauseln der Europäischen Kommission

1.2 Vercel, Inc.
Leistung: Betrieb und Auslieferung der Webanwendung und der Programmierschnittstellen, technische Betriebsprotokolle
Verarbeitete Daten: Inhalte der jeweiligen Anfrage, Netzwerkadresse, Gerätekennung, technische Protokolldaten
Verarbeitungsort: Ausführung der Anwendung in Frankfurt am Main (Region fra1). Die Infrastruktur des Anbieters ist weltweit verteilt; eine Verarbeitung von Anfragedaten, Netzwerkadressen und technischen Protokolldaten in den Vereinigten Staaten von Amerika und anderen Staaten ist möglich.
Übermittlungsinstrument: Auftragsverarbeitungsvertrag des Anbieters einschließlich der Standardvertragsklauseln der Europäischen Kommission

1.3 Resend (Plus Five Five, Inc.)
Leistung: Versand von Konto- und Systemnachrichten, etwa Einladungen, Kennwort-Rücksetzungen, Benachrichtigungen und Sicherheitshinweisen an Administratoren (zum Beispiel bei einer Änderung der Bankverbindung); auf Wahl des Verantwortlichen außerdem Versand seiner Geschäftskorrespondenz an dessen Kunden, etwa Angebote, Rechnungen, Mahnungen, Auftragsunterlagen und Arbeitsnachweise, sowie von Bestellungen an dessen Lieferanten
Verarbeitete Daten: E-Mail-Adresse, Name, Inhalt der jeweiligen Nachricht, Zustellprotokoll mit Empfängeradresse und Zustellstand; bei Geschäftskorrespondenz zusätzlich die Angaben des jeweiligen Dokuments, insbesondere Anschrift sowie Auftrags-, Rechnungs- und Mahndaten der Kunden des Verantwortlichen; bei Bestellungen die E-Mail-Adresse des Lieferanten sowie Text und Positionen der Bestellung
Verarbeitungsort: Versand über Rechenzentrum in Irland; Verwaltungs- und Protokolldaten können in den Vereinigten Staaten von Amerika verarbeitet werden.

Die Übertragung an den Empfänger erfolgt ausschließlich transportverschlüsselt.
Übermittlungsinstrument: Auftragsverarbeitungsvertrag des Anbieters einschließlich der Standardvertragsklauseln der Europäischen Kommission

1.4 Functional Software, Inc. (Sentry)
45 Fremont Street, 8th Floor, San Francisco, CA 94105, Vereinigte Staaten von Amerika
Leistung: Erkennung und Auswertung von Programmfehlern und Abstürzen der Webanwendung und der mobilen Anwendung
Verarbeitete Daten: Fehlermeldung und technischer Ablaufpfad, Fassung und Baunummer der Anwendung, Art des Geräts und des Betriebssystems, Zeitpunkt, aufgerufener Pfad ohne Abfrageteil sowie gegebenenfalls eine pseudonyme Kennung des Benutzerkontos. Inhalte aus der Auftragsverarbeitung werden vor der Übermittlung nach Möglichkeit automatisiert entfernt. Namen in Freitexten von Fehlermeldungen lassen sich nicht in jedem Fall erkennen. Übermittelt werden keine E-Mail-Adressen, keine Zugangsmerkmale und keine Netzwerkadressen des Anwendungsnutzers.
Verarbeitungsort: Speicherung in der Europäischen Union (Rechenzentrum Frankfurt am Main); Zugriff durch den Anbieter aus den Vereinigten Staaten von Amerika möglich
Übermittlungsinstrument: Data Processing Amendment des Anbieters einschließlich der Standardvertragsklauseln der Europäischen Kommission
Speicherdauer: 30 Tage

2. OPTIONALE FUNKTIONEN (NUR BEI NUTZUNG)

2.1 Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland

Leistung: Sprach- und Textauswertung über den Azure OpenAI Service: Umwandlung gesprochener Angaben in strukturierte Auftragsdaten. Nur bei aktiver Nutzung der Sprachfunktion.
Verarbeitete Daten: Sprachaufnahme, Transkript, zur Zuordnung erforderlicher Ausschnitt des Materialkatalogs
Verarbeitungsort: Spracherkennung in Schweden; Textauswertung innerhalb der EU-Datenzone. Für begrenzte, vom Anbieter dokumentierte Betriebs-, Sicherheits- und Supportfälle ist eine Verarbeitung außerhalb der EU-Datengrenze möglich. Die Modelle arbeiten zustandslos; Eingaben und Ausgaben werden nicht zum Training verwendet.

Übermittlungsinstrument: Microsoft Products and Services Data Protection Addendum einschließlich der Standardvertragsklauseln der Europäischen Kommission, soweit erforderlich

2.2 Google Ireland Limited
Gordon House, Barrow Street, Dublin 4, Irland
Leistung: Zustellung von Push-Benachrichtigungen an Android-Geräte über Firebase Cloud Messaging. Nur nach Freigabe der Benachrichtigungen durch die nutzende Person.
Verarbeitete Daten: Push-Kennung des Geräts, Titel und Kurztext der Benachrichtigung
Verarbeitungsort: Europäische Union und Vereinigte Staaten von Amerika
Ein gesonderter Auftragsverarbeitungsvertrag liegt nicht vor; die Übermittlung der Push-Kennung an den Anbieter ist für die Zustellung auf dem Gerät technisch erforderlich.

2.3 Apple Distribution International Ltd.

Hollyhill Industrial Estate, Hollyhill, Cork, Irland
Leistung: Zustellung von Push-Benachrichtigungen an Geräte mit iOS über den Apple Push Notification service. Nur nach Freigabe der Benachrichtigungen durch die nutzende Person.
Verarbeitete Daten: Push-Kennung des Geräts, Titel und Kurztext der Benachrichtigung
Verarbeitungsort: Europäische Union und Vereinigte Staaten von Amerika
Ein gesonderter Auftragsverarbeitungsvertrag liegt nicht vor; die Übermittlung der Push-Kennung an den Anbieter ist für die Zustellung auf dem Gerät technisch erforderlich.

3. HINWEIS ZUR ABGRENZUNG

Für die Abwicklung des Abonnements zwischen dem Verantwortlichen und HeWo Systems GbR setzt HeWo den Zahlungsdienstleister Stripe (Stripe Payments Europe, Limited) ein. Dieser Dienst betrifft das Vertragsverhältnis der Parteien, nicht die Daten, die der Verantwortliche mit der Software verarbeitet. Insoweit ist HeWo Systems GbR selbst Verantwortliche, und der Dienst ist nicht als Unterauftragsverarbeitung aufgeführt. Einzelheiten enthält die Datenschutzerklärung.

Die Verbindung mit einem Microsoft-Konto des Verantwortlichen (Kalenderabgleich über Microsoft Graph, Anmeldung mit dem Microsoft-Konto) richtet sich nach Ziffer 9.7 des Vertrags; Microsoft ist insoweit kein Unterauftragsverarbeiter des Auftragsverarbeiters.

Ebenfalls nicht als Unterauftragsverarbeitung gelten Nebenleistungen ohne bestimmungsgemäßen Zugriff auf personenbezogene Daten des Verantwortlichen, etwa Telekommunikationsdienste.

4. AKTUALITÄT

Die jeweils geltende Fassung dieser Anlage ist unter https://app.hewosystems.com/subprozessoren abrufbar. Änderungen werden nach Ziffer 9.2 des Auftragsverarbeitungsvertrags vorab mitgeteilt.

Nutzungsbedingungen

Fassung 2026-10-18 · Prüfsumme SHA-256: 44d52eea30a09cd2e34aaad08627560bafc2a08f0994d0feab9c90fc8bd05f6c

Nutzungsbedingungen
Fassung vom 18. Oktober 2026

1. Geltungsbereich und Anbieter

Diese Nutzungsbedingungen gelten für die Nutzung der Software „HeWo“ (Web-Anwendung und mobile App) der HeWo Systems GbR, Bo Herzog und Lios Wolters, Elbchaussee 17, 22765 Hamburg (nachfolgend „Anbieter“). Sie gelten gegenüber Unternehmern im Sinne des § 14 BGB; die Software richtet sich nicht an Verbraucher. Vertragspartner des Anbieters ist der Betrieb (Unternehmer), für den das Konto angelegt wurde; er wird in diesen Bedingungen mit „Sie“ bezeichnet. „Nutzer“ sind Sie und die Beschäftigten, die die Software mit ihren Konten für Sie nutzen. Mit der Registrierung oder der ersten Nutzung erkennt der Nutzer diese Bedingungen an. Abweichende Bedingungen des Nutzers finden keine Anwendung, es sei denn, der Anbieter stimmt ihnen ausdrücklich schriftlich zu.

2. Vertragsgegenstand

Der Anbieter stellt eine cloudbasierte Software zur Planung, Durchführung, Dokumentation und Abrechnung von Handwerksaufträgen bereit. Umfang und Verfügbarkeit der Funktionen ergeben sich aus der jeweils gebuchten Leistungsbeschreibung beziehungsweise dem gewählten Tarif. Der Anbieter entwickelt die Software fortlaufend weiter und darf Funktionen ändern oder ergänzen, soweit der Vertragszweck dadurch nicht gefährdet wird.

3. Test- und Pilotzugänge

Test- und Pilotzugänge werden ausschließlich zur Erprobung der Software für den eigenen betrieblichen Bedarf eingeräumt. Sie sind zeitlich begrenzt, personengebunden und können vom Anbieter jederzeit ohne Angabe von Gründen widerrufen werden. Ein Anspruch auf Fortführung, Verfügbarkeit oder Übernahme von Testdaten in einen späteren Produktivbetrieb besteht nicht. Nach Ende des Testzeitraums darf der Anbieter die im Testzugang angelegten Daten löschen; er kündigt dies mindestens 14 Tage vorher in Textform an, und Sie können Ihre Daten bis dahin über die Exportfunktionen oder auf Anforderung bei uns abrufen. Die Weitergabe von Testzugängen an Dritte ist untersagt.

4. Vergütung, Laufzeit und Kündigung

Die Vergütung richtet sich nach dem bei Vertragsschluss gewählten Tarif. Alle Preise verstehen sich netto zuzüglich der gesetzlichen Umsatzsteuer. Zusätzlich gebuchte Zugänge und Zusatzleistungen werden nach der jeweils gültigen Preisliste berechnet.

Der Anbieter bietet zwei Laufzeitmodelle an. Im Jahrestarif beträgt die Laufzeit zwölf Monate; das Entgelt für die gesamte Laufzeit ist zu Beginn im Voraus fällig. Der Jahrestarif verlängert sich um jeweils weitere zwölf Monate, wenn er nicht bis zum Ende der laufenden Laufzeit gekündigt wird. Im Monatstarif beträgt die Laufzeit einen Monat; er ist jederzeit zum Ende des laufenden Abrechnungsmonats kündbar und verlängert sich andernfalls um jeweils einen weiteren Monat.

Die Kündigung erfolgt über die Abo-Verwaltung in der Anwendung und wird zum Ende des jeweils laufenden Abrechnungszeitraums wirksam. Bereits im Voraus gezahlte Entgelte werden bei einer Kündigung zum Laufzeitende nicht anteilig erstattet. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt für beide Seiten unberührt.

Ein Wechsel in einen höheren Tarif oder in den Jahrestarif ist während der Laufzeit möglich; der Anbieter rechnet die verbleibende Zeit des bisherigen Zeitraums anteilig an. Ein Wechsel in einen niedrigeren Tarif, in den Monatstarif oder eine Verringerung gebuchter Zugänge wird zum Ende des laufenden Abrechnungszeitraums wirksam.

Die Zahlung erfolgt über den Zahlungsdienstleister Stripe per Kreditkarte oder SEPA-Lastschrift. Gerät der Nutzer mit der Zahlung in Verzug, darf der Anbieter den Zugang nach vorheriger Ankündigung sperren, bis der offene Betrag ausgeglichen ist.

Elektronische Rechnung. Der Anbieter stellt Rechnungen elektronisch bereit, in der Regel als PDF-Datei per E-Mail oder über die Zahlungsseite des Zahlungsdienstleisters. Sie stimmen der Übermittlung elektronischer Rechnungen zu. Sobald das Gesetz für Rechnungen an Unternehmer eine elektronische Rechnung im strukturierten Format vorschreibt, stellt der Anbieter diese Rechnungen in diesem Format aus.

Entgeltänderung. Der Anbieter kann das Entgelt für eine künftige Laufzeit ändern. Er teilt Ihnen die beabsichtigte Änderung (Änderungsangebot) mindestens sechs Wochen vor dem Beginn der Laufzeit, für die das geänderte Entgelt gelten soll, in Textform mit und weist darauf hin, dass die Änderung nur gilt, wenn Sie ihr zustimmen. Sie stimmen zu, indem Sie das Änderungsangebot in der Anwendung bestätigen oder dem Anbieter Ihre Zustimmung in Textform mitteilen. Stimmen Sie nicht zu, bleibt es bis zum Ende der Laufzeit, die dem vorgeschlagenen Beginn vorausgeht, bei dem bisherigen Entgelt; der Vertrag verlängert sich danach nicht. Das Entgelt für eine bereits laufende, im Voraus bezahlte Laufzeit bleibt unverändert. Änderungen der gesetzlichen Umsatzsteuer geben wir weiter.

5. Zugangsdaten und Konten

Konten sind personengebunden. Der Nutzer hält seine Zugangsdaten geheim, schützt sie vor dem Zugriff Dritter und informiert den Anbieter unverzüglich bei Verdacht auf Missbrauch. Handlungen, die über ein Konto vorgenommen werden, werden dem jeweiligen Kontoinhaber zugerechnet. Die gemeinsame Nutzung eines Kontos durch mehrere Personen ist nicht gestattet.

6. Zulässige Nutzung

Die Nutzung ist ausschließlich im Rahmen des bestimmungsgemäßen Gebrauchs für eigene betriebliche Zwecke des Nutzers beziehungsweise seines Betriebs gestattet. Der Nutzer stellt sicher, dass die von ihm eingegebenen Inhalte keine Rechte Dritter verletzen und nicht gegen geltendes Recht verstoßen.

7. Verbotene Handlungen

Untersagt sind insbesondere:

- das Zurückentwickeln, Dekompilieren, Disassemblieren oder sonstige Analysieren der Software oder ihrer Bestandteile (Reverse Engineering), soweit nicht zwingendes Recht (§ 69e UrhG) dies erlaubt;
- das automatisierte Auslesen, Abgreifen oder Kopieren von Inhalten, Daten, Oberflächen oder Schnittstellen (Scraping, Crawling, Bots), einschließlich der systematischen Erfassung der Benutzeroberfläche durch Screenshots, Bildschirmaufnahmen oder KI-gestützte Auswertung;
- die Nutzung der Software oder von Erkenntnissen aus ihr zum Zweck des Leistungsvergleichs (Benchmarking) für die Entwicklung, Verbesserung oder Vermarktung eines konkurrierenden Produkts;
- die vollständige oder teilweise Nachbildung der Software, ihrer Abläufe, Datenmodelle oder Benutzeroberfläche für kommerzielle Zwecke;
- das Umgehen oder Testen von Sicherheitsmechanismen, Zugriffskontrollen oder Nutzungsgrenzen ohne vorherige schriftliche Zustimmung des Anbieters;
- die Überlassung, Vermietung oder Unterlizenzierung des Zugangs an Dritte.

8. Schutzrechte

Sämtliche Rechte an der Software, ihrem Quellcode, ihrer Benutzeroberfläche, ihren Datenbanken, Marken, Logos und Inhalten stehen dem Anbieter zu. Der Nutzer erhält ein einfaches, nicht übertragbares, auf die Vertragslaufzeit beschränktes Nutzungsrecht. Die von Ihnen eingegebenen Daten bleiben Ihre Daten. Der Anbieter verarbeitet personenbezogene Daten in Ihrem Auftrag nach dem Auftragsverarbeitungsvertrag; für seine eigenen Verarbeitungen gilt die Datenschutzerklärung.

9. Protokollierung und Sperrung

Der Anbieter protokolliert sicherheitsrelevante Ereignisse (etwa An- und Abmeldungen sowie fehlgeschlagene Anmeldeversuche) gemäß der Datenschutzerklärung, um Missbrauch zu erkennen und die Sicherheit des Dienstes zu gewährleisten. Bei einem Verstoß gegen diese Bedingungen, insbesondere gegen Ziffer 7, darf der Anbieter den Zugang nach Abwägung der Interessen vorübergehend sperren oder außerordentlich kündigen. Weitergehende Ansprüche, insbesondere auf Unterlassung und Schadensersatz, bleiben vorbehalten.

10. Verfügbarkeit, Wartung und Haftung

10.1 Der Anbieter stellt die Software über das Internet bereit und bemüht sich um einen möglichst störungsfreien Betrieb. Eine bestimmte prozentuale Verfügbarkeit wird nicht zugesagt; für Testzugänge wird keine Verfügbarkeit zugesagt.

10.2 Planbare Wartungsarbeiten führt der Anbieter nach Möglichkeit werktags zwischen 22:00 und 06:00 Uhr oder an Sonn- und Feiertagen durch. Wartungen, die die Nutzung voraussichtlich länger als 30 Minuten einschränken, kündigt er mindestens 24

Stunden vorher in der Anwendung oder per E-Mail an. Dringende Wartungen, etwa zur Abwehr einer Sicherheitslücke, darf er jederzeit vornehmen; er hält sie so kurz wie möglich.

10.3 Störungen, die Sie dem Anbieter unter kontakt@hewosystems.com melden, bearbeitet er an Werktagen in der Regel binnen eines Werktags nach Eingang der Meldung.

10.4 Ihre gesetzlichen Rechte bei Mängeln der Software bleiben unberührt. Zeiten, in denen die Software wegen höherer Gewalt oder wegen Ihrer Internetverbindung, Ihrer Geräte oder von Ihnen eingebundener Dienste Dritter nicht nutzbar ist, gelten nicht als Mangel der Software.

10.5 Der Anbieter haftet unbeschränkt für Vorsatz und grobe Fahrlässigkeit sowie bei Verletzung von Leben, Körper oder Gesundheit. Bei einfacher Fahrlässigkeit haftet der Anbieter nur für die Verletzung wesentlicher Vertragspflichten (Kardinalpflichten), begrenzt auf den vertragstypischen, vorhersehbaren Schaden. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt. Für Testzugänge gilt zusätzlich: Sie werden unentgeltlich bereitgestellt; die Haftung richtet sich insoweit nach den gesetzlichen Regeln für unentgeltliche Leistungen.

11. Änderungen dieser Bedingungen

11.1 Der Anbieter kann diese Bedingungen mit Wirkung für die Zukunft nur mit Ihrer Zustimmung ändern; für Änderungen des Entgelts gilt ausschließlich Ziffer 4. Der Anbieter teilt Ihnen die Änderung mindestens sechs Wochen vor dem vorgeschlagenen Zeitpunkt in Textform mit und nennt die geänderten Klauseln. Sie stimmen in der Anwendung oder in Textform zu. Ohne Ihre Zustimmung gelten die bisherigen Bedingungen weiter.

11.2 Ohne Ihre Zustimmung darf der Anbieter nur Änderungen vornehmen, die wegen einer Änderung des Gesetzes oder einer bindenden behördlichen oder gerichtlichen Entscheidung zwingend erforderlich sind oder die lediglich Schreibfehler und Verweise berichtigen, ohne Rechte und Pflichten zu ändern. Er informiert Sie darüber in Textform.

11.3 Stimmen Sie einer Änderung nach 11.1 nicht zu, kann der Anbieter den Vertrag mit einer Frist von drei Monaten zum Ende einer Laufzeit kündigen.

12. Datenexport und Vertragsende

Sie können Ihre Daten während der Laufzeit über die Exportfunktionen der Software abrufen. Nach Vertragsende löschen wir Ihre Daten nach Ziffer 11 des Auftragsverarbeitungsvertrags und bieten Ihnen vorher einen Export an. Unterlagen, die Sie nach Steuer- und Handelsrecht aufbewahren müssen, müssen Sie vor der Löschung exportieren und selbst vorhalten.

13. Schlussbestimmungen

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit der Nutzung ist, soweit gesetzlich zulässig, Hamburg. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.