Anlage 3: Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO)

Fassung vom 22.11.2026. Zwischen dem Kunden (Verantwortlicher) und der AWAI-Analytics GmbH, Hauptstraße 33c, 09573 Gornau OT Dittmannsdorf, vertreten durch Andreas Wolfgruber („AWAI“, Auftragsverarbeiter). Der AVV wird mit der Online-Bestellung oder mit der Beta-Vereinbarung abgeschlossen. Er gilt, solange der Kunde kalle nutzt, und darüber hinaus bis zur Löschung nach § 9.

§ 1 Gegenstand und Dauer. AWAI stellt dem Kunden die Branchensoftware „kalle“ für Aufträge, Objekte, Einsatzplanung, Zeiterfassung, Berichte, Mängel, Angebote, Rechnungen, Belege, Material, Lohnvorbereitung, die Zusammenarbeit mit Subunternehmern und einen KI-Assistenten als Webanwendung und App bereit (Software als Dienst). Dabei verarbeitet AWAI personenbezogene Daten im Auftrag des Kunden. Dauer: Laufzeit des Hauptvertrags (AGB bzw. Beta-Vereinbarung) zuzüglich der Löschfrist nach § 9.

§ 2 Art und Zweck. Speichern, Ordnen, Anzeigen, Auswerten, Erstellen von PDF-Dokumenten und Übergabedateien (z. B. für das Lohnbüro), Übermitteln an vom Kunden bestimmte Empfänger (E-Mails an Kunden, Bewohner, Subunternehmer und eigene Leute, entweder über den Postausgang von kalle oder über das Postfach des Kunden; Kunden-Freigabelink; Subunternehmer und verbundene Firmen nach § 13), Übernahme von Altdaten aus Dateien des Kunden (§ 14), Verarbeitung durch KI-Dienste auf Anstoß einer Person des Kunden oder als Folge ihrer Handlung (z. B. Belegerkennung nach dem Hochladen, Lesen einer Anfrage als PDF), Sprachausgabe von Antworten des Assistenten, Zwischenspeichern in der App, solange das Telefon kein Netz hat, Sichern und Löschen — jeweils nur, um die Software bereitzustellen und zu betreiben.

§ 3 Arten der Daten.

- *Beschäftigte des Kunden*, auch ehemalige, wenn der Kunde ihre Daten übernimmt: Name, Kontaktdaten, Personalnummer, Geburtsdatum, Ein- und Austrittsdatum, Wohnadresse (freiwillig, auch als Start und Ende der Tagesroute), Foto (freiwillig), Rollen und Rechte, Arbeitszeiten, Verfügbarkeit je Wochentag, Stundengrenze bei Minijobs, Einsatz- und Standortbezug (Stempelung am Einsatzort, NFC-Chip; kein GPS), Abwesenheiten mit Art und Zeitraum, Urlaubskonten, Nachweise mit Ablaufdatum (z. B. Führerschein, Unterweisung), Stundensätze, Lohn nach Vorgabezeit, Zuschläge, Spesen (auch nach der Entfernung zwischen Niederlassung und Einsatzort), Vorschüsse und Auszahlungen mit Weg (Lohn, Überweisung, bar) und Quittung (Bestätigung in der App oder Unterschrift am Bildschirm), Anmelde- und Sicherheitsdaten; keine Bankverbindung für Auszahlungen. Beim Umstieg ein Archiv alter Arbeitszeiten und Abwesenheiten, Startwerte für Urlaub und Gleitzeit und die Originale von Stundenzetteln und Urlaubslisten. Bei verbundenen Firmen zusätzlich Personen-ID und Belegt-Zeiten ohne Inhalt (§ 13).
- *Kunden, Ansprechpartner und Interessenten des Kunden*: Name, Anschrift, Kontaktdaten, Objekte (auch Haus mit Einheiten) und Hinweise vor Ort, Anfragen und Reparaturaufträge (auch als PDF oder Scan), Angebote (beim Umstieg auch alte Angebote mit Preisen und Originaldatei), Aufträge, Auftragsbestätigungen, Berichte mit Fotos und Unterschrift, Mängel (Text, Objekt, meldende Person, Datum, Frist, Folgeeinsatz), Rechnungen und Zahlungen.

- *Bewohner und Mieter von Objekten*: Name, Telefon, E-Mail, Ankündigungen und Erinnerungen zu Terminen per E-Mail, Protokolle bei Abnahme und Übergabe einer Wohnung mit Unterschrift.
- *Lieferanten und Subunternehmer* (Firmen und Einzelpersonen): Name, Anschrift, Kontaktdaten, USt-IdNr., Steuernummer, Bankverbindung, Belege und Eingangsrechnungen samt Zuordnung zu Einsätzen, Nachweise, Vereinbarung je Einsatz (Pauschale oder Stundensatz); bei Subunternehmern mit App-Zugang dazu Konto, Zeitbuchungen und Berichte.
- *Freitext und Dateien*: Freitext, Sprachaufnahmen (nur zur Umschrift), Gespräche mit dem Assistenten als Text (sichtbar nur für die jeweilige Person), Bildschirmfotos an den Assistenten (höchstens zwei, nicht im Gespräch gespeichert), Antwortsätze des Assistenten für die Sprachausgabe und Dateien, die der Kunde einstellt.
- *Besondere Kategorien (Art. 9 DSGVO)*: Krankheit, Kinderkrank und Mutterschutz als Art einer Abwesenheit; Krankmeldungen, Eingang von Arbeitsunfähigkeitsbescheinigungen und Krankheitsfälle, auch wenn sie über den Assistenten erledigt werden; beim Umstieg die Art „Krank“ im Archiv alter Zeiten und alles, was auf hochgeladenen Stundenzetteln und Urlaubslisten steht, auch Randnotizen; Schwerbehinderung (nur für den Zusatzurlaub); in Betreuungsbetrieben können Berichte Gesundheitsangaben betreuter Personen enthalten. AWAI verarbeitet sie nur, weil und soweit der Kunde sie einstellt. Die Art einer Krankheit erfasst kalle nicht: Für Diagnosen gibt es kein Feld, und eine Arbeitsunfähigkeitsbescheinigung wird nur als eingegangen vermerkt und nicht hochgeladen. Der Kunde hält seine Nutzer an, dem Assistenten und in Freitexten keine Diagnosen zu nennen.

§ 4 Betroffene. Beschäftigte des Kunden, auch ehemalige; dessen Kunden, Ansprechpartner, Interessenten und betreute Personen; Bewohner und Mieter von Objekten; Lieferanten, Subunternehmer und deren Kontaktpersonen; Beschäftigte verbundener Firmen, soweit sie angebunden sind; sonstige in Freitext oder Dateien genannte Personen.

§ 5 Weisungen. AWAI verarbeitet nur auf dokumentierte Weisung des Kunden. Die Weisung ist dieser Vertrag; weitere Weisungen erteilt der Kunde durch seine Einstellungen und Handlungen in der Software (z. B. Module ein- und ausschalten, Versandweg für E-Mails wählen, KI-Funktionen abschalten, Personen anonymisieren, Gesamtexport) oder in Textform. Hält AWAI eine Weisung für rechtswidrig, weist AWAI den Kunden darauf hin.

§ 6 Vertraulichkeit und Zugriff durch AWAI. Wer bei AWAI Zugang zu Systemen hat, ist zur Vertraulichkeit verpflichtet. Die Betreiber-Konsole hat keinen Lesezugriff auf Personendaten der Kunden. Ausgenommen sind Rückmeldungen, die Nutzer des Kunden selbst an AWAI senden (Name, E-Mail-Adresse, Text, bis zu drei Bilder, die auch Daten des Kunden zeigen können, bei einer Rückmeldung zu einer Antwort des Assistenten der Gesprächsausschnitt, den die Person selbst absendet). AWAI greift auf Daten eines Kunden nur zur Fehlerbehebung oder Wiederherstellung zu, grundsätzlich auf dessen Anfrage. Der Rettungsweg der Betreiber-Konsole vermerkt sich im Änderungsprotokoll des Kunden; ein direkter Datenbankzugriff ist nur autorisierten Mitarbeitern der AWAI-Analytics GmbH im Störungsfall möglich und wird schriftlich dokumentiert. Die Daten des Vermittlers für verbundene Firmen (§ 13) liegen in der Plattform-Datenbank von AWAI; die Betreiber-Konsole zeigt sie nicht.

§ 7 Unterauftragsverarbeiter. Der Kunde genehmigt die in Anlage 3b genannten Unterauftragsverarbeiter. Über neue oder ersetzte Unterauftragsverarbeiter informiert AWAI

mindestens 30 Tage vorher in Textform; der Kunde kann aus wichtigem datenschutzrechtlichem Grund widersprechen und den Hauptvertrag dann zum Änderungszeitpunkt kündigen. AWAI verpflichtet jeden Unterauftragsverarbeiter vertraglich auf gleichwertige Pflichten.

§ 8 Unterstützung des Kunden. AWAI unterstützt bei Betroffenenrechten vor allem durch Funktionen in der Software: Auskunft als PDF und JSON je Mitarbeiter und je Kunde, Anonymisieren von Personen mit Wiedervorlage (Vorgabe 36 Monate nach Austritt), Gesamtexport aller Daten und Dateien, Änderungsprotokoll. Gespräche mit dem Assistenten sind nur für die jeweilige Person sichtbar; dem Kunden gibt AWAI sie nur auf dessen dokumentierte Weisung im Einzelfall heraus, etwa für ein Auskunftsersuchen dieser Person. Darüber hinaus hilft AWAI bei Meldungen nach Art. 33/34, Folgenabschätzungen und Anfragen von Behörden im angemessenen Umfang. Eine Verletzung des Schutzes personenbezogener Daten meldet AWAI unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis.

§ 9 Löschung und Rückgabe nach Vertragsende. Nach Vertragsende sperrt AWAI den Zugang und hält die Daten 90 Tage für den Gesamtexport und Rückfragen bereit. Danach löscht AWAI Datenbank, Dateien und Schlüssel des Kunden; Sicherungen laufen höchstens 14 Tage nach. Aufbewahrungspflichten (z. B. GoBD für Rechnungen) erfüllt der Kunde selbst; er exportiert vorher. Für das Rechnungsarchiv mit unveränderlicher Ablage gilt: Der Kunde erhält dessen Dateien mit dem Gesamtexport. Nach Ablauf der 90 Tage löscht AWAI auch das Archiv, es sei denn, der Kunde beauftragt AWAI vorher in Textform, es bis zum Ende seiner gesetzlichen Aufbewahrungsfrist gesperrt weiter aufzubewahren; dafür gilt dieser Vertrag fort.

§ 10 Nachweise und Kontrollen. AWAI weist die Einhaltung durch die TOM (Anlage 3a), auf Anfrage durch Selbstauskunft nach. Der Kunde prüft vorrangig anhand dieser Unterlagen. Eine Kontrolle vor Ort findet nur statt, wenn die Unterlagen im Einzelfall nicht ausreichen, nach Absprache und auf Kosten des Kunden.

§ 11 Ort der Verarbeitung. In der EU: Rechenzentren in Schweden und Irland, KI-Modelle in Schweden oder der EU-Datenzone, E-Mail-Versand mit Datenstandort Europa (Anlage 3b). Eine Übermittlung in Drittländer ist nicht vorgesehen.

§ 12 Haftung. Es gilt Art. 82 DSGVO; im Übrigen die Haftungsregel der AGB (§ 15).

§ 13 Subunternehmer und verbundene Firmen. Richtet der Kunde einem Subunternehmer einen App-Zugang ein, schickt er ihm über die Software eine Nachricht oder verbindet er sein Konto mit einem anderen Kunden von AWAI, bestimmt er, welche Daten dieser erhält. Das ist eine Weisung nach § 5. Bei verbundenen Firmen kopiert ein Hintergrundlauf von AWAI nur einen festen Feldkatalog; keine Firma hat Zugriff auf die Datenbank der anderen. Für das, was bei ihr ankommt, ist die empfangende Firma selbst Verantwortlicher. Subunternehmer und verbundene Firmen sind keine Unterauftragsverarbeiter von AWAI. Der Kunde informiert die Betroffenen und schließt mit dem Subunternehmer die nötigen Vereinbarungen.

§ 14 Übernahme von Altdaten und Lesen von Dokumenten. Der Kunde entscheidet, welche Altdaten und Dokumente er hochlädt, und prüft vorher, ob er sie weiter verarbeiten darf, auch zu ausgeschiedenen Beschäftigten. Das Hochladen und der Start des Lesens sind Weisungen nach § 5. Die KI liest Dokumente mit allem, was darauf steht; übernommen wird nur, was eine Person des Kunden

bestätigt. Vorbilder und Katalog-Vorschläge aus alten Angeboten entstehen nur für diesen Kunden; kein Modell wird damit trainiert.

§ 15 Änderungen. Änderungen dieses Vertrags bedürfen der Textform. Anlage 3a beschreibt den jeweiligen Stand der Technik; AWAI darf sie fortschreiben, solange das Schutzniveau nicht sinkt. Für Anlage 3b gilt § 7.

§ 16 Auswertungen zur Verbesserung von kalle. Zusammengefasste Kennzahlen ohne Personenbezug (AGB § 13) bildet AWAI als eigener Verantwortlicher; Inhalte aus den Daten des Kunden und Angaben zu einzelnen Personen fließen dort nicht ein. Besondere Kategorien nach § 3 und Gespräche mit dem Assistenten wertet AWAI nicht aus; einen Gesprächsausschnitt erhält AWAI nur als Rückmeldung der Person selbst (§ 6). Ein KI-Modell wird mit Inhalten des Kunden nicht trainiert.

Anlage 3a: Technische und organisatorische Maßnahmen

Die Maßnahmen beschreiben den Stand der Produktion am 17.11.2026. Drei Punkte sind noch offen und zu erledigen, bevor echte Kundendaten verarbeitet werden: der Verzicht auf die Missbrauchsüberwachung bei Microsoft, die Entscheidung über eine Virenprüfung hochgeladener Dateien und die eigene Datenbankrolle des Vermittlers für verbundene Firmen.

Bereich (Art. 32 DSGVO)	Maßnahme
Trennung der Kunden	Eine eigene Datenbank je Kunde, zusätzlich Zeilensicherheit (Row Level Security); ein eigener, verschlüsselter Dateibereich je Kunde. Der Kunde wird allein aus der aufgerufenen Adresse bestimmt, nie aus einer Angabe des Browsers. Die Trennung wird mit automatischen Gegentests geprüft. Auch verbundene Firmen greifen nicht aufeinander zu.
Verschlüsselung	Übertragung nur verschlüsselt (TLS ab 1.2, die Datenbank verlangt verschlüsselte Verbindungen, E-Mail-Versand mit STARTTLS). Gespeicherte Daten, Dateien und Sicherungen sind beim Rechenzentrumsbetreiber verschlüsselt (AES-256).
Netz	Die Datenbank ist nur über ein privates Netz erreichbar (Private Endpoint), nicht aus dem Internet. Die Betreiber-Konsole antwortet Fremden nicht.
Schlüssel und Geheimnisse	Schlüsseltresor (Azure Key Vault) mit Lösch- und Bereinigungsschutz. Die Anwendung meldet sich bei Datenbank-Nebendiensten, Speicher und KI-Diensten über verwaltete Identitäten an, ohne dauerhafte Schlüssel im Code.
Zugang der Nutzer	Persönliche Konten, Passwortwechsel bei Erstanmeldung, zweiter Faktor für Verwaltungsrollen (Pflicht für Verwaltungsaufgaben in der App; einzige Ausnahme:

Bereich (Art. 32 DSGVO)	Maßnahme
	Anfragen verbundener Firmen annehmen, ablehnen, einteilen und zurückgeben), Begrenzung von Anmeldeversuchen. Sitzungen im Browser nur in geschützten Cookies mit CSRF-Schutz; App mit Sitzungstoken im sicheren Speicher des Geräts und Biometrie-Sperre. App-Zugänge kommen nicht in die Web-Konsole.
Rechte	Rollen und Rechte je Kunde, vom Kunden selbst gepflegt; Teamleitungen sehen nur ihr Team. Die eigene Lohn- und Auszahlungsübersicht ist ein eigenes Recht. App-Zugänge von Subunternehmern erreichen nur ausdrücklich freigegebene Wege (eigene Einsätze und Zeiten, Berichte, Profil, Postfach); jede neue Route ist für sie zunächst gesperrt. Kritische Schritte (Module schalten, Rollen ändern, Gesamtexport, Anonymisieren) verlangen den zweiten Faktor. Daten übernehmen darf ab Werk nur die Verwaltung; Lesen starten, Übernehmen und Rückgängig verlangen den zweiten Faktor. Das Archiv alter Zeiten sieht nur, wer Benutzer verwaltet; der Assistent liest es nicht.
Endgerät (App ohne Netz)	Ohne Netz merkt sich die App Zeiten, Checklisten und Berichtsteile (Diktat, Foto, Unterschrift) in ihrer eigenen Datenbank auf dem Telefon und sendet sie, sobald Verbindung besteht. Die Datenbank liegt im geschützten App-Bereich des Betriebssystems und ist nicht zusätzlich verschlüsselt. Die Warteschlange ist an die angemeldete Person gebunden. Die App liest den Standort des Telefons nicht (kein GPS).
E-Mail-Versand	Der Postausgang von kalle (Absender noreply@kalle-app.de) versendet nur E-Mails aus den Abläufen der Software an bekannte Empfänger. Absender, Antwort-an und Fußzeile stammen allein aus den Firmendaten des sendenden Kunden. Tageslimit je Kunde (500) und Sperre bei vielen abgelehnten Empfängern. Inhalte werden nicht aufbewahrt, nur ein Versandprotokoll (Empfänger, Betreff, Zeit, Ergebnis). Der Kunde kann stattdessen sein eigenes Postfach nutzen.
Zugriff durch AWAI	Rechte in der Betreiber-Konsole je Person einzeln vergeben (geringste Rechte); keine Betreiber-Funktion zeigt Personendaten der Kunden, außer Rückmeldungen, die Nutzer selbst an AWAI senden, auch Gesprächsausschnitte mit dem Assistenten. Freigabe in die Produktion nur nach

Bereich (Art. 32 DSGVO)	Maßnahme
	manueller Bestätigung.
Protokollierung	Unveränderliches Änderungsprotokoll je Kunde (wer, wann, was), sichtbar für den Kunden; nur die Einträge „Assistent genutzt“ werden nach zwölf Monaten gelöscht. Technische Protokolle ohne Personendaten, 30 Tage. KI-Aufrufe werden ohne Inhalt protokolliert; gespeicherte Gespräche mit dem Assistenten stehen nicht im Protokoll, sondern getrennt und nur für die Person sichtbar.
Integrität von Rechnungen	Festgeschriebene Rechnungen sind in der Datenbank gegen Änderung gesperrt; Rechnungsdateien liegen in einem Archiv mit unveränderlicher Ablage und Echtheitsprüfung per Prüfsumme.
Dateien	Hochgeladene Dateien werden am Inhalt geprüft (nicht nur an der Endung); Zugriff nur über kurzlebige, vom Server signierte Adressen. Gelöschte Dateien sind sieben Tage wiederherstellbar, danach endgültig fort. Rechnungs-XML nimmt nur der Beleg-Eingang an. Beim Umstieg nimmt die Software auch ZIP-Dateien an: bis 200 MB, 2.000 Dateien und 1 GB entpackt, jede Datei bis 25 MB und am Inhalt geprüft. Eine Virenprüfung gibt es noch nicht.
Verfügbarkeit und Sicherung	Sicherungen der Datenbank mit Wiederherstellung auf jeden Zeitpunkt der letzten 14 Tage, georedundant innerhalb der EU (Schweden). Überwachung von außen aus zwei EU-Standorten alle 15 Minuten, Warnungen bei Last und Speicher. Notfallplan für den Ausfall einer Region (geschätzte Wiederanlaufzeit 3–5 Stunden, noch nicht geübt).
Sichere Entwicklung	Automatische Tests vor jeder Auslieferung, Prüfung aller Abhängigkeiten und des Container-Abbilds auf bekannte Schwachstellen, signierte App.
Löschung	Löschkonzept mit Fristen je Datenklasse: Wiedervorlage zur Anonymisierung ausgeschiedener Mitarbeiter (Vorgabe 36 Monate), Anonymisieren von Privatkunden, Gespräche mit dem Assistenten 90 Tage nach der letzten Nutzung, Rohtexte von Berichten zwölf Monate nach dem Abschicken, KI-Verbrauchszeilen nach zwölf Monaten ohne Person und drei Jahre nach Jahresende ganz gelöscht, Rohwerte und Tabellendateien der Datenübernahme 30 Tage nach Übernahme oder Verwerfen, Löschung aller Daten außer dem Rechnungsarchiv 90 Tage nach Vertragsende,

Bereich (Art. 32 DSGVO)	Maßnahme
	Sicherungen höchstens 14 Tage nach. Kopien und Vermittlerdaten verbundener Firmen werden zwölf Monate nach dem Ende der Verbindung gelöscht.
KI-Funktionen	Jede Funktion einzeln abschaltbar; Monatsbudget je Kunde; Eingaben auf das Nötige gekürzt (z. B. Berichte ohne Namen; der Angebotsvorschlag erhält den Projekttitel ohne Kundennamen). PDF-Anfragen gehen als Text mit höchstens 8.000 Zeichen an das Modell, Scans als Bilder (höchstens zwei Seiten an den Assistenten, sechs an den Angebotsvorschlag). E-Rechnungen im Beleg-Eingang liest AWAI ohne KI. Die Abfrage von Abwesenheiten nennt Krankheit, Kinderkrank und Mutterschutz nur „abwesend“; was eine Person selbst sagt, tippt oder auswählt, geht so an die KI. Sprachaufnahmen werden nach der Umschrift gelöscht, Kalles Stimme wird nicht gespeichert. Der Assistent sieht und tut nie mehr als die fragende Person; schreibende Schritte bestätigt eine Person, auch im Agent-Betrieb. Löschen fragt immer und geht nie per Sprache. Rechnungen festschreiben und stornieren verlangt eine Prüfbestätigung der Person und den zweiten Faktor. Einzelheiten: KI-Handreichung (Heft 99, Teil B).
Verbundene Firmen	Keine Firma greift auf die Datenbank einer anderen zu. Ein Hintergrundlauf mit eigener Verbindung je Firma kopiert einen festen Feldkatalog, jede Abfrage des Vermittlers prüft die Beteiligung. Verbinden geht nur nach Bestätigung der anderen Firma, ohne Verzeichnis; Name und Ort zu einer Kalle-ID sind nur mit Freigabe der Firma nachschlagbar, höchstens 20 Abfragen am Tag. Vor der Annahme liegt nur die Vorschau in der Plattform-Datenbank und wird bei der Entscheidung gelöscht. Der Vermittler nutzt in Produktion noch die Anwendungsrolle; eine eigene Datenbankrolle ist vorbereitet, aber nicht eingerichtet.
Organisation	Vertraulichkeitsverpflichtung aller Personen mit Zugang; dokumentierte Abläufe für Wiederherstellung, Schlüsselverlust und Mandantenlöschung; Datenschutz-Ansprechperson: Daniel Schrenk, info@awai-analytics.com.