Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Rechtstexte sind nur in deutscher Sprache verbindlich.

zwischen

dem Kunden gemäß Registrierung bzw. Nutzungsvertrag über SolvePlus (S+)
– nachfolgend „Auftraggeber“ (Verantwortlicher) –

und

SolveITKL, Inhaber Nirojh Sritharan (Einzelunternehmen), Burgherrenstraße 9B, 67661 Kaiserslautern; Niederlassung/Büro: Maxstraße 7, 67659 Kaiserslautern; Telefon 0631 41436555, E-Mail info@solve-it-kl.de, USt-IdNr. DE320975603
– nachfolgend „Auftragnehmer“ (Auftragsverarbeiter) –

§ 1 Gegenstand, Dauer, Art und Zweck

(1) Der Auftragnehmer stellt dem Auftraggeber die Software SolvePlus (S+) als Software-as-a-Service bereit (Hauptvertrag: Nutzungsvertrag nach den AGB von S+). Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand, Art und Zweck der Verarbeitung, Art der Daten und Kategorien betroffener Personen ergeben sich aus Anlage 1.

(2) Dieser Vertrag gilt für die Dauer des Hauptvertrags. Er endet nicht, solange der Auftragnehmer noch Daten des Auftraggebers verarbeitet, insbesondere bis zur Rückgabe und Löschung nach § 10.

(3) Dieser Vertrag gilt nicht für Daten, die der Auftragnehmer als eigener Verantwortlicher verarbeitet, z. B. Vertrags-, Registrierungs- und Abrechnungsdaten des Auftraggebers, Sicherheitsprotokolle der Plattform sowie die Nachweise über den Abschluss dieses Vertrags. Hierzu informiert die Datenschutzerklärung.

§ 2 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf Übermittlungen in ein Drittland, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats dazu verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen sind in diesem Vertrag und im Hauptvertrag festgelegt. Weitere Weisungen erteilt der Auftraggeber durch die Nutzung und Einstellung von S+, z. B. durch das Erfassen und Löschen von Daten, das Einschalten von Modulen, Anbindungen, Benachrichtigungskanälen, KI-Funktionen und Partner-Apps sowie durch Freigaben. Einzelweisungen erteilt er in Textform an info@solve-it-kl.de. Weisungsberechtigt sind die im Mandanten als Inhaber bzw. Admin hinterlegten Personen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 UAbs. 2 DSGVO). Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

§ 3 Vertraulichkeit

(1) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung gilt auch nach Ende ihrer Tätigkeit fort.

(2) Der Auftragnehmer greift auf Daten des Auftraggebers nur zu, soweit das für Betrieb, Support, Störungsbeseitigung und Sicherheit erforderlich ist. Für Support nutzt er ein eigenes Technik-Konto im Mandanten, das sich nur über einen kurzlebigen Einmal-Link anmelden kann und das der Auftraggeber in S+ sperren kann. Anmeldungen und Änderungen des Auftragnehmers werden im Protokoll des Mandanten vermerkt.

(3) Der Auftragnehmer nutzt die Daten nicht für eigene Zwecke. Kopien erstellt er nur, soweit das für die vertragsgemäße Leistung erforderlich ist, insbesondere für Datensicherungen.

§ 4 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO).

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie weiterentwickeln und durch gleichwertige Maßnahmen ersetzen, soweit das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.

§ 5 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt die allgemeine schriftliche Genehmigung, Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 Teil A aufgeführt und gelten als genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen vorher in Textform (z. B. per E-Mail oder Hinweis in S+) über jede beabsichtigte Hinzuziehung oder Ersetzung eines

Unterauftragsverarbeiters. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Einigen sich die Parteien nicht, kann der Auftraggeber den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten wie in diesem Vertrag (Art. 28 Abs. 4 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Einhaltung.

(4) Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere bei einem Angemessenheitsbeschluss (z. B. EU-US Data Privacy Framework für zertifizierte Empfänger) oder geeigneten Garantien wie Standardvertragsklauseln.

(5) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind Dienste, die der Auftraggeber selbst mit eigenem Konto anbindet oder durch seine Einstellungen als Empfänger bestimmt (Anlage 3 Teil B). Für diese schließt der Auftraggeber die erforderlichen Verträge selbst ab und prüft die Zulässigkeit einer Drittlandübermittlung in eigener Verantwortung. Ebenfalls keine Unterauftragsverarbeitung sind Nebenleistungen ohne Zugriff auf personenbezogene Daten, z. B. Telekommunikationsleistungen.

§ 6 Unterstützung bei Betroffenenrechten

(1) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 lit. e DSGVO), insbesondere Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit. S+ stellt dafür Funktionen zum Anzeigen, Ändern, Exportieren, Archivieren und Löschen bereit, z. B. die Kontolöschung einzelner Personen.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter. Er beantwortet sie nicht selbst, es sei denn, der Auftraggeber weist ihn dazu an.

§ 7 Unterstützung bei den Pflichten nach Art. 32 bis 36 DSGVO, Meldung von Verletzungen

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung und Benachrichtigung bei Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation der Aufsichtsbehörde), Art. 28 Abs. 3 lit. f DSGVO.

(2) Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten, die Daten des Auftraggebers betrifft, unverzüglich nach Kenntnis,

möglichst innerhalb von 24 Stunden (Art. 33 Abs. 2 DSGVO). Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Fehlende Angaben reicht er unverzüglich nach.

(3) Der Auftragnehmer ergreift unverzüglich die erforderlichen Maßnahmen, um die Verletzung zu beheben und mögliche nachteilige Folgen zu mindern, und stimmt diese, soweit möglich, mit dem Auftraggeber ab. Meldungen an die Aufsichtsbehörde und Benachrichtigungen der Betroffenen nimmt der Auftraggeber vor.

(4) Unterstützungsleistungen, die über die in S+ bereitgestellten Funktionen hinausgehen, kann der Auftragnehmer nach Aufwand angemessen vergütet verlangen, es sei denn, der Anlass beruht auf einem Verstoß des Auftragnehmers.

§ 8 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage, die Information der Betroffenen, die Beteiligung einer Arbeitnehmervertretung und die Festlegung von Aufbewahrungsfristen.

(2) Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen feststellt.

§ 9 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer und trägt dazu bei (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Nachweis kann vorrangig durch Selbstauskünfte, die aktuelle Beschreibung der Maßnahmen nach Anlage 2 sowie Nachweise und Zertifikate der Unterauftragsverarbeiter (z. B. des Hosters) erbracht werden.

(3) Inspektionen vor Ort sind nach Anmeldung mit einer Frist von mindestens 14 Tagen während der üblichen Geschäftszeiten möglich, in der Regel nicht häufiger als einmal im Kalenderjahr, außer bei konkretem Anlass (z. B. einer Datenschutzverletzung). Sie dürfen den Betrieb nicht unverhältnismäßig stören und keine Daten anderer Kunden offenlegen. Prüfer, die im Wettbewerb zum Auftragnehmer stehen, können abgelehnt werden; Prüfer sind zur Verschwiegenheit zu verpflichten. Rechte der Aufsichtsbehörden bleiben unberührt.

(4) Den Aufwand für Inspektionen vor Ort kann der Auftragnehmer angemessen vergütet verlangen, es sei denn, die Prüfung deckt einen erheblichen Verstoß des Auftragnehmers auf.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Nach Ende des Hauptvertrags stellt der Auftragnehmer dem Auftraggeber auf Verlangen einen Export seiner Daten bereit, einschließlich der unveränderlichen Verläufe (z. B. Export-Verlauf, Akten-Vermerke, Änderungsverläufe), soweit S+ sie für den Auftraggeber führt, und der hochgeladenen Dateien, in gängigen maschinenlesbaren Formaten bzw. als PDF (Art. 28 Abs. 3 lit. g DSGVO). Das Verlangen ist bis 30 Tage nach Vertragsende möglich.

(2) Nach Ablauf dieser Frist löscht der Auftragnehmer sämtliche personenbezogenen Daten des Auftraggebers einschließlich vorhandener Kopien, es sei denn, nach dem Recht der Union oder eines Mitgliedstaats besteht eine Verpflichtung zur Speicherung. In Datensicherungen werden die Daten mit dem regulären Überschreiben der Sicherungen gelöscht (derzeit spätestens nach acht Wochen, siehe Anlage 2); bis dahin sind sie vor jeder weiteren Nutzung geschützt.

(3) Die Löschung wird protokolliert und auf Anfrage in Textform bestätigt.

(4) Gesetzliche Aufbewahrungspflichten des Auftraggebers (z. B. für Arbeitszeitnachweise, Lohn- und Buchungsunterlagen) erfüllt dieser in eigener Verantwortung, insbesondere durch den rechtzeitigen Export.

§ 11 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für Schäden, die auf ihren eigenen Verstößen beruhen. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags (AGB § 8), soweit Art. 82 DSGVO nicht entgegensteht.

§ 12 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag vor.

(2) Dieser Vertrag wird elektronisch abgeschlossen (Art. 28 Abs. 9 DSGVO): bei der Registrierung bzw. durch Bestätigung einer berechtigten Person des Auftraggebers in S+. Fassung, Zeitpunkt, bestätigende Person und ein Hashwert der IP-Adresse werden gespeichert. Änderungen dieses Vertrags teilt der Auftragnehmer in Textform mit; § 10 Abs. 3 der AGB gilt entsprechend. Änderungen der Anlage 3 richten sich nach § 5 Abs. 2.

(3) Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit zulässig, Kaiserslautern.

Anlage 1 – Gegenstand, Art und Zweck, Datenarten, Kategorien betroffener Personen

Gegenstand: Bereitstellung, Betrieb, Wartung, Datensicherung und Support der SaaS-Software S+ (Webportal, Apps für iOS und Android, Uhren-Apps, Schnittstellen).

Dauer: Laufzeit des Hauptvertrags zuzüglich der Fristen nach § 10.

Art der Verarbeitung: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung an vom Auftraggeber bestimmte Empfänger, Abgleichen, Einschränken, Archivieren, Löschen.

Zweck: Organisation des Betriebs des Auftraggebers mit den von ihm gebuchten Modulen, insbesondere Zeiterfassung, Dienst- und Einsatzplanung, Leistungsnachweise (Rapporte), Qualitätskontrolle, Personal- und Bewerberverwaltung, Lohnvorbereitung und Steuerberater-Export, Abrechnung und Belege, Fuhrpark, Inventur, interne Kommunikation (Chat, Benachrichtigungen, Push-Mitteilungen), Dokumentenablage, Kundenportal, Anbindungen an Drittsysteme sowie optionale KI-Funktionen.

Kategorien betroffener Personen:

- Beschäftigte des Auftraggebers einschließlich Aushilfen, Minijobber, Werkstudenten, Auszubildender und ausgeschiedener Beschäftigter
- Bewerberinnen und Bewerber
- Kunden des Auftraggebers und deren Ansprechpartner, Nutzer des Kundenportals, Kontakte an Einsatzorten
- Lieferanten und Dienstleister und deren Ansprechpartner
- Absender und Empfänger von E-Mails in verbundenen Postfächern
- Nutzer von Einmal- und Freigabe-Links (z. B. Unterschrift von Stundenzetteln)

Arten personenbezogener Daten:

- Identifikations- und Kontaktdaten (Name, Anschrift, E-Mail, Telefon, Personalnummer, Profilbild)
- Zugangs- und Gerätedaten (Benutzerkonto, Passwort-Hash, Geräte- und Push-Kennungen, Anmeldeprotokoll)
- Arbeitszeit- und Einsatzdaten (Beginn, Ende, Pausen, Einsatzort, Standort beim Stempeln soweit aktiviert, Korrekturen mit Verlauf, Schichten, Termine)
- Abwesenheiten einschließlich Krankheit (Gesundheitsdaten nach Art. 9 DSGVO, soweit der Auftraggeber sie erfasst)
- Rapport- und Qualitätsdaten (Tätigkeiten, Material, Bemerkungen, Fotos, Unterschriften, Mängel)
- Personaldaten (Vertragsdaten, Qualifikationen, Nachweise, Aufenthalts- und Arbeitserlaubnisdaten, Dokumente)
- Lohn- und Abrechnungsdaten (Stundensätze, Zuschläge, Bankverbindung, Sozialversicherungs- und Steuer-Identifikationsnummer, soweit erfasst)
- Bewerbungsdaten (Lebenslauf, Anschreiben, Anhänge, Status)

- Kommunikationsdaten (Chat-Nachrichten, Bilder, Sprachnachrichten, E-Mails mit Anhängen, Benachrichtigungen)
- Fuhrparkdaten (Kennzeichen, Fahrtenbuch, Tankbelege), Kunden-, Rechnungs- und Belegdaten
- Protokolldaten (Änderungsprotokoll mit Akteur und Zeitpunkt, IP-Adressen nur gekürzt bzw. als Hashwert)
- weitere Daten, die der Auftraggeber in Freitexten, Dokumenten oder E-Mails selbst einstellt

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

1. Vertraulichkeit

- **Zutrittskontrolle:** Der Auftragnehmer betreibt keine eigenen Server. Anwendung, Datenbanken, Dateien und Sicherungen liegen beim Hoster Mittwald in Rechenzentren in Deutschland; für die physische Sicherung gelten dessen Maßnahmen.
- **Zugangskontrolle:** Anmeldung nur mit nicht erratbarer Firmen-ID, Firmen-Kennung, E-Mail und Passwort bzw. mit kurzlebigen Einmal-Codes (QR-Anmeldung, Anmelde-Link) oder Passkey. Passwörter und Kennungen werden nur als Hashwert gespeichert. Anmeldeversuche sind begrenzt; nach wiederholten Fehlversuchen wird die Anmeldung zeitweise gesperrt. Anmelde-Links sind nur kurz gültig und einmal verwendbar; gespeichert wird nur ihr Hashwert.
- **Zugriffskontrolle:** Rollen- und Stufenmodell je Mandant (z. B. Mitarbeiter, Leitung, Inhaber/Admin) mit zentraler Rechteprüfung bei jeder Anfrage. Mitarbeiter sehen nur eigene bzw. freigegebene Daten; Antworten an Mitarbeiter werden zusätzlich automatisiert auf fremde Personendaten und Preise geprüft („Datenschutz-Wächter“), Telefonnummern und E-Mail-Adressen in Freitexten von Mitarbeitern werden maskiert. Die Funktion „Ansicht als …“ ist nur lesend, zeitlich begrenzt und protokolliert. Das Technik-Konto des Auftragnehmers meldet sich nur per Einmal-Link an und kann vom Auftraggeber gesperrt werden.
- **Trennungskontrolle:** Jeder Auftraggeber (Mandant) hat eine eigene, getrennte Datenbank; der Mandant wird bei jeder Anfrage über Firmen-ID und Kennung bestimmt. Dateien werden je Mandant getrennt abgelegt.
- **Verschlüsselung:** Übertragung ausschließlich über HTTPS/TLS (mit HSTS). Besonders schutzbedürftige Felder werden zusätzlich mit dem Anwendungsschlüssel verschlüsselt gespeichert, u. a. Bankverbindung, Sozialversicherungs- und Steuer-ID, Lohnunterlagen, Zugangsdaten zu Anbindungen und Postfächern, Einträge des Passwort-Tresors, Push-Kennungen sowie Verläufe des KI-Assistenten.
- **Pseudonymisierung:** IP-Adressen werden in Protokollen nur gekürzt bzw. als Hashwert gespeichert. Vor dem Versand an KI- und Übersetzungsdienste werden Namen und Kontaktdaten durch Platzhalter ersetzt bzw. entfernt.

2. Integrität

- **Weitergabekontrolle:** Ziel-Adressen von Anbindungen sind fest hinterlegt; Webhooks und Abgleiche mit anderen Systemen sind signiert. Dateien liegen außerhalb des öffentlichen

Webverzeichnisses und werden nur nach Rechteprüfung ausgeliefert.
- **Eingabekontrolle:** Änderungsprotokoll schreibender Aktionen mit Akteur und Zeitpunkt, Geheimnisse maskiert. Protokoll-Tabellen sind gegen Änderung und Löschung gesperrt (nur Anfügen). Zeiteinträge und Korrekturen werden mit Verlauf geführt; Löschaktionen archivieren in der Regel statt zu löschen. Zugriffe des Auftragnehmers werden im Protokoll des Mandanten vermerkt.

3. Verfügbarkeit und Belastbarkeit

- Tägliche automatische Sicherung aller Datenbanken und Dateien mit Integritätsprüfung und Prüfsumme; Aufbewahrung 14 Tage täglich und 8 Wochen wöchentlich; tägliche Kontrolle mit Alarmierung des Auftragnehmers. Die Sicherungen liegen außerhalb des Webverzeichnisses beim Hoster.
- Begrenzung der Anfragen gegen Überlast, Not-Aus zum sofortigen Sperren der Plattform bei Angriffen, stündliche Prüfung geschützter Programmdateien auf unerwartete Änderungen.
- Offline-Warteschlange in den Apps für Zeiterfassung ohne Netz.

4. Wiederherstellbarkeit

- Wiederherstellung aus den Sicherungen nach Nr. 3; Programmänderungen werden mit Sicherung des vorherigen Stands und automatischem Rücksprung bei Fehlern eingespielt.

5. Verfahren zur regelmäßigen Überprüfung

- Automatisierte Tests, darunter Tests zur Mandantentrennung und zu Rechten, vor dem Einspielen von Änderungen.
- Regelmäßige automatisierte Auswertung der Protokolle auf Auffälligkeiten.
- Datenschutzfreundliche Voreinstellungen: optionale Module, KI-Funktionen, Übersetzung und Anbindungen sind standardmäßig ausgeschaltet.
- Überprüfung dieser Maßnahmen mindestens einmal jährlich.

Anlage 3 – Unterauftragsverarbeiter

Teil A – Unterauftragsverarbeiter des Auftragnehmers

Unternehmen	Leistung / Daten	Ort	Drittland-Grundlage
Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4–6, 32339 Espelkamp	Hosting von Anwendung, Datenbanken, Dateien und Sicherungen; Versand von System-E-Mails über den Mailserver von Mittwald (mail.agenturserver.de) – alle Daten	Deutschland	entfällt
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (Firebase Cloud Messaging); Unterauftragnehmer Google LLC, USA	Zustellung von Push-Mitteilungen an die Apps: Geräte-Kennung (Push-Token), Titel und Text der Mitteilung, technische Zusatzdaten	EU / USA	EU-US Data Privacy Framework (Google LLC), ergänzend Standardvertragsklauseln
Apple Distribution International Ltd., Hollyhill Industrial Estate, Cork, Irland; Unterauftragnehmer Apple Inc., USA (Apple Push Notification Service)	Zustellung von Push-Mitteilungen auf iPhone/iPad (über Firebase weitergeleitet): Geräte-Kennung, Inhalt der Mitteilung	EU / USA	EU-US Data Privacy Framework (Apple Inc.)
OpenAI Ireland Ltd., Dublin, Irland (Vertragspartner für Kunden im EWR); Unterauftragnehmer OpenAI OpCo, LLC und verbundene Unternehmen, USA	Nur wenn der Auftraggeber die KI-Abschrift im Feedback einschaltet: Sprachaufnahme der Feedback-Nachricht zur Umwandlung in Text	Irland / USA	Standardvertragsklauseln der EU-Kommission bzw. Angemessenheitsbeschluss nach dem Auftragsverarbeitungsvertrag (Data Processing Addendum) von OpenAI

Unternehmen	Leistung / Daten	Ort	Drittland-Grundlage
DeepL SE, Maarweg 165, 50825 Köln, oder Microsoft Ireland Operations Ltd., Dublin (Azure Translator, Endpunkt Europa)	Nur bei eingeschalteter Übersetzung: Arbeitsinhalte (z. B. Mängel, Tagesplan, Anleitungen); vor dem Versand werden E-Mail-Adressen, Telefonnummern, IBAN, Links mit Zugangsdaten sowie die im Mandanten bekannten Personen- und Kundennamen durch Platzhalter ersetzt	EU (DeepL: Rechenzentren in Europa; Azure: Rechenzentren der Region Europa)	entfällt; eine von DeepL angebotene Verarbeitung in weltweiten Cloud-Regionen (AWS) wird nicht freigegeben
OpenStreetMap Foundation, St John's Innovation Centre, Cambridge, Vereinigtes Königreich (Geocoding „Nominatim")	Fahrzeiten und Karten: Anschriften von Einsatzorten und – für die Fahrzeitberechnung – Wohnanschriften von Beschäftigten zur Umwandlung in Koordinaten	Vereinigtes Königreich / Niederlande (Angabe der OpenStreetMap Foundation)	Angemessenheitsbeschluss der EU-Kommission für das Vereinigte Königreich (erneuert am 19.12.2025, gültig bis 27.12.2031); Niederlande: EU
FOSSGIS e.V., Bundesallee 23, 10717 Berlin (Routing-Dienst „OSRM", router.project-osrm.org = routing.openstreetmap.de)	Fahrzeiten: Koordinaten von Start und Ziel zur Berechnung von Strecke und Fahrzeit	Schweiz (Server im Rechenzentrum der nine Internet Solutions AG, Zürich)	Angemessenheitsbeschluss der EU-Kommission für die Schweiz (Entscheidung 2000/518/EG)

Wetterdaten (Open-Meteo) werden nur mit Ort, Postleitzahl bzw. gerundeten Koordinaten ohne Personenbezug abgefragt; der Auftragnehmer setzt hierfür keinen Unterauftragsverarbeiter ein. Betriebs- und Sicherheitsmeldungen an den Auftragnehmer (Telegram) sind so aufgebaut, dass sie keine Inhalte aus den Daten des Auftraggebers enthalten, sondern nur Firmenname, Firmen-ID, Art des Ereignisses und interne Kennziffern (z. B. Personen-Nummer ohne Namen, Feldnamen ohne Werte).

Teil B – Vom Auftraggeber selbst beauftragte bzw. bestimmte Empfänger (§ 5 Abs. 5)

Diese Dienste werden nur genutzt, wenn der Auftraggeber sie einschaltet und – soweit vorgesehen – eigene Zugangsdaten hinterlegt. Den Vertrag einschließlich Auftragsverarbeitung schließt der Auftraggeber unmittelbar mit dem Anbieter.

Funktion	Anbieter (nach Wahl des Auftraggebers)	Daten
KI-Assistent	Anthropic PBC (USA), Amazon Web Services EMEA SARL (Bedrock, Region Frankfurt), Mistral AI SAS (Frankreich) oder eigener Server des Auftraggebers	pseudonymisierte Anfragen; Gesundheits-, Lohn-, Bank- und Zugangsdaten werden nicht übermittelt
Rechnungen/Belege	lexoffice (Haufe-Lexware GmbH & Co. KG, Freiburg)	Rechnungs-, Kunden- und Belegdaten
IT-Verwaltung	NinjaOne, LLC (USA; Region nach Wahl)	Geräte-, Lizenz- und Ticketdaten
Benachrichtigungskanäle	SMS-Anbieter, Webhook-Empfänger, eigener Telegram-Kanal oder E-Mail-Postfach des Auftraggebers	Benachrichtigungstexte nach den Regeln des Auftraggebers
E-Mail-Postfach	Mailanbieter des Auftraggebers (IMAP/SMTP)	E-Mails und Anhänge
Partner-Apps	vom Auftraggeber freigegebene Partner-Anwendungen	Daten im freigegebenen Umfang
Steuerberater, Lohnprogramm	vom Auftraggeber bestimmte Empfänger der Exporte	Inhalt der vom Auftraggeber ausgelösten Exporte

Stand: 21.10.2026 (Version 2026-10-21)