Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Version: 2026-11

Die Vertragsparteien sind:

Nutzer der Handwerkersoftware Hawepro

– im Folgenden: Auftraggeber – und

Hawepro, Marco Bullin, Emseloher Schulgasse 9, 06542 Allstedt

– im Folgenden: Auftragnehmer –

schließen folgenden Vertrag zur Auftragsverarbeitung.

1. Gegenstand und Dauer der Vereinbarung

Gegenstand sind alle Arten personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet. Folgende Daten werden vom Auftragnehmer verarbeitet:

- Personendaten (z. B. Name, Adresse)
- Kommunikationsdaten (z. B. Telefon, Fax, E-Mail)
- Vertragsstammdaten (z. B. Abrechnungs- und Zahlungsinformationen, Bankverbindung)
- Nutzungsdaten (z. B. Steuernummern)
- Sprachdaten (nur bei Nutzung der Diktierfunktion, siehe Anlage 2)

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag wird auf unbestimmte Zeit geschlossen.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Alle Arten von Verarbeitungen von Daten im Sinne der DS-GVO werden umfasst. Der Zweck der Verarbeitung ist die Erfüllung der vertraglich vereinbarten Leistung. Die Art zur Erfüllung unserer Leistung ist:

- Bereitstellung von IT-Infrastruktur sowie die Speicherung und Sicherung der Daten über die im Internet angebotenen Dienste (Cloud-Dienste) des Auftragnehmers.
- Wartung und Support per Fernwartungssoftware, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann.
- Bereitstellung KI-gestützter Funktionen (derzeit: KI-Angebotsassistent einschließlich Diktierfunktion) gemäß Anlage 2. Diese Verarbeitung findet nur statt, wenn der Auftraggeber die Funktion selbst aufruft.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

- Vorname
- Nachname
- Firmenname
- Anschrift
- Telefonnummer / Fax
- E-Mail-Adresse
- Sprachaufnahmen und daraus erkannter Text (nur bei Nutzung der Diktierfunktion)

Wir speichern die eingetragenen Kundendaten des Auftraggebers in einer verschlüsselten Datenbank in Rechenzentren in Frankfurt am Main (Deutschland). Der KI-Angebotsassistent nach Anlage 2 wird in einem Rechenzentrum in Irland (EU) verarbeitet, die Diktierfunktion in einem Rechenzentrum in Frankfurt am Main (Deutschland). Diese Kundendaten werden ausschließlich vom Auftraggeber verwendet, um seine Angebote und Rechnungen erstellen zu können.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- Unternehmen
- Privatpersonen
- Kunden
- Interessenten
- Vertreter
- Lieferanten des Auftraggebers
- Mitarbeiter des Auftraggebers und deren Ansprechpartner

Die Laufzeit dieser Auftragsverarbeitungsvereinbarung richtet sich nach der Laufzeit des Vertrags zur Leistungserbringung. Ergeben sich aus den Bestimmungen dieser

Vereinbarung darüber hinausgehende Verpflichtungen, verlängern sich die Vereinbarungen aus diesem Vertrag um die dafür nötige Dauer.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Pflichten

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Das Aufrufen einer Funktion der Software durch den Auftraggeber gilt als Weisung zur damit verbundenen Verarbeitung.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

Rechte

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Weisungsempfänger beim Auftragnehmer ist: Marco Bullin, Emseloher Schulgasse 9, 06542 Allstedt.

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

4. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Dies gilt ausdrücklich auch für KI-gestützte Funktionen: Die Daten werden weder vom Auftragnehmer noch von dessen Unterauftragnehmern zum Training von KI-Modellen verwendet. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt; ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt (logisch) getrennt werden.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

- Regelmäßige Sicherheitsüberprüfungen der Software.
- Datenschutzkonforme Löschung der Daten nach Beendigung der Laufzeit.
- Sicherung der Datenträger mit einer aktuellen Verschlüsselung.
- Datenträger, Unterlagen sowie sämtliche sonstigen Materialien werden nach Vertragsende auf Verlangen des Auftraggebers entweder herausgegeben oder gelöscht.

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach

Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.
Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

Sofern einschlägig: Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

Anfragen betroffener Personen

Der Auftragnehmer wird betroffene Personen, die sich mit Forderungen zur Löschung, Berichtigung oder Auskunft an den Auftragnehmer wenden, an den Auftraggeber verweisen, sofern eine Zuordnung zum Auftraggeber möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter und unterstützt ihn im Rahmen seiner Möglichkeiten auf Weisung, soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

5. Möglichkeiten zum Nachweis

Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis kann der Auftragnehmer dem Auftraggeber folgende Informationen zur Verfügung stellen:

- Ergebnisse durchgeführter Sicherheitsüberprüfungen (Security-Audits)
- Interne Verhaltensregeln und die Beschreibung der technischen und organisatorischen Maßnahmen
- Zertifikate der eingesetzten Rechenzentrums- und Cloud-Anbieter zu Datenschutz und Informationssicherheit (z. B. ISO 27001, ISO 27017, ISO 27018, SOC 2)
- Weitere Informationen zur Informationssicherheit unter https://hawepro.de/sicherheit

Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten des Auftragnehmers ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt.

Der Auftragnehmer kann diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und dem Abschluss einer Verschwiegenheitsvereinbarung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

Der Auftragnehmer hat ein Einspruchsrecht gegenüber einem vom Auftraggeber beauftragten Prüfer, der in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

Der Auftragnehmer darf für die Unterstützung bei der Durchführung einer Inspektion eine angemessene Vergütung verlangen, sofern dies im Vertrag zur Leistungserbringung nicht anders vereinbart wurde. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

Sollte eine Inspektion durch eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde vorgenommen werden, gilt grundsätzlich Abs. 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsvereinbarung ist nicht erforderlich, sofern die Aufsichtsbehörde einer gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach StGB strafbewehrt ist.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Der Auftragnehmer ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragnehmern berechtigt. Mit Abschluss dieser Vereinbarung stimmt der Auftraggeber dem Einsatz der in Anlage 1 aufgeführten Unterauftragnehmer zu. Beabsichtigt der Auftragnehmer den Einsatz weiterer oder anderer Unterauftragnehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form mitteilen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Unterauftragnehmer nicht eingesetzt werden. Die Zustimmung kann auch elektronisch innerhalb der Software erteilt werden.

Unterauftragnehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

Sämtliche Verträge zwischen Auftragnehmer und Unterauftragnehmer müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO im Betrieb des Unterauftragnehmers. Bei Unterauftragnehmern, die standardisierte Vertragsbedingungen verwenden (z. B. große Cloud-Anbieter), werden deren Auftragsverarbeitungsbedingungen (Data Processing Addendum) zugrunde gelegt; die Kontroll- und Weisungsrechte des Auftraggebers werden in diesem Fall über die vom Unterauftragnehmer bereitgestellten Prüfberichte und Zertifikate ausgeübt. Der Auftragnehmer ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Unterauftragnehmers zu erteilen und die entsprechenden Vertragsunterlagen oder Prüfberichte zur Verfügung zu stellen.

Der Auftragnehmer ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragnehmer verantwortlich. Er haftet gegenüber dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

Die Beauftragung von Unterauftragnehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DS-GVO gegeben sind und der Auftraggeber zugestimmt hat.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Hosting

Die Software läuft auf Infrastruktur von Amazon Web Services (AWS) in deren Rechenzentren in Frankfurt am Main (Deutschland). KI-gestützte Funktionen nach Anlage 2 werden über den AWS-Dienst Amazon Bedrock in einem Rechenzentrum in Irland (EU) verarbeitet. Die Diktierfunktion nach Anlage 2 wird über den AWS-Dienst Amazon Transcribe in einem Rechenzentrum in Frankfurt am Main (Deutschland) verarbeitet. AWS stellt eine etablierte Sicherheitsinfrastruktur, Backups, Protokollierung und Überwachung bereit und erfüllt unter anderem die Standards ISO 27001, ISO 27017, ISO 27018, SOC 2 und SOC 3.

Weitere eingesetzte Dienste

Die zur Leistungserbringung eingesetzten Unterauftragnehmer sind in Anlage 1 aufgeführt.

Zugangs- und Zugriffskontrolle

Der Zugriff auf die Software ist ausschließlich mit einem gültigen Benutzerkonto möglich. Passwörter werden ausschließlich als “salted” Hashwerte (bcrypt) gespeichert und niemals im Klartext; sie können daher auch vom Auftragnehmer nicht wiederhergestellt werden. Bei Registrierung wird eine Mindestlänge des Passworts vorgegeben. Zusätzlich ist eine Zwei-Faktor-Authentifizierung via E-Mail aktiv. Optional kann eine andere Zwei-Faktor-Authentifizierungen aktiviert werden. Die Anmeldung erfolgt über signierte, zeitlich begrenzt gültige Zugriffstoken (JSON Web Token); diese enthalten kein Passwort. Bei Missbrauch können Benutzer kurzfristig gesperrt werden. Die Daten verschiedener Auftraggeber sind logisch voneinander getrennt; jeder Zugriff wird auf den Datenbestand des jeweiligen Auftraggebers beschränkt.

Pseudonymisierung

Es findet keine Pseudonymisierung statt. Pseudonymisierung bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z. B. Verwendung von Fantasienamen).

Verschlüsselung

Die gesamte Kommunikation zwischen dem Auftraggeber, Hawepro und den Servern erfolgt verschlüsselt über HTTPS (TLS). Bei der Diktierfunktion wird die Sprache über eine verschlüsselte WebSocket-Verbindung (TLS) direkt aus dem Browser an Amazon Transcribe übertragen. Die gespeicherten Daten in der Datenbank und in den Datensicherungen sind mit dem Industriestandard AES-256 verschlüsselt (Encryption at Rest). Zur Verarbeitung werden die Daten innerhalb der gesicherten Systeme entschlüsselt.

Anwendungssicherheit

Eingaben werden serverseitig validiert und begrenzt. Datenbankabfragen werden parametrisiert ausgeführt, um Injection-Angriffe zu verhindern. Das Frontend (ReactJS) schützt in Kombination mit tokenbasierter Authentifizierung vor üblichen Bedrohungen wie Cross-Site-Scripting (XSS) und Cross-Site-Request-Forgery (CSRF). Anfragen werden zur Abwehr von Missbrauch mengenmäßig begrenzt (Rate-Limiting).

Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Backup-Konzepte (regelmäßige, verschlüsselte Datensicherungen)
- Recovery-Konzepte (dokumentierte Wiederherstellungsverfahren)

Überprüfung, Evaluierung und Anpassung der Maßnahmen

Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis wird dem Auftraggeber auf Anfrage mitgeteilt.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DS-GVO)

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z. B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragnehmers in geeigneter Weise zu überprüfen.

10. Datengeheimnis und Vertraulichkeit

Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z. B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragnehmer bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen. Der Auftragnehmer wird die Einhaltung dieser Maßnahmen in geeigneter Weise dokumentieren und die Dokumentation dem Auftraggeber auf Verlangen vorlegen.

11. Informationspflichten, Schriftform, Rechtswahl

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber darüber umgehend zu informieren. Der Auftragnehmer hat alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DS-GVO liegen.

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile, einschließlich etwaiger Zusicherungen durch den Auftragnehmer, bedürfen der Schriftform. Diese kann auch in elektronischer Form (z. B. Webformular, E-Mail oder Zustimmung innerhalb der Software) erfolgen und muss einen ausdrücklichen Hinweis darauf enthalten, dass es sich um eine Änderung oder Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrags zur Leistungserbringung vor. Es gilt deutsches Recht.

12. Haftung und Schadenersatz

Eine zwischen den Parteien im Vertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, sofern nicht ausdrücklich etwas Abweichendes vereinbart wurde. Soweit keine Haftungsregelung vereinbart wurde, haften Auftraggeber und Auftragnehmer gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelungen.

13. Schlussbestimmungen

Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

Sollte sich die DS-GVO oder sonstige in Bezug genommene gesetzliche Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil:

- Anlage 1: Unterauftragnehmer
- Anlage 2: KI-Angebotsassistent und Diktierfunktion

Anlage 1: Unterauftragnehmer

Mit Zustimmung zu dieser Vereinbarung stimmt der Auftraggeber dem Einsatz folgender Unterauftragnehmer zu. Eine Übermittlung in Drittländer findet nicht statt.

Unterauftragnehmer	Leistung	Standort der Verarbeitung	Hinweis
Amazon Web Services EMEA SARL, Luxemburg	Hosting, Datenspeicherung, Datensicherung, E-Mail-Versand	Frankfurt am Main (Deutschland)	–
Amazon Web Services EMEA SARL, Luxemburg	KI-Verarbeitung (Amazon Bedrock) für den KI-Angebotsassistenten	Irland (EU)	nur bei Nutzung der Funktion, siehe Anlage 2
Amazon Web Services EMEA SARL, Luxemburg	Spracherkennung (Amazon Transcribe) für die Diktierfunktion des KI-Angebotsassistenten	Frankfurt am Main (Deutschland)	nur bei Nutzung der Diktierfunktion, siehe Anlage 2
MongoDB Deutsche GmbH	Datenbankbetrieb (MongoDB Atlas)	Frankfurt am Main (Deutschland)	–

Anlage 2: KI-Angebotsassistent und Diktierfunktion

Mit Zustimmung zu dieser Vereinbarung (ab Version 2026-10) erlaubt der Auftraggeber dem Auftragnehmer, für die Funktion „Angebot mit KI befüllen“ den Unterauftragnehmer Amazon Web Services EMEA SARL (Dienst Amazon Bedrock, Rechenzentrum Irland, EU) einzusetzen.

Verarbeitet werden ausschließlich bei Nutzung der Funktion:

- die vom Auftraggeber eingegebene Auftragsbeschreibung,
- Auszüge aus seinen Stammdaten (Bezeichnung, Einheit, Kurzbeschreibung),
- zur Kundenzuordnung Name, Kundennummer, PLZ und Ort passender Kunden.

Zweck ist die Erstellung eines Angebotsentwurfs, den der Auftraggeber vor der Verwendung prüft. Die Daten werden nicht zum Training von KI-Modellen verwendet und nicht in Drittländer übermittelt. Der Auftragnehmer speichert die Auftragsbeschreibung nicht; der erzeugte Entwurf wird nach dem Abruf gelöscht, spätestens nach einer Stunde.

Die Verarbeitung findet ausschließlich statt, wenn der Auftraggeber die Funktion „Angebot mit KI befüllen“ selbst aufruft; das Aufrufen gilt als Weisung im Sinne von Ziff. 3. Nutzt der Auftraggeber die Funktion nicht, werden keine Daten an diesen Dienst übermittelt.

Diktierfunktion

Mit Zustimmung zu dieser Vereinbarung ab Version 2026-11 erlaubt der Auftraggeber dem Auftragnehmer, für die Diktierfunktion des KI-Angebotsassistenten den Unterauftragnehmer Amazon Web Services EMEA SARL (Dienst Amazon Transcribe, Rechenzentrum Frankfurt am Main, Deutschland) einzusetzen.

Verarbeitet werden ausschließlich bei Nutzung der Diktierfunktion:

- die Sprache der diktierenden Person, die schon während des Sprechens verschlüsselt und direkt aus dem Browser an den Dienst übertragen wird,
- der daraus erkannte Text, den der Dienst an den Browser des Auftraggebers zurückgibt.

Zweck ist die Umwandlung der gesprochenen Auftragsbeschreibung in Text, den der Auftraggeber vor der weiteren Verwendung prüft. Der erkannte Text wird anschließend wie eine eingetippte Auftragsbeschreibung verarbeitet. Eine Identifizierung von Personen anhand ihrer Stimme findet nicht statt. Die Daten werden nicht zum Training von KI-Modellen verwendet und nicht in Drittländer übermittelt. Der Auftragnehmer speichert weder den Ton noch den erkannten Text; er speichert nur einen Zähler der gestarteten Diktate je Auftraggeber und Tag, der nach zwei Tagen gelöscht wird.

Der Auftraggeber stellt sicher, dass nur die eigene Auftragsbeschreibung eingesprochen wird und keine Gespräche mit anderen Personen erfasst werden.

Die Verarbeitung findet ausschließlich statt, wenn der Auftraggeber die Diktierfunktion selbst startet; das Starten gilt als Weisung im Sinne von Ziff. 3. Nutzt der Auftraggeber die Diktierfunktion nicht, werden keine Daten an diesen Dienst übermittelt.