Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

für die Nutzung der Software AlltagQuest

Stand: Mai 2026 –

§ 1 Vertragsparteien

Zwischen

dem Auftraggeber (Verantwortlicher im Sinne der DSGVO):

[Name der Einrichtung / des Trägers] [Anschrift] [Ansprechpartner, E-Mail]

– nachfolgend 'Auftraggeber' –

und

dem Auftragnehmer (Auftragsverarbeiter):

Frank M. Schaefer – Soziale und Digitale Dienstleistungen Am Industriehafen 4a, 24937 Flensburg E-Mail: kontakt@alltagquest.de

– nachfolgend 'Auftragnehmer' –

wird folgender Vertrag zur Auftragsverarbeitung geschlossen:

§ 2 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Bereitstellung und des Betriebs der webbasierten Software AlltagQuest (Software-as-a-Service).

(2) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags (Nutzungsvertrag für AlltagQuest). Nach Vertragsende werden die Daten gemäß § 10 dieses AVV behandelt.

(3) Die Verarbeitung erfolgt ausschließlich in der Europäischen Union, derzeit auf Servern der IONOS SE in Deutschland.

§ 3 Art und Zweck der Verarbeitung

(1) Art der Verarbeitung: Speicherung, Veränderung, Abfrage, Verwendung, Übermittlung (an den Auftraggeber), Löschung von personenbezogenen Daten im Rahmen des Betriebs der SaaS-Anwendung.

(2) Zweck der Verarbeitung: Bereitstellung einer webbasierten Anwendung zur Dokumentation, Planung und Begleitung im Bereich der Kinder- und Jugendhilfe gemäß dem zwischen den Parteien geschlossenen Nutzungsvertrag.

§ 4 Kategorien betroffener Personen und Daten

(1) Kategorien betroffener Personen:

Kategorie	Beschreibung
Betreute Personen	Kinder und Jugendliche in Einrichtungen der Jugendhilfe
Mitarbeiter des AG	Betreuer, Erzieher, Leitung der Einrichtung
Sonstige	Sorgeberechtigte, Bezugsbetreuer, Ansprechpartner

(2) Kategorien personenbezogener Daten:

Datenkategorie	Beispiele
Stammdaten	Name, Vorname, Geburtsdatum, Anschrift
Kontaktdaten	E-Mail, Telefonnummer
Betreuungsdaten	Stimmungsverläufe, Tagesgespräche, Entwicklungsziele (Quests), Termine, Anträge, Routinen, Dienstpläne
Nutzungsdaten	Login-Zeiten, Session-Daten, Geräteinformationen
Abrechnungsdaten	Rechnungsanschrift, Zahlungsinformationen

(3) Besondere Kategorien: Es werden grundsätzlich keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO verarbeitet. Sollte der Auftraggeber dennoch solche Daten eingeben (z. B. Gesundheitsdaten in Freitextfeldern), erfolgt dies in alleiniger Verantwortung des Auftraggebers.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet.

(2) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragnehmer trifft alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (siehe Anlage: TOMs).

(4) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Betroffenenrechten (Art. 15–22 DSGVO).

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten gemäß Art. 32–36 DSGVO (Datensicherheit, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Verletzungen des Schutzes personenbezogener Daten (Art. 33 Abs. 2 DSGVO).

§ 6 Unterauftragsverarbeiter

(1) Der Auftragnehmer setzt derzeit folgende Unterauftragsverarbeiter ein:

Unternehmen	Anschrift	Leistung	Ort der Verarbeitung
IONOS SE	Elgendorfer Str. 57, 56410 Montabaur	Webhosting, Datenbank	Deutschland

(2) Der Auftragnehmer darf weitere Unterauftragsverarbeiter nur mit vorheriger allgemeiner schriftlicher Genehmigung des Auftraggebers einsetzen. Über beabsichtigte Änderungen wird der Auftraggeber informiert und kann Einspruch erheben.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich von der Einhaltung dieses Vertrags zu überzeugen. Der Auftragnehmer stellt hierfür die erforderlichen Informationen zur Verfügung.

(2) Inspektionen können nach angemessener Vorankündigung (mindestens 14 Tage) während der Geschäftszeiten durchgeführt werden. Alternativ kann der Auftragnehmer aktuelle Zertifizierungen, Berichte oder Audit-Ergebnisse vorlegen.

§ 8 Datenübermittlung in Drittstaaten

Eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation findet nicht statt und darf nur mit vorheriger dokumentierter Weisung des Auftraggebers und unter Einhaltung der Voraussetzungen des Kapitels V DSGVO erfolgen.

§ 9 Meldepflichten bei Datenschutzverletzungen

(1) Der Auftragnehmer meldet dem Auftraggeber unverzüglich jede Verletzung des Schutzes personenbezogener Daten.

(2) Die Meldung enthält mindestens: Art der Verletzung, betroffene Datenkategorien und Personen, wahrscheinliche Folgen, ergriffene Abhilfemaßnahmen.

§ 10 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Hauptvertrags stellt der Auftragnehmer dem Auftraggeber sämtliche personenbezogenen Daten für 30 Tage über die Export-Funktion der Software zur Verfügung.

(2) Nach Ablauf dieser Frist löscht der Auftragnehmer sämtliche personenbezogenen Daten unwiderruflich, sofern nicht eine gesetzliche Aufbewahrungspflicht besteht.

(3) Der Auftragnehmer bestätigt die Löschung auf Verlangen schriftlich.

§ 11 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV vor.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Flensburg.

Ort, Datum _____ Auftraggeber (Einrichtung)	Ort, Datum _____ Auftragnehmer (Frank M. Schaefer)

Anlage: Technische und organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO

1. Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren:

Maßnahme	Umsetzung
Serverstandort	Rechenzentrum IONOS SE in Deutschland mit Zutrittskontrollsystem, Videoüberwachung und 24/7-Wachpersonal

Arbeitsplatz	Verschlossener Arbeitsbereich des Auftragnehmers, Zugang nur für autorisierte Personen

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen können:

Maßnahme	Umsetzung
Passwortrichtlinie	Mindestlänge, bcrypt-Hashing (Kostenfaktor 10+), keine Klartextspeicherung
Brute-Force-Schutz	Automatische Sperrung nach 5 Fehlversuchen pro IP für 15 Minuten
Session-Management	Automatischer Timeout, Session-Regeneration bei Login, sichere Cookie-Attribute
SSH/DB-Zugang	Nur über SFTP/SSH mit Key-Authentifizierung, DB-Zugang nur über Hosting-Backend

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass nur berechtigte Personen auf Daten zugreifen:

Maßnahme	Umsetzung
Rollenkonzept	4-stufiges Rollenmodell: Systemmanager, Admin, Betreuer, Jugendlicher – jeweils mit eingeschränkten Berechtigungen
Mandantentrennung	Strenge Datenisolierung durch institution_id auf allen Datenbankebenen
Kontextwechsel	Systemmanager-Zugriff auf Kundendaten nur über zeitlich begrenzte, protokollierte Tokens

4. Weitergabekontrolle / Übertragungssicherheit

Maßnahme	Umsetzung
Transportverschlüsselung	TLS/SSL für alle Verbindungen (HTTPS erzwungen)
E-Mail-Versand	Versand über authentifizierten SMTP mit TLS
Datenexport	CSV/PDF-Export nur durch authentifizierte, autorisierte Benutzer

5. Eingabekontrolle

Maßnahme	Umsetzung
Protokollierung	Alle Änderungen an Stammdaten werden mit Benutzer-ID, Zeitstempel und Aktion protokolliert (created_by, updated_by)
Versionierung	Tagesgespräche und Quests haben created_at/updated_at Timestamps

6. Auftragskontrolle

Maßnahme	Umsetzung
Weisungsbindung	Verarbeitung ausschließlich nach dokumentierter Weisung des Auftraggebers

Vertragliche Regelung	Dieser AVV regelt Umfang und Zweck der Verarbeitung verbindlich
Unterauftragnehmer	Nur mit Genehmigung des AG, derzeit: IONOS SE (Hosting)

7. Verfügbarkeitskontrolle

Maßnahme	Umsetzung
Backups	Tägliche automatische Datenbank-Backups durch Hosting-Provider, zusätzlich manuelle Backups
Redundanz	IONOS-Rechenzentrum mit redundanter Stromversorgung und Netzwerkanbindung
Monitoring	Überwachung der Erreichbarkeit, automatische Benachrichtigung bei Ausfällen

8. Trennungsgebot

Maßnahme	Umsetzung
Mandantentrennung	Logische Trennung aller Kundendaten durch institution_id auf Datenbankebene
Testdaten	Demo-System mit separatem is_demo-Flag, keine Vermischung mit Produktivdaten
Zweckbindung	Daten werden ausschließlich für den vereinbarten Zweck verarbeitet