Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Dieser Auftragsverarbeitungsvertrag wird zwischen dem Kunden (Verantwortlicher) und der Lichtmannegger GmbH (Auftragsverarbeiter) geschlossen. Mit der Registrierung stimmt der Kunde diesem AVV zu; die Zustimmung wird mit Version und Zeitstempel dokumentiert. Version: 2026-09-18 · Stand: 18.09.2026

Parteien

Verantwortlicher: das jeweilige Kundenunternehmen (Angaben aus der Registrierung / dem Nutzungsvertrag).
Auftragsverarbeiter: Lichtmannegger GmbH, Gewerbering 7, 83549 Eiselfing, Amtsgericht Traunstein, HRB 35272, vertreten durch Geschäftsführer Georg Lichtmannegger, support@lme-arbeitsschutz.de.

§ 1 Gegenstand und Dauer

Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Nutzung der Software „Lichtmannegger Safety Manager“ (Arbeitsschutz-/EHS-Plattform).
Die Verarbeitung erfolgt für die Dauer des zugrunde liegenden Hauptvertrags (Nutzungsvertrag). Der AVV endet automatisch mit Beendigung des Hauptvertrags.
Mehrstufige Verarbeitung: Der Verantwortliche kann die Software entweder für das eigene Unternehmen nutzen oder – etwa als Fachkraft für Arbeitssicherheit (Fasi) bzw. Dienstleister – als Auftragsverarbeiter für eigene Kundenunternehmen (Mandanten). Im letzteren Fall sind die jeweiligen Kundenunternehmen die datenschutzrechtlich Verantwortlichen, der Verantwortliche dieses Vertrags ist deren Auftragsverarbeiter und der Auftragsverarbeiter dieses Vertrags handelt als dessen Unterauftragsverarbeiter.
Der Verantwortliche sichert für den Fall der mehrstufigen Verarbeitung zu, dass er zur Einbindung des Auftragsverarbeiters als Unterauftragsverarbeiter berechtigt ist und mit den jeweils Verantwortlichen (seinen Kundenunternehmen) einen wirksamen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO geschlossen hat, der den Einsatz von Unterauftragsverarbeitern zulässt.

§ 2 Art, Umfang und Zweck der Verarbeitung

Art und Zweck: Bereitstellung und Betrieb einer mandantenfähigen Arbeitsschutz-Software (u. a. Gefährdungsbeurteilungen, Maßnahmen, Unterweisungen, Arbeitsmittel/Prüfungen, Gefahrstoffe, Unfälle, Mitarbeiterverwaltung, Dokumentenablage).

Kategorien betroffener Personen: Beschäftigte des Verantwortlichen, ggf. weitere im Arbeitsschutz erfasste Personen (z. B. Ersthelfer, Sicherheitsbeauftragte, externe Beteiligte).
Arten der Daten: siehe Anlage 1 (Datenkategorien). Hierzu zählen auch Gesundheitsdaten (Art. 9 DSGVO) im Modul Unfälle/Beinaheunfälle; deren Erfassung ist auf das Erforderliche begrenzt.

§ 3 Weisungsbindung

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf die Übermittlung in Drittländer, sofern er nicht durch Rechtsvorschriften zu einer anderen Verarbeitung verpflichtet ist.
Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.
Zur Einrichtung, Störungsbeseitigung und Qualitätssicherung kann der Auftragsverarbeiter auf die Daten des Verantwortlichen zugreifen. Dieser Zugriff erfolgt ausschließlich durch hierzu berechtigte Personen des Auftragsverarbeiters und wird mit Zeitpunkt, handelnder Person und betroffener Organisation protokolliert; ein Teil dieser Zugriffe ist ausschließlich lesend. Der Verantwortliche kann jederzeit Auskunft über die protokollierten Zugriffe verlangen; der Auftragsverarbeiter erteilt sie innerhalb von zehn Werktagen.

§ 4 Vertraulichkeit

Der Auftragsverarbeiter setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

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

Der Auftragsverarbeiter trifft die zur Sicherheit der Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen. Diese sind in Anlage 2 beschrieben.
Die Maßnahmen unterliegen dem technischen Fortschritt und können fortentwickelt werden, sofern das Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverhältnisse

Der Verantwortliche stimmt dem Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter zu (Hosting der Anwendung, Datenbank-/Speicher-/Authentifizierungsdienst, E-Mail-Versand sowie – nur bei gebuchtem Zusatzmodul „KI-Assistenz“ – die KI-Verarbeitung).
Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag mit Datenschutzpflichten, die den hiesigen entsprechen. Beabsichtigte Wechsel oder die Hinzunahme weiterer Unterauftragsverarbeiter werden dem Verantwortlichen rechtzeitig mitgeteilt; er kann diesen aus wichtigem Grund widersprechen.
Eigenes Absender-Postfach: Der Verantwortliche kann ein eigenes E-Mail-Konto hinterlegen. Der fachliche Mailversand (Berichte, Maßnahmenpläne, Unterweisungs-Einladungen, Fristen-Erinnerungen) läuft dann ausschließlich über dieses Konto; ein Unterauftragsverarbeiter für den E-Mail-Versand wird insoweit nicht eingesetzt (Anlage 3 weist den jeweils geltenden Stand aus). Der Verantwortliche verantwortet Betrieb, Erreichbarkeit und Zugangsdaten dieses Kontos sowie das dortige Vertragsverhältnis zu seinem E-Mail-Anbieter. Ist das Konto nicht erreichbar, unterbleibt der Versand – ein ersatzweiser Versand über das Konto des Auftragsverarbeiters findet ausdrücklich NICHT statt. Unberührt bleibt der Versand von Konto- und Vertragsnachrichten (z. B. Zugangsdaten, Passwort-Zurücksetzen, Rechnungen des Auftragsverarbeiters); er

läuft weiterhin über den Auftragsverarbeiter. Die Verarbeitung der Inhalte in der Anwendung selbst bleibt in jedem Fall Auftragsverarbeitung nach diesem Vertrag.

§ 7 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).
Er unterstützt den Verantwortlichen ferner bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung).

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, damit dieser seine Pflichten nach Art. 33 und 34 DSGVO (insbesondere die 72-Stunden-Meldung an die Aufsichtsbehörde) erfüllen kann.

§ 9 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen –, die der Verantwortliche oder ein beauftragter Prüfer durchführt.
Nachweise können auch durch geeignete Zertifizierungen oder Berichte der Unterauftragsverarbeiter erbracht werden.

§ 10 Löschung und Rückgabe nach Beendigung

Nach Abschluss der Verarbeitung löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und vernichtet vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht.

§ 11 Haftung und Schlussbestimmungen

Die Haftung richtet sich nach Art. 82 DSGVO sowie den Regelungen des Hauptvertrags. Änderungen und Ergänzungen dieses AVV bedürfen der Textform.
Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 – Betroffene Personen & Datenkategorien

Kategorien betroffener Personen:

- Beschäftigte des Verantwortlichen
- Sicherheitsbeauftragte, Ersthelfer, Brandschutzhelfer
- Weitere im Arbeitsschutz erfasste Personen (z. B. externe Beteiligte)

Kategorien personenbezogener Daten:

- **Mitarbeiter-Stammdaten:** Vor-/Nachname, Funktion/Rolle, Abteilung, Personalnummer, Telefon, E-Mail, Beschäftigungsart und Befristung, Austrittsdatum und -grund
- **Unterweisungen:** Teilnahme, Datum, digitale Unterschrift (Bestätigung „gelesen & verstanden“)
- **Unfälle / Beinaheunfälle:** Hergang, Verletzungsart, Ausfallzeiten, ggf. Name/Personalnummer (Gesundheitsdaten = besondere Kategorie (Art. 9 DSGVO). Name/Personalnummer sind optional (Datenminimierung); der Verantwortliche benötigt eine Rechtsgrundlage.)
- **Begehungen / Fotos:** Mängelfotos (können mittelbar Personen zeigen)
- **Mängelmeldungen:** Beschreibung, Fotos, Name der beauftragten Person, optional GPS-Standort (Der GPS-Standort wird nur erfasst, wenn der meldende Nutzer den Knopf „Standort erfassen“ aktiv betätigt und der Browser die Freigabe erteilt (Datenminimierung; keine Hintergrund-Ortung).)
- **Interne Kundenakte des betreuenden Büros:** Notizen des Büros zur betreuten Firma (Datum, Verfasser, Text), private Notizen einzelner Büro-Mitarbeiter, Verträge, Angebote, AV-Vertrag und Schriftverkehr mit Wiedervorlage (Nur für Mitglieder des betreuenden Büros sichtbar (Datenbank-Rechte), nie für die betreute Firma. Private Notizen sieht ausschließlich ihr Verfasser. Gespeichert in einem eigenen, nicht öffentlichen Speicherbereich je Büro.)
- **Nachrichten zwischen Benutzern:** Text der Nachricht, Absender und Empfänger, Zeitpunkt, Kennzeichen „wichtig“, gelesen und erledigt (Sichtbar nur für Absender und Empfänger (Datenbank-Rechte) – auch Administratoren lesen fremde Nachrichten nicht, und der Text steht in keinem Änderungsprotokoll. Bleibt eine Nachricht einen Tag ungelesen, geht eine Hinweis-Mail OHNE den Inhalt. Löschung nach 12 Monaten.)
- **Kontaktaufnahme:** Name, E-Mail und Nachricht aus dem Kontaktformular; Telefonnummer bei Rückfragen
- **Benutzerkonten:** Name, E-Mail, Telefon, Rolle, Anmelde-/Authentifizierungsdaten (Passwort nur als Hash). Bei der Registrierung eines Testzugangs kann freiwillig eine Telefonnummer angegeben werden – ausschließlich für eine telefonische Rückfrage zum Testzugang; ohne Angabe funktioniert der Zugang genauso.

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

- **Verschlüsselung Transport:** Gesamte Kommunikation ausschließlich über HTTPS/TLS (verschlüsselte Verbindung).
- **Verschlüsselung Speicher:** Verschlüsselung der Daten und Backups „at rest“ nach Angaben der Anbieter (AWS/Supabase, Hostinger).
- **Mandantentrennung (zweistufig):** Strikte Trennung der Daten auf Datenbankebene durch Row Level Security (RLS) – auf zwei Ebenen: zwischen Organisationen (z. B. verschiedene Fasi-Büros/Unternehmen) und innerhalb einer Organisation zwischen deren Mandanten. Jeder Nutzer sieht ausschließlich die Daten, für die er berechtigt ist; ein organisationsübergreifender Zugriff ist technisch ausgeschlossen.
- **Zugriffskontrolle:** Benutzer-Authentifizierung, rollenbasierte Rechte (Plattform-/Organisations-/Mandanten-Ebene), erzwungene Passwortänderung bei Erstanmeldung,

optionale Zwei-Faktor-Anmeldung (TOTP-Code aus einer Authenticator-App), je Firma als Pflicht schaltbar.

- **Least Privilege:** Privilegierter Datenbankzugriff (Service-Role) ausschließlich serverseitig, nie im Browser.
- **Keine Drittanbieter-Tracker:** Beim normalen Seitenaufruf werden keine externen Dienste geladen: kein Google Fonts/Analytics, kein Tracking, keine Werbe-Cookies, kein externes CDN. Ausnahme: Bindet der Betreiber in einer Neuigkeit ausdrücklich ein Video ein (YouTube im „nocookie"-Modus, Vimeo mit „Do Not Track", Loom), lädt der Video-Player erst beim Aufruf dieser Neuigkeit Inhalte des jeweiligen Anbieters. Ebenso Lernvideos einer Online-Unterweisung, die als YouTube-Video hinterlegt sind: Sie laden erst nach Klick auf „Video laden" (youtube-nocookie.com). Gespeichert wird zur Teilnahme nur die abgespielte Zeit und der Zeitpunkt „vollständig angesehen".
- **Protokollierung:** Änderungsverlauf zentraler Daten (wer/wann) zur Nachvollziehbarkeit.
- **Backups:** Regelmäßige Backups durch den Hosting-Anbieter (Backup-Standort Frankreich/EU).

Anlage 3 – Unterauftragsverarbeiter

- **Supabase (Supabase Inc.)** – Datenbank, Datei-Speicher (Storage) und Benutzer-Authentifizierung. Standort: Frankfurt am Main, Deutschland (AWS eu-central-1); Sitz: USA. AVV/DPA liegt vor (Anbieter-DPA inkl. EU-Standardvertragsklauseln/SCC; gilt über die Nutzungsbedingungen). SOC 2 Type II nach Angaben des Anbieters.
- **Hostinger (Hostinger International Ltd.)** – Hosting der Anwendung (Web-/App-Server), Backups sowie Versand der System-E-Mails (SMTP-Postfach). Standort: Server: Deutschland · Backups: Frankreich (beide EU); Sitz: Litauen (EU). AVV/DPA liegt vor (Anbieter-DPA inkl. EU-SCC; gilt über die Nutzungsbedingungen).
- **Anthropic (Anthropic PBC)** – KI-Assistenzfunktionen (Claude API) – nur bei gebuchtem Zusatzmodul „KI-Assistenz" und nur für die konkret angefragte Funktion. Die Funktionen benötigen keine personenbezogenen Daten; enthalten Eingaben oder hochgeladene Dokumente solche Daten, werden sie mit übermittelt. Standort: USA; Sitz: USA. AVV/DPA mit EU-Standardvertragsklauseln (SCC); über die API gesendete Inhalte werden nicht zum Training der Modelle verwendet, Protokolldaten werden standardmäßig nach 7 Tagen gelöscht.

Lichtmannegger Safety Manager · Stand: 18.9.2026