Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 Abs. 3 DSGVO – Anlage 2 zum SaaS-Rahmenvertrag. Version 2.0, Stand 14. Oktober 2026.

zwischen [Firma des Kunden], [Anschrift] („Verantwortlicher") und der

Aldor GmbH, Wilmersdorfer Straße 60, 10627 Berlin („Auftragsverarbeiter").

Präambel

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen nach Maßgabe des Rahmenvertrags („Hauptvertrag"). Hierbei verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO. Die in Art. 4 DSGVO definierten Begriffe gelten entsprechend.

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

(1) Gegenstand und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag und sind in Anlage 1 näher beschrieben.

(2) Die Verarbeitung umfasst die Bereitstellung der Anwendung „Aldor" einschließlich der mobilen App für Beschäftigte des Verantwortlichen. Dazu gehören insbesondere Klienten- und Leistungsdokumentation, Anfragen, Touren- und Einsatzplanung, Zeiterfassung mit Standortnachweis, Personalverwaltung und Vorbereitung der Lohnabrechnung, Abrechnung mit Klienten und Kostenträgern, Kommunikation (E-Mail einschließlich angebundener Postfächer, Push-Benachrichtigungen, Chat), Dokumentenverwaltung mit elektronischen Unterschriften, das White-Label-Endkundenportal, KI-gestützte Hilfsfunktionen, die Übernahme von Daten aus Vorsystemen sowie optional zuschaltbare Zusatzdienste (z. B. elektronische Abrechnung nach § 105 SGB XI, Zahlungsabgleich über das Geschäftskonto, postalischer Briefversand). Anlage 1 beschreibt die Verarbeitung im Einzelnen.

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Nach dessen Beendigung gilt § 10.

§ 2 Art der Daten und Kategorien betroffener Personen

Die Arten der verarbeiteten personenbezogenen Daten und die Kategorien der betroffenen Personen ergeben sich aus Anlage 1. Die Verarbeitung umfasst auch besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO (insbesondere Gesundheitsdaten der Klienten wie Pflegegrad und Dokumentation sowie Gesundheitsdaten der Beschäftigten); hierfür gelten die erhöhten Anforderungen nach § 4 und § 12. Verarbeitet der Verantwortliche Sozialdaten, insbesondere bei der Abrechnung mit Pflegekassen, erfolgt die Verarbeitung im Auftrag zugleich nach § 80 SGB X.

§ 3 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich im Hinblick auf eine Übermittlung in Drittländer, sofern nicht eine Rechtsvorschrift, der der Auftragsverarbeiter unterliegt, die Verarbeitung vorschreibt.

(2) Weisungen werden grundsätzlich in Textform erteilt und dokumentiert. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt.

§ 4 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter gewährleistet insbesondere:

- Vertraulichkeit: Er verpflichtet alle zur Verarbeitung befugten Personen zur Vertraulichkeit, soweit sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung umfasst, soweit einschlägig, die Wahrung von Berufsgeheimnissen nach § 203 StGB (siehe § 12).
- Sicherheit der Verarbeitung: Er trifft alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (Anlage 2).
- Unterstützung: Er unterstützt den Verantwortlichen mit angemessenen Maßnahmen bei der Erfüllung der Betroffenenrechte (Art. 12–23 DSGVO) sowie der Pflichten aus Art. 32–36 DSGVO.
- Meldung: Er meldet Verletzungen des Schutzes personenbezogener Daten gemäß § 8.

- Löschung/Rückgabe: Er verfährt nach Vertragsende gemäß § 10.
- Nachweise: Er stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen gemäß § 9.
- Datenschutzbeauftragter: Der Auftragsverarbeiter hat die heyData GmbH als externen Datenschutzbeauftragten benannt; Kontakt: datenschutz@aldor.ai.

§ 5 Technische und organisatorische Maßnahmen (TOM)

Die vom Auftragsverarbeiter getroffenen Maßnahmen nach Art. 32 DSGVO sind in Anlage 2 beschrieben.

Der Auftragsverarbeiter darf diese im Laufe der Zeit weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt seine allgemeine Genehmigung zur Hinzuziehung der in Anlage 3 aufgeführten Unterauftragsverarbeiter.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mit einer Frist von vier Wochen vorab in Textform. Dem Verantwortlichen steht insoweit ein Widerspruchsrecht aus wichtigem Grund zu.

(3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter durch Vertrag zu denselben Datenschutzpflichten, die in diesem Vertrag festgelegt sind, einschließlich – soweit einschlägig – der Verpflichtung nach § 203 Abs. 4 StGB.

§ 7 Betroffenenrechte

Wendet sich eine betroffene Person mit einem Begehren nach Art. 15–22 DSGVO unmittelbar an den Auftragsverarbeiter, leitet dieser das Begehren unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst, sofern nicht der Verantwortliche dies anweist.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach

Bekanntwerden, und stellt die zur Erfüllung der Pflichten des Verantwortlichen aus Art. 33, 34 DSGVO erforderlichen Informationen bereit.

§ 9 Kontrollrechte und Nachweise

(1) Der Auftragsverarbeiter weist die Einhaltung seiner Pflichten vorrangig durch geeignete Nachweise nach (z. B. aktuelle Zertifikate, Testate oder Prüfberichte anerkannter Stellen).
(2) Soweit dies zur Erfüllung der Kontrollpflichten des Verantwortlichen erforderlich ist, ermöglicht der Auftragsverarbeiter Überprüfungen, einschließlich Inspektionen, die nach angemessener Vorankündigung während der üblichen Geschäftszeiten und ohne unverhältnismäßige Betriebsstörung durchzuführen sind.

§ 10 Löschung und Rückgabe nach Vertragsende

Nach Abschluss der Verarbeitungstätigkeiten löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht eine gesetzliche Pflicht zur Speicherung besteht. Bis zum Ablauf der in § 12 des Rahmenvertrags genannten Exportfrist hält er die Daten zum Export bereit.

§ 11 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Innenverhältnis bleiben die Haftungsregelungen des Hauptvertrags bzw. der AGB unberührt, soweit Art. 82 DSGVO dem nicht entgegensteht.

§ 12 Besondere Kategorien und Berufsgeheimnis (§ 203 StGB)

(1) Da die Verarbeitung Gesundheitsdaten (Art. 9 DSGVO) umfasst, trifft der Auftragsverarbeiter erhöhte Schutzmaßnahmen nach Anlage 2, insbesondere Verschlüsselung, strikte Zugriffstrennung je Mandant und protokollierte Zugriffskontrolle.
(2) Soweit der Verantwortliche oder von ihm eingesetzte Personen einer Schweigepflicht nach § 203 StGB unterliegen, wird der Auftragsverarbeiter als sonstige mitwirkende Person nach § 203

Abs. 3 S. 2 StGB tätig. Er und alle von ihm hinzugezogenen Personen sind nach § 203 Abs. 4 StGB zur Geheimhaltung verpflichtet. Ergänzend gilt § 6 des Rahmenvertrags.

§ 13 Drittlandtransfer

(1) Die Verarbeitung findet grundsätzlich innerhalb der Bundesrepublik Deutschland bzw. der EU/des EWR statt. Hosting, Datenbank, Dokumentenablage und E-Mail-Versand erfolgen in Rechenzentren in Deutschland. Verschlüsselte Sicherungskopien liegen zusätzlich in einem Rechenzentrum der Hetzner Online GmbH in Helsinki (Finnland, EU).

(2) Soweit einzelne in Anlage 3 aufgeführte Unterauftragsverarbeiter Daten in Drittländern verarbeiten (insbesondere Push-Benachrichtigungsdienste, Kartendienste und der optionale postalische Briefversand), erfolgt dies ausschließlich auf Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission (Art. 45 DSGVO – derzeit für die Schweiz) oder geeigneter Garantien nach Art. 44 ff. DSGVO (insbesondere EU-Standardvertragsklauseln, Art. 46 Abs. 2 lit. c DSGVO) und beschränkt auf die in Anlage 3 genannten Datenarten.

§ 14 Schlussbestimmungen

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen in Fragen des Datenschutzes die Regelungen dieses AVV vor. Im Übrigen gelten die Schlussbestimmungen des Rahmenvertrags entsprechend. Änderungen bedürfen der Textform.

Anlage 1 – Beschreibung der Verarbeitung

Merkmal	Beschreibung
Gegenstand	Bereitstellung und Betrieb der SaaS-Anwendung „Aldor" einschließlich der mobilen App für Beschäftigte des Verantwortlichen
Art der Verarbeitung	Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Abgleichen, Übermitteln, Einschränken, Löschen

Zweck	Klienten- und Leistungsdokumentation; Anfragen und Angebote; Touren- und Einsatzplanung; Zeiterfassung mit Standortnachweis über die mobile App; Personalverwaltung und Vorbereitung der Lohnabrechnung; Abrechnung mit Klienten und Kostenträgern, optional einschließlich elektronischer Abrechnung nach § 105 SGB XI; Zahlungsabgleich über das Geschäftskonto (optional); Kommunikation mit Klienten, Angehörigen und Beschäftigten (E-Mail einschließlich angebundener Postfächer, Push-Benachrichtigungen, Chat, Briefpost); Dokumentenverwaltung und elektronische Unterschriften; Endkundenportal; KI-gestützte Hilfsfunktionen; Übernahme von Daten aus Vorsystemen; Support und Fehleranalyse einschließlich zeitlich begrenzter, protokollierter Kontoansicht
Kategorien betroffener Personen	Klienten und Interessenten des Verantwortlichen; deren Angehörige, Kontaktpersonen, gesetzliche Betreuer und Bevollmächtigte; Beschäftigte des Verantwortlichen und deren Angehörige (z. B. Notfallkontakte); Ansprechpartner bei Kostenträgern, Ärzten und sonstigen Stellen; sonstige Korrespondenzpartner
Datenarten (allgemein)	Stamm- und Kontaktdaten; Zugangsinformationen zu Wohnungen (z. B. Schlüssel, Zugangscodes); Termin-, Einsatz- und Leistungsdaten; Leistungsansprüche und Bewilligungen; Versicherten- und Sozialdaten (z. B. Krankenversichertennummer, Pflegekasse); Abrechnungs- und Zahlungsdaten einschließlich Bankverbindungen; Beschäftigtendaten (Vertrags-, Arbeitszeit-, Abwesenheits- und Lohndaten, Steuer-Identifikationsnummer, Sozialversicherungsnummer, Angaben zu Lohnpfändungen); Standortdaten (Position beim Ein- und Ausstempeln, Position während einer aktiven Tour); Unterschriften; Kommunikationsinhalte und Dokumente; Nutzungs-, Geräte- und Protokolldaten
Besondere Kategorien (Art. 9, Art. 10)	Gesundheitsdaten der Klienten (z. B. Pflegegrad, Bescheide, Pflege- und Gesundheitshinweise, Betreuungs- und Leistungsdokumentation); Gesundheitsdaten der Beschäftigten (z. B. Arbeitsunfähigkeit, Schwerbehinderung); Religionszugehörigkeit (Kirchensteuermerkmal); Angaben zu Führungszeugnissen, soweit der Verantwortliche sie erfasst
Empfänger	Übermittlungen erfolgen nur auf Veranlassung des Verantwortlichen: an Klienten und deren Angehörige, an Kostenträger und deren Datenannahmestellen, an vom Verantwortlichen gewählte Abrechnungs-, Factoring- und Buchhaltungsdienste, an Steuerberater oder Lohnbüro sowie an über Freigabelinks benannte Dritte
Ausgeschlossen	Daten aus Leistungen nach dem Vierten Kapitel SGB V (insb. § 37, § 132/132a SGB V) – vgl. § 7 Rahmenvertrag

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

Vertraulichkeit

- Zutrittskontrolle: Hosting in zertifizierten Rechenzentren in Deutschland (Falkenstein, Nürnberg), verschlüsselte Sicherungskopien in Finnland (Helsinki), jeweils mit Zutrittsschutz des Betreibers.
- Zugangskontrolle: Individuelle Benutzerkonten, verfügbare Multi-Faktor-Authentifizierung, Passwort-Richtlinien, automatische Sperrmechanismen.
- Zugriffskontrolle: Rollen- und Berechtigungskonzept; strikte Mandantentrennung durch Row-Level-Security auf Datenbankebene (PostgreSQL RLS) je Tenant; Protokollierung von Zugriffen.
- Trennungskontrolle: Logische Trennung der Mandantendaten; getrennte Test- und Produktivsysteme.

Integrität

- Weitergabekontrolle: Transportverschlüsselung (TLS) für alle Verbindungen; Verschlüsselung sensibler Daten im Ruhezustand.

- Eingabekontrolle: Protokollierung von Änderungen an personenbezogenen Daten (Audit-Log).

Verfügbarkeit und Belastbarkeit

- Regelmäßige, verschlüsselte Backups; dokumentiertes Wiederherstellungsverfahren; Monitoring und Alerting.
- Schutzmaßnahmen gegen Schadsoftware und unbefugte Zugriffe; regelmäßige Aktualisierung der Systeme.

Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen (Art. 32 Abs. 1
lit. d DSGVO).
- Auftragskontrolle: vertragliche Bindung der Unterauftragsverarbeiter; dokumentierte Weisungen.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Standort / Region	Datenarten
Hetzner Online GmbH	Hosting, Datenbank, Object Storage, E-Mail-Versand, verschlüsselte Sicherungskopien	Deutschland (Falkenstein, Nürnberg); Sicherungskopien Finnland (Helsinki)	Alle in der Anwendung verarbeiteten Daten
BANKSapi Technology GmbH	Kontoinformationsdienst (Bankabgleich)	Deutschland (München)	Bankverbindungs- und Umsatzdaten
Google Cloud EMEA Ltd. (Vertex AI)	KI-gestützte Hilfsfunktionen	EU (Frankfurt), keine Speicherung der Inhalte (Zero Data Retention)	Zur KI-Verarbeitung übergebene Inhalte
Google Ireland Limited (Google Maps Platform)	Adress-Autovervollständigung, Geokodierung, Routenberechnung, Kartendarstellung	Globale Google-Infrastruktur (EU-Standardvertragsklauseln)	Adressen, Koordinaten, IP-Adressen und Geräteinformationen der Nutzer
Apple Distribution International Ltd. (APNs)	Push-Benachrichtigungen (iOS)	Irland (EU-Standardvertragsklauseln)	Push-Token, Benachrichtigungstexte (können Namen und Nachrichtenauszüge enthalten)
Google Ireland Limited (Firebase Cloud Messaging)	Push-Benachrichtigungen (Android)	Globale Google-Infrastruktur (EU-Standardvertragsklauseln)	Push-Token, Benachrichtigungstexte (können Namen und Nachrichtenauszüge enthalten)
Pingen GmbH	Postalischer Briefversand: Druck, Kuvertierung, Zustellung (optional)	Schweiz, Zürich (Angemessenheitsbeschluss der EU-Kommission, Art. 45 DSGVO)	Empfängername und Anschrift, Inhalte der versandten Dokumente (können Gesundheitsdaten umfassen)

PflegeHelfer24 GmbH	Softwareentwicklung, Wartung und Support der Anwendung; Zugriff auf personenbezogene Daten nur im Einzelfall, soweit für Fehleranalyse oder Support erforderlich	Deutschland (Berlin)	Alle in der Anwendung verarbeiteten Daten

Aldor GmbH
gez. Benedikt Hübenthal, Geschäftsführer
Berlin, 4. November 2026
✓ Anbieter · elektronisch signiert

[Firma des Kunden]
Ort, Datum / Unterschrift
Kunde