DSGVO-Compliance-Bericht

AlltagQuest – Progressive Web App

für die stationäre Kinder- und Jugendhilfe

Datenschutz- und Sicherheitsmaßnahmen
Technische und organisatorische Umsetzung

Frank M. Schaefer
Soziale und Digitale Dienstleistungen
Am Industriehafen 4a, 24937 Flensburg
Tel: 0461 – 406 807 85 | support@alltagquest.de

Stand: März 2026

Für Einrichtungsleitungen, Datenschutzbeauftragte und Aufsichtsbehörden

Inhaltsverzeichnis

1. Hosting und Infrastruktur

AlltagQuest wird ausschließlich auf Servern in Deutschland betrieben. Es findet keine Datenübertragung in Drittländer statt.

Hosting-Anbieter

- IONOS SE, Elgendorfer Str. 57, 56410 Montabaur
- Rechenzentren in Deutschland (ISO 27001 zertifiziert)
- Keine Datenübertragung in Drittländer
- Server-Standort: Deutschland (DSGVO-konform)

Technische Eckdaten

- PHP 8.2, MySQL/MariaDB, Apache
- Verschlüsselte Datenbankverbindung
- Automatische Backups durch IONOS
- SSH-Zugang für Administration (kein FTP)

> **Sensible Dateien: Zugangsdaten (.credentials.php) werden serverseitig blockiert. Die .htaccess verhindert Zugriff auf .sql, .env, .log, .bak und Konfigurationsdateien.**

---

2. Transportverschlüsselung und Security Headers

HTTPS/TLS

- HTTPS wird erzwungen (HTTP 301-Redirect in .htaccess)
- HSTS-Header mit max-age=31536000 (1 Jahr) inkl. Subdomains
- TLS 1.2+ für alle Verbindungen
- E-Mail-Versand über Brevo SMTP mit STARTTLS (Port 587)

Security Headers

- Content-Security-Policy (CSP): Strikte Quellenbeschränkung
- X-Frame-Options: SAMEORIGIN (Clickjacking-Schutz)
- X-Content-Type-Options: nosniff (MIME-Sniffing-Prävention)
- Referrer-Policy: strict-origin-when-cross-origin
- Permissions-Policy: Kamera, Mikrofon, Geolocation deaktiviert

Rechtsgrundlage: Art. 32 DSGVO (Sicherheit der Verarbeitung)

---

3. Authentifizierung und Zugriffskontrolle

Passwort-Sicherheit

- bcrypt-Hashing mit Kostenfaktor 12
- Keine Klartextspeicherung von Passwörtern
- Brute-Force-Schutz durch Rate-Limiting

Session-Sicherheit

- httpOnly-Cookies (kein JavaScript-Zugriff)
- secure-Flag (nur über HTTPS)
- sameSite=Lax (CSRF-Basisschutz)
- strict_mode (keine fremden Session-IDs)
- 24-Stunden Inaktivitäts-Timeout
- Session-Regeneration nach Login

Rollenbasierte Zugriffskontrolle (RBAC)

- 5 Rollen: Systemmanager, Admin, Betreuer, Jugendlicher, Gast
- Multi-Tenancy: Jede Einrichtung sieht nur eigene Daten
- Filterung über institution_id in jeder Datenbankabfrage
- Jugendliche sehen ausschließlich eigene Daten (user_id-Filter)

SQL-Injection und XSS-Schutz

- Ausschließlich PDO Prepared Statements (keine String-Konkatenation)
- Output-Encoding: htmlspecialchars(ENT_QUOTES, UTF-8) bei jeder Ausgabe
- CSRF-Token bei allen POST-Requests im Admin-Backend

---

4. Einwilligungsmanagement (Consent)

AlltagQuest implementiert ein mehrstufiges Einwilligungssystem, das den besonderen Schutzanforderungen für Minderjährige gerecht wird.

Doppel-Einwilligung (ab 14 Jahren)

- 1. Sorgeberechtigte erteilen Einwilligung (beim Anlegen des Jugendlichen)
- 2. Jugendliche/r bestätigt eigene Einwilligung (beim ersten App-Login)
- Erst nach beiden Einwilligungen wird die App freigeschaltet

Consent-Typen in der Datenbank

- guardian_general: Allgemeine Einwilligung der Sorgeberechtigten
- youth_general: Eigene Einwilligung des Jugendlichen
- youth_mood_health: Separate Art. 9 DSGVO-Einwilligung (Stimmungsdaten)
- disclosure_203: Schweigepflichtentbindung nach § 203 StGB

Audit-Trail

- Datum und Uhrzeit der Einwilligung
- Name des Einwilligenden (consent_by)
- Methode: digital, Papier oder mündlich
- Erfasst durch (recorded_by, User-ID)
- Widerrufsdatum (revoked_at) bei Rücknahme

Rechtsgrundlage: Art. 7, 8, 9 DSGVO; Erwägungsgrund 38 (Schutz Minderjähriger)

5. Besondere Kategorien – Art. 9 DSGVO

Das Stimmungstracking erfasst Daten zum emotionalen Befinden. Diese gelten als Gesundheitsdaten im Sinne von Art. 9 DSGVO und erfordern eine separate Einwilligung.

Technische Umsetzung

- Eigener Consent-Typ: youth_mood_health
- Consent-Screen VOR dem ersten Mood-Check
- Prüfung bei jedem Zugriff: aq_consent_mood_ok()
- Ohne Einwilligung ist Stimmungserfassung gesperrt
- Widerruf jederzeit möglich (bestehende Daten bleiben, keine neuen Einträge)

> **Die Stimmungsdaten werden ausschließlich dem pädagogischen Team der eigenen Einrichtung angezeigt. Kein automatisiertes Scoring oder Profiling.**

---

6. Schweigepflichtentbindung (§ 203 StGB)

Pädagogische Fachkräfte unterliegen der beruflichen Schweigepflicht. AlltagQuest dokumentiert den Status der Schweigepflichtentbindung digital.

Dokumentierte Angaben

- Name des/der Entbindenden (Sorgeberechtigte/Jugendliche)
- Empfänger der Entbindung
- Methode der Erteilung (schriftlich, digital, mündlich)
- Datum der Erteilung
- Optionale Notizen

> **Die Einrichtung ist verantwortlich für das Original der Entbindungserklärung. AlltagQuest dient der digitalen Dokumentation des Status.**

---

7. KI-Pseudonymisierung

Für optionale KI-gestützte Berichte werden personenbezogene Daten VOR der Übermittlung an die KI-API pseudonymisiert.

Pseudonymisierungsmechanismus

- Echte Namen werden durch J1, J2, J3 etc. ersetzt
- Geburtsdaten werden entfernt
- Gruppennamen werden generisch (»Wohngruppe«)
- Betreuer-Namen werden entfernt
- Nach KI-Antwort: Rück-Mapping auf Vornamen

> **Keine Klardaten verlassen den Server in Richtung KI-API. Das KI-Modul ist derzeit als optionales Zusatzmodul vorgesehen und nicht standardmäßig aktiviert.**

Rechtsgrundlage: Art. 32(1)(a) DSGVO (Pseudonymisierung als Sicherheitsmaßnahme)

---

8. Datenexport und Langzeitarchivierung

Self-Service-Export (Art. 20 DSGVO)

- ZIP-Download aller Institutionsdaten (JSON-Format)
- PDF-Archiv pro Jugendlichem (Stammdaten, Stimmung, Gespräche, Ziele)
- Rate-Limiting: maximal 1 Export pro Tag
- CSRF-Token-Schutz beim Download
- Temporäre Datei wird nach Download gelöscht

Langzeitarchivierung

Heimakten müssen gemäß UBSKMG bis zu 70 Jahre aufbewahrt werden. AlltagQuest generiert PDF-Archive, die zur Konvertierung in PDF/A geeignet sind. Empfehlung: Nach Export in revisionssicheres Archivsystem überführen.

9. Recht auf Löschung (Art. 17 DSGVO)

Account-Löschung (Self-Service)

- 3-Stufen-Bestätigung: Text „LOESCHEN" + Checkbox + Passwort
- CSRF-Token und Passwort-Verifikation (bcrypt)
- Löschprotokoll mit Datum, Uhrzeit, User-ID
- E-Mail-Benachrichtigung an Admin und Kontaktadresse

Spezielle Behandlung

- Rechnungen: Anonymisiert, 10 Jahre aufbewahrt (§ 147 AO)
- Server-Logfiles: Automatische Löschung nach 7 Tagen
- Vertragsdaten: 30 Tage nach Vertragsende verfügbar, dann gelöscht

---

10. Technisch-Organisatorische Maßnahmen (TOM)

Gemäß Art. 32 DSGVO werden folgende Maßnahmen umgesetzt:

Maßnahme	Umsetzung
Zutrittskontrolle (physisch)	IONOS Rechenzentrum mit ISO 27001, biometrischer Zugangskontrolle und Videoüberwachung.
Zugangskontrolle (logisch)	bcrypt mit Kostenfaktor 12, Rate-Limiting, 24h Inaktivitäts-Timeout, HTTPS/HSTS, Session-Härtung.
Zugriffskontrolle	RBAC mit 5 Rollen, Multi-Tenancy mit institution_id, CSRF-Token, Prepared Statements, XSS-Prävention.
Weitergabekontrolle	TLS 1.2+, ausschließlich Deutschland-Hosting, STARTTLS für E-Mail, kein Tracking, CSP-Header.
Eingabekontrolle	Audit-Trail für Einwilligungen, Timestamps, Löschprotokolle, recorded_by-Felder.
Auftragskontrolle	AVV nach Art. 28 vor Nutzungsbeginn, Weisungsgebundenheit dokumentiert.
Verfügbarkeitskontrolle	Regelmäßige Backups, IONOS-Redundanz, PWA-Offline-Fähigkeit, Datenexport-Funktion.
Trennungsgebot	Multi-Tenancy mit logischer Trennung, separate Consent-Verwaltung pro Einrichtung.
Schutz Minderjähriger	Doppel-Einwilligung, Art. 9 separate Einwilligung, Pseudonym-Option, jugendgerechte Sprache, kein Tracking.
Regelmäßige Überprüfung	Code-Reviews, Update-Zyklen, Incident-Response-Verfahren.

11. Datenschutz-Folgenabschätzung (DSFA)

Gemäß Art. 35 DSGVO wurde eine DSFA durchgeführt, da besondere Kategorien personenbezogener Daten von Minderjährigen verarbeitet werden.

Risikobewertung

Risiko	Stufe	Gegenmaßnahmen
Unbefugter Zugriff	MITTEL	RBAC, Verschlüsselung, Timeout
Datenverlust	MITTEL	Backups, Redundanz, Export
Verletzung § 203 StGB	MITTEL	Entbindung, Rollenkonzept
Diskriminierung (Mood)	GERING	Separate Einwilligung, kein Scoring
XSS / SQL-Injection / CSRF	MITTEL	Prepared Statements, CSP, Token

> **Ergebnis: Risiken auf vertretbares Maß reduziert. Konsultation der Aufsichtsbehörde nach aktueller Einschätzung nicht erforderlich.**

---

12. Auftragsverarbeitung (AVV)

Der Auftragsverarbeitungsvertrag nach Art. 28 DSGVO ist in den AGB (§ 7) geregelt und wird VOR Nutzungsbeginn geschlossen.

Wesentliche Regelungen

- Gegenstand: Bereitstellung der SaaS-Plattform AlltagQuest
- Daten ausschließlich auf EU-Servern (IONOS, Deutschland)
- TOM-Dokumentation als Anlage
- Weisungsgebundenheit des Auftragsverarbeiters
- Unterauftragsverarbeiter: IONOS (Hosting), Brevo (E-Mail-Versand)
- Rückgabe/Löschung der Daten nach Vertragsende

---

13. Rate-Limiting und Missbrauchsschutz

Zum Schutz vor Missbrauch und Spam implementiert AlltagQuest ein differenziertes Rate-Limiting-System.

Aktion	Tageslimit	Cooldown
Stimmungseinträge	max. 3	30 s
Anträge/Beschwerden	max. 5	60 s
Ziele erstellen	max. 5	30 s

Aktion	Tageslimit	Cooldown
Routinen abhaken	max. 30	3 s
Passwort ändern	max. 3	30 s

Bei Überschreitung der Soft-Cap-Schwelle wird das pädagogische Team benachrichtigt (Eskalation). Die Partizipation der Jugendlichen bleibt durch großzügige Limits gewährleistet.

14. DSGVO-Konformität nach Artikel

Artikel	Umsetzung in AlltagQuest
Art. 5	Grundsätze: Rechtmäßigkeit, Transparenz, Datensparsamkeit, Richtigkeit, Speicherbegrenzung, Integrität
Art. 6	Rechtsgrundlagen: Vertragserfüllung (b), Rechtliche Verpflichtung (c), Einwilligung (a)
Art. 7	Consent-Helper mit Audit-Trail, Widerrufsfunktion
Art. 8	Doppel-Einwilligung: Sorgeberechtigte + ab 14 Jahre eigene
Art. 9	Separate Einwilligung für Stimmungsdaten (Gesundheitsdaten)
Art. 15–16	Datenexport-Funktion, Admin-Backend für Auskunft und Berichtigung
Art. 17	Account-Löschung mit 3-Stufen-Bestätigung und Protokoll
Art. 20	Datenübertragbarkeit: ZIP-Export mit JSON + PDF-Archiv
Art. 28	Auftragsverarbeitung: AVV vor Nutzungsbeginn, TOM-Dokumentation
Art. 32	Sicherheit: TLS, bcrypt, RBAC, Multi-Tenancy, CSP, Session-Härtung
Art. 35	Datenschutz-Folgenabschätzung durchgeführt und dokumentiert

15. Rechtlicher Rahmen (SGB VIII)

Artikel	Umsetzung in AlltagQuest
§ 36 SGB VIII	Hilfeplanung: Tagesgespräche, Quests, Ziele und Verlaufsdokumentation
§ 8 SGB VIII	Partizipation: Youth-App mit Einsichtsrecht, Anträge, eigenständige Einwilligung ab 14 J.
§ 8a SGB VIII	Schutzauftrag: Schweigepflichtentbindung dokumentieren, Datenweitergabe kontrollieren
§ 45 SGB VIII	Betriebserlaubnis: Dokumentationspflicht durch digitale Erfassung erfüllt
§ 203 StGB	Berufsgeheimnis: Separate Entbindungsdokumentation pro Jugendlichem
§ 147 AO	Aufbewahrung: Rechnungen 10 Jahre, anonymisiert nach Account-Löschung
UBSKMG	Heimakten: PDF-Archiv für 70-Jahre-Aufbewahrungspflicht

Dieses Dokument wurde auf Basis der technischen Implementierungen von AlltagQuest erstellt. Stand: März 2026. Frank M. Schaefer – Soziale und Digitale Dienstleistungen, Flensburg.