

Vertrag zur Auftragsverarbeitung (AVV)

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO für Einsatzbuch – Stand 22.10.2026 (Fassung 2026-10-22). Rechtstexte sind nur in deutscher Sprache verbindlich.

zwischen

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

und

SolveITKL („Solve IT“), Inhaber Nirojh Sritharan (Einzelunternehmen), Burgherrenstraße 9B, 67661 Kaiserslautern; 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 Einsatzbuch als Software-as-a-Service bereit (Hauptvertrag: Nutzungsvertrag nach den [AGB von Einsatzbuch](#)). 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-, Bestell- und Abrechnungsdaten des Auftraggebers, Sicherheitsprotokolle der Plattform, Meldungen über neue Registrierungen an den Auftragnehmer 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 Einsatzbuch, z. B. durch das Erfassen, Freigeben, Berichtigen und Löschen von Daten, das Vergeben von Rollen und Beitrittscodes, das Einschalten der Wetteranzeige und das Auslösen der Texterkennung. Einzelweisungen erteilt er in Textform an info@solve-it-kl.de. Weisungsberechtigt sind die im Betrieb als Inhaber 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, Unterstützung, Störungsbeseitigung und Sicherheit erforderlich ist. Dafür nutzt er einen eigenen Betreiber-Zugang mit getrennter Anmeldung; jeder Einblick in die Daten eines Betriebs wird mit Zeitpunkt, Person und Grund protokolliert, das Protokoll kann nicht gelöscht werden.

(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](#) 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 Einsatzbuch) 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 findet derzeit nicht statt. Sie erfolgt künftig nur nach Information gemäß Abs. 2 und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere bei einem Angemessenheitsbeschluss oder geeigneten Garantien wie Standardvertragsklauseln.

(5) Keine Unterauftragsverarbeitung sind Nebenleistungen ohne Zugriff auf personenbezogene Daten, z. B. Telekommunikationsleistungen, sowie Abfragen ohne Personenbezug (Anlage 3, Hinweise).

§ 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. Einsatzbuch stellt dafür Funktionen zum Anzeigen, Berichtigen (mit

Verlauf), Exportieren und Löschen bereit, z. B. die Kontolöschung einzelner Personen und den Export unter Betrieb → Export.

(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 Einsatzbuch 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 Beschäftigten, 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) Der Auftraggeber kann seine Daten jederzeit im angebotenen Umfang selbst exportieren (Betrieb → Export, Stundenzettel). Nach Ende des Hauptvertrags stellt der Auftragnehmer dem Auftraggeber auf Verlangen einen Export der übrigen Daten in gängigen maschinenlesbaren Formaten bzw. als PDF bereit (Art. 28 Abs. 3 lit. g DSGVO). Das Verlangen ist bis 30 Tage nach Vertragsende möglich.

(2) Löscht der Inhaber den Betrieb selbst, werden die Daten nach Ablauf der Widerrufsfrist von 14 Tagen gelöscht (AGB § 10 Abs. 3). Endet der Vertrag auf andere Weise, löscht der Auftragnehmer nach Ablauf der Frist nach Abs. 1 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 Arbeitszeitchronik, 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 § 11), 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 des Inhabers des Betriebs in Einsatzbuch. Fassung, Zeitpunkt, bestätigende Person und eine Prüfsumme der IP-Adresse werden gespeichert. Änderungen dieses Vertrags teilt der Auftragnehmer in Textform mit; § 12 Abs. 1 und 2 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 Unterstützung der SaaS-Software Einsatzbuch (Webseite einsatzbuch.de, Apps für iPhone/iPad und Android, Schnittstelle der Apps).

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

Art der Verarbeitung: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Abgleichen, Einschränken, Löschen.

Zweck: Arbeitszeiterfassung und Arbeitsorganisation des Betriebs des Auftraggebers mit den von ihm genutzten Modulen, insbesondere Zeiterfassung (Stempeln vor Ort, Monatsübersicht), Korrekturen und Freigaben, Schichten und Einsatzorte, Abwesenheiten, Stundenzettel, Rapporte mit Fotos und Unterschrift, Fotos zur Kundenakte, Unterlagen, Notizen, Whiteboard und Hinweifenster.

Kategorien betroffener Personen:

- Beschäftigte des Auftraggebers einschließlich Aushilfen, Minijobber, Auszubildender und ausgeschiedener Beschäftigter
- Inhaber und Leitungspersonen des Auftraggebers als Nutzer
- Ansprechpartner an Einsatzorten (Kunden des Auftraggebers), soweit der Auftraggeber sie einträgt

Arten personenbezogener Daten:

- Identifikations- und Kontaktdaten (Name, E-Mail-Adresse, Telefon, Personalnummer, Profilbild)
- Zugangsdaten (Benutzerkonto, Passwort nur als Hashwert, Anmelde-Schlüssel der Apps, Anmelde-Protokoll)
- Arbeitszeit- und Einsatzdaten (Datum, Beginn, Ende, Pausen, Einsatzort, Erfassungsart, Standort beim Stempeln nur mit Erlaubnis der Person, Korrekturen mit Verlauf, Freigaben, Schichten)
- Abwesenheiten einschließlich Krankheit (Gesundheitsdaten nach Art. 9 DSGVO, soweit der Auftraggeber sie erfasst)
- Report-, Foto- und Unterlagendaten (Tätigkeiten, Material, Bemerkungen, Fotos, Unterschriften, Dokumente wie Lohnzettel oder Bescheinigungen)
- Kommunikations- und Notizdaten (Notizen, Hinweifenster mit Lesebestätigung, Whiteboard-Inhalte)
- Protokolldaten (Änderungsverläufe mit Person, Zeitpunkt und IP-Adresse; Anmelde-Protokoll mit gekürzter IP-Adresse bzw. Prüfsumme)
- weitere Daten, die der Auftraggeber in Freitexten oder Dokumenten selbst einstellt

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

1. Vertraulichkeit

- **Zutrittskontrolle:** Der Auftragnehmer betreibt keine eigenen Server. Anwendung, Datenbank, Dateien und Sicherungen liegen beim Hoster Mittwald in Rechenzentren in Deutschland; für die physische Sicherung gelten dessen Maßnahmen.
- **Zugangskontrolle:** Anmeldung mit E-Mail-Adresse und Passwort (mindestens 10 Zeichen); Passwörter werden nur als Hashwert gespeichert. Nach wiederholten Fehlversuchen wird die Anmeldung zeitweise gesperrt, öffentliche Formulare sind gedrosselt; gehäufte Fehlanmeldungen werden dem Auftragnehmer gemeldet. Die Apps melden sich mit einem eigenen, widerrufbaren Schlüssel an. Beitrittscodes sind sperrbar und können begrenzt werden.
- **Zugriffskontrolle:** Rollenmodell je Betrieb (Mitarbeiter, Schichtleitung, Personal, Lohn, Inhaber) mit Rechteprüfung bei jeder Anfrage. Mitarbeiter sehen nur eigene bzw. ausdrücklich freigegebene Daten. Ein automatisierter Datenschutz-Wächter prüft täglich, dass Mitarbeiter nur sehen, was sie sehen dürfen. Der Betreiber-Zugang des Auftragnehmers hat eine eigene, getrennte Anmeldung; jeder Einblick in einen Betrieb wird mit Grund protokolliert.
- **Trennungskontrolle:** Jeder Datensatz ist genau einem Betrieb zugeordnet; ein Filter auf Ebene der Anwendung beschränkt jede Abfrage auf den Betrieb der angemeldeten Person. Die Trennung ist durch automatisierte Tests abgesichert, die bei jeder Änderung laufen. Dateien liegen außerhalb des öffentlichen Webverzeichnisses und werden nur nach Prüfung von Betrieb und Rolle ausgeliefert.
- **Verschlüsselung:** Übertragung ausschließlich über HTTPS/TLS (mit HSTS). Schlüssel für Schnittstellen werden verschlüsselt gespeichert.
- **Pseudonymisierung und Datensparsamkeit:** Das Anmelde-Protokoll speichert IP-Adressen nur gekürzt bzw. als Prüfsumme. Profilbilder werden neu berechnet, Metadaten (auch Aufnahmeort) entfallen. Der

Standort beim Stempeln wird nur mit Erlaubnis der Person und nur am Zeiteintrag gespeichert, es gibt keine Ortung zwischen den Stempeln.

2. Integrität

- **Weitergabekontrolle:** Dateien werden nur nach Rechteprüfung ausgeliefert. Der Datenaustausch mit anderen Anwendungen des Auftragnehmers ist mit einem gemeinsamen Geheimnis signiert und höchstens fünf Minuten gültig.
- **Eingabekontrolle:** Änderungen an Arbeitszeiten werden mit Verlauf (vorher/nachher, Person, Zeitpunkt, Grund, IP-Adresse) geführt; Korrekturen laufen über Antrag und Freigabe. Zugriffe des Auftragnehmers werden protokolliert.

3. Verfügbarkeit und Belastbarkeit

- Tägliche automatische Sicherung der Datenbank und der Dateien mit Prüfung; Aufbewahrung 14 Tage täglich und 8 Wochen wöchentlich; tägliche Kontrolle mit Meldung an den Auftragnehmer bei Fehlern. Die Sicherungen liegen außerhalb des Webverzeichnisses beim Host.
- Begrenzung der Anfragen gegen Überlast und Angriffe.
- Speicherung der Stempel in der App, solange keine Verbindung besteht, und Übertragung danach.

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 zur Trennung der Betriebe und zu Rechten, vor dem Einspielen von Änderungen.
- Täglicher Lauf des Datenschutz-Wächters; Bericht nur mit Bezeichnungen von Fundstellen, nie mit Werten.
- Datenschutzfreundliche Voreinstellungen: Die Wetteranzeige ist standardmäßig aus, der Standort beim Stempeln wird nur mit Erlaubnis der Person erfasst, die Texterkennung läuft nur auf Knopfdruck.
- Überprüfung dieser Maßnahmen mindestens einmal jährlich.

Anlage 3 – Unterauftragsverarbeiter

Unternehmen	Leistung / Daten	Ort	Drittland
Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4–6, 32339 Espelkamp	Hosting von Anwendung, Datenbank, Dateien und Sicherungen; Versand der E-Mails von Einsatzbuch über den Mailserver des Hosters – alle Daten	Deutschland	nein
a9t9 software GmbH, Postfach 1343, 69184 Walldorf (Dienst „OCR.space“)	Nur wenn Personal oder Inhaber für eine Unterlage die Texterkennung per Knopfdruck auslösen: ein Bild der ersten Seite dieser Unterlage (nicht die Datei) zur Umwandlung in Text; das Ergebnis wird beim Betrieb gespeichert	Deutschland (Sitz)	nein

Hinweise:

- **Wetter:** Nur wenn der Inhaber die Wetteranzeige einschaltet, fragt der Server bei Open-Meteo (api.open-meteo.com) das Wetter am Betriebsort ab – mit einer auf etwa einen Kilometer gerundeten Koordinate, ohne Namen, Anschrift, Kennung oder Standort von Personen. Dabei werden keine personenbezogenen Daten übermittelt; Open-Meteo ist deshalb kein Unterauftragsverarbeiter.
- **Maschinelle Übersetzung:** Die Übersetzung von Arbeitsanweisungen ist derzeit ausgeschaltet; es wird kein Übersetzungsdienst eingesetzt. Bevor der Auftragnehmer einen Dienst (z. B. DeepL SE, Köln, oder Microsoft Ireland Operations Ltd., Dublin, Rechenzentren in Europa) einschaltet, informiert er den Auftraggeber nach § 5 Abs. 2.
- **Andere Anwendungen des Auftragnehmers:** S+ und splus sind Anwendungen desselben Auftragnehmers beim selben Host und daher keine Unterauftragsverarbeiter. Ein Austausch von Arbeitszeiten, Schichten und Objekten findet nur für Betriebe statt, die diese Anwendungen nebeneinander nutzen und die Verbindung eingerichtet haben.
- **Apps:** Die Apps werden über den App Store (Apple) und Google Play bereitgestellt. Einsatzbuch nutzt keine Push-Dienste von Apple oder Google; Benachrichtigungen erzeugt die App auf dem Gerät selbst.

Stand: 22.10.2026 (Fassung 2026-10-22)