Technische und organisatorische Maßnahmen (TOM)

der PflegeHelfer24 GmbH für den Betrieb der Anwendung „Aldor" – Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 DSGVO. Version 1.0, Stand June 24, 2026.

1. Geltungsbereich und Grundsätze

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, die die PflegeHelfer24 GmbH („Anbieter") zum Schutz personenbezogener Daten – einschließlich besonderer Kategorien nach Art. 9 DSGVO (insbesondere Gesundheitsdaten) – beim Betrieb der Anwendung „Aldor" getroffen hat. Die Maßnahmen berücksichtigen den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Personen. Sie werden regelmäßig überprüft und fortgeschrieben (Ziffer 7).

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Betrieb ausschließlich in ISO-27001-zertifizierten Rechenzentren der Hetzner Online GmbH in Deutschland (Falkenstein, Nürnberg) mit Zutrittsschutz des Betreibers.
- Kein physischer Zugriff des Anbieters auf die Server erforderlich; die Administration erfolgt ausschließlich aus der Ferne über verschlüsselte Verbindungen.

Zugangskontrolle

- Individuelle Benutzerkonten; keine Sammel- oder Funktionskonten.
- Passwort-Richtlinien und sichere, gesalzene Passwort-Speicherung (bcrypt); Zwei-Faktor-Authentifizierung für Benutzerkonten.
- Automatische Sperrmechanismen und Sitzungsverwaltung mit Abmeldung.
- Administrativer Systemzugriff nur für einen eng begrenzten Personenkreis, ausschließlich über persönliche SSH-Schlüssel; kein Passwort-Login auf Produktionssystemen.

Zugriffskontrolle

- Abgestuftes Rollen- und Rechtesystem: 15 Datenbereiche, je Bereich Keine/Ansehen/Bearbeiten, zusätzlich Reichweiten-Begrenzung (nur eigene, nur zugewiesene oder alle Datensätze) und

optionale Standort-Einschränkung je Rollenzuweisung.

- Jede Anfrage wird serverseitig autorisiert (Berechtigungsprüfung pro Aktion); Bearbeitungsrechte sind stets eine Teilmenge der Leserechte.
- Need-to-know-Prinzip für Beschäftigte des Anbieters; Produktivzugriffe nur anlassbezogen.
- Support-Zugriff („Ansicht als Nutzer"): Ein Zugriff des Anbieters auf ein Kundenkonto erfolgt ausschließlich anlassbezogen zur Störungs- und Fehlerbehebung, durch ausdrücklich berechtigte, zur Vertraulichkeit (auch § 203 StGB) verpflichtete Beschäftigte. Der Zugriff ist zeitlich strikt begrenzt (automatische Beendigung nach 30 Minuten), jederzeit serverseitig widerrufbar und lückenlos in einem manipulationssicheren (append-only) Audit-Log protokolliert (Auslöser, betroffenes Konto, Grund, Zeitpunkt). Rechtsverbindliche Handlungen — elektronische Signaturen, Abtretungserklärungen, Änderung des Pflegegrads, Einreichung von Pflegekassen-Abrechnungen, Festschreibung von Leistungsnachweisen — sind dabei technisch gesperrt. Änderungen werden in der Änderungshistorie als „Aldor Support" ausgewiesen. Ein Support-Zugriff stellt keine Unterauftragsverarbeitung dar (kein Dritter wird hinzugezogen).

Trennungskontrolle

- Strikte Mandantentrennung auf Datenbankebene durch PostgreSQL Row-Level-Security: jede Zeile ist an die Organisation des Kunden gebunden, die Datenbank erzwingt die Trennung zusätzlich zur Anwendungsschicht.
- Getrennte Entwicklungs-, Staging- und Produktionsumgebungen mit getrennten Datenbeständen und getrennten Schlüsseln; keine Produktivdaten in Entwicklungs- oder Testumgebungen.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

- Telemetrie (Protokolle, Metriken, Fehlerberichte) enthält ausschließlich pseudonyme Kennungen (UUIDs) – keine Klarnamen und keine Gesundheitsdaten. Automatische Prüfungen in der Entwicklungs-Pipeline verhindern, dass personenbezogene Daten in Protokolle gelangen.
- IP-Adressen werden in der Telemetrie nur gekürzt oder mit täglich wechselndem Schlüssel gehasht verarbeitet.
- Hintergrundaufträge transportieren ausschließlich pseudonyme Datensatz-Kennungen; die eigentlichen Daten werden erst innerhalb der geschützten Verarbeitung geladen.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Transportverschlüsselung (TLS) für sämtliche Verbindungen – zwischen Endgerät und Anwendung ebenso wie zwischen den Systemkomponenten.
- Anwendungsseitige Feldverschlüsselung (AES-256-GCM) für personenbezogene Daten und Gesundheitsdaten: Namen, Kontaktdaten, Adressen, Pflegegrade, Dokumentation u. a. werden verschlüsselt, bevor sie die Datenbank erreichen. Die Schlüssel werden außerhalb der Datenbank verwaltet; ein entwendeter Datenbankabzug bleibt unlesbar.
- Sämtliche Backups sind verschlüsselt.

Eingabekontrolle

- Lückenloser Änderungs-Audit-Trail: Änderungen an Datensätzen werden versioniert protokolliert; Signatur-Ereignisse werden unveränderlich (append-only) gespeichert.
- Elektronische Signaturen werden als PAdES-signierte PDF-Dokumente mit Signaturprotokoll erzeugt.
- Löschungen erfolgen zweistufig (Soft-Delete mit kontrollierter Endlöschung), sodass versehentliche Löschungen nachvollziehbar und korrigierbar sind.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Tägliche, verschlüsselte Backups in einen räumlich getrennten Objektspeicher in Deutschland; kontinuierliche Sicherung des Transaktionsprotokolls (Point-in-Time-Recovery).
- Replikation der Datenbank auf einen Standby-Server; dokumentierte Wiederherstellungs- und Failover-Verfahren (Runbooks).
- Automatisiertes Monitoring und Alarmierung für alle Systemkomponenten – selbst betrieben auf eigener Infrastruktur, ohne Übermittlung an Drittanbieter.
- Regelmäßige und zeitnahe Sicherheitsaktualisierungen von Betriebssystem und Abhängigkeiten.
- Lasttrennung: rechenintensive Aufgaben laufen getrennt vom Web-Betrieb in einer Hintergrund-Warteschlange.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Datenschutz-Management

- Externer Datenschutzbeauftragter (heyData GmbH); Verzeichnis von Verarbeitungstätigkeiten; dokumentiertes Dienstleister-Verzeichnis mit jährlicher Überprüfung aller Unterauftragsverarbeiter.
- Vertraulichkeitsverpflichtung aller Beschäftigten, einschließlich der Verpflichtung nach § 203 Abs. 4 StGB, soweit einschlägig.

Incident-Response-Management

- Dokumentierter Prozess zur Erkennung, Bewertung und Meldung von Verletzungen des Schutzes personenbezogener Daten; Meldung an den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden (vgl. § 8 AVV).

Sichere Softwareentwicklung

- Vier-Augen-Prinzip: jede Änderung durchläuft eine Code-Review, automatisierte Tests und statische Prüfungen, bevor sie produktiv geht.
- Änderungen werden vor der Produktivsetzung auf einer Staging-Umgebung erprobt; Produktiv-Releases sind versioniert und nachvollziehbar.
- Datenschutzprüfungen sind in die Entwicklungs-Pipeline integriert (u. a. automatische Prüfung gegen Protokollierung personenbezogener Daten).

Auftragskontrolle

- Schriftliche Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern; die aktuelle Liste ist öffentlich einsehbar (Trust Center) und Bestandteil des AVV (Anlage 3).
- Unterauftragsverarbeiter werden vor Beauftragung auf EU-Datenresidenz und – bei Drittlandbezug – auf geeignete Garantien nach Art. 44 ff. DSGVO geprüft.

6. Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- Datenminimierung: erhoben und verarbeitet wird nur, was für die Leistungserbringung erforderlich ist; keine Werbe-Tracker, kein Profiling.
- Aufbewahrungs- und Löschkonzept entlang der gesetzlichen Fristen; nach Vertragsende Datenexport und anschließende Löschung nach Maßgabe des AVV.
- Neue Funktionen werden vor Einführung auf Datenschutz-Auswirkungen geprüft.

7. Weiterentwicklung

Der Anbieter darf die beschriebenen Maßnahmen fortentwickeln und durch gleichwertige oder wirksamere Maßnahmen ersetzen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

Maßgeblich ist die jeweils im Trust Center veröffentlichte Fassung.