Technische und organisatorische Maßnahmen

StudyConnect – Maßnahmen nach Art. 28 Abs. 3 und Art. 32 DSGVO

Dokumentangabe	Wert
Stand	22.06.2026
Anbieter	Marcos Caprile Santos, handelnd unter MinutMate, Heltorfer Mark 131, 40489 Düsseldorf
Datenschutzkontakt	datenschutz@minutmate.com
Dokumentstatus	Finalisierte Prüffassung für die anwaltliche Prüfung

1. Schutzziele und Risikoorientierung

Die Maßnahmen dienen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der StudyConnect-Systeme. Sie werden risikoorientiert überprüft und bei wesentlichen technischen oder organisatorischen Änderungen angepasst.

2. Zutritts- und physische Sicherheit

- Produktive Systeme werden in Rechenzentren der eingesetzten Hostinganbieter betrieben.
- Physische Zutrittskontrollen liegen im Verantwortungsbereich der vertraglich gebundenen Rechenzentrums- und Hostinganbieter.
- Lokale Geräte mit Administrationszugriff sind durch Betriebssystemanmeldung, Gerätesperre und aktuelle Sicherheitssoftware zu schützen.

3. Zugangs- und Authentifizierungskontrolle

- Passwörter werden mit bcrypt und Cost-Faktor 12 gehasht; Klartextpasswörter werden nicht gespeichert.
- JWTs werden signiert. Sitzungen werden zusätzlich als SHA-256-Hash serverseitig gespeichert, auf Ablauf geprüft und können widerrufen werden.
- Authentifizierungs-Cookies sind httpOnly, SameSite=Lax und in Produktion Secure.
- Passwort-Reset-Token werden zufällig erzeugt; gespeichert wird nur ein SHA-256-Hash.
- Rate-Limits schützen insbesondere Login, Passwort-Reset, Administration, Chat, Uploads und öffentliche Schreibvorgänge.

4. Zugriffskontrolle und Mandantentrennung

- Rollen und Berechtigungen unterscheiden insbesondere Schüler-, Schuladmin- und Plattformadmin-Funktionen.
- Schulbezogene Datensätze werden über school_id zugeordnet; zentrale Abfragen prüfen die Schulzugehörigkeit.
- Chat-Zugriffe erfordern zusätzlich eine gültige Mitgliedschaft.
- Berechtigungen werden nach dem Erforderlichkeitsprinzip vergeben und bei Rollenwechsel oder Ausscheiden entzogen.

5. Verschlüsselung und Übertragung

- Transportverschlüsselung über HTTPS/TLS für produktive Web- und API-Zugriffe.
- Chat-Inhalte werden serverseitig mit AES-256-GCM verschlüsselt. StudyConnect kann sie für die vereinbarte Bereitstellung entschlüsseln; es liegt keine Ende-zu-Ende-Verschlüsselung vor.

- Der Datenbank-Dateifallback unterstützt AES-256-GCM.
- Firebase-Dateien werden über zeitlich begrenzte V4-Signed-URLs bereitgestellt; Standardgültigkeit 15 Minuten.
- Firebase Storage Rules verweigern direkte öffentliche Lese- und Schreibzugriffe.

6. Protokollierung und Nachvollziehbarkeit

- Audit-Logs erfassen sicherheitsrelevante Ereignisse mit Akteur, Ziel, Schule, IP-Adresse, User-Agent, Ergebnis und Schweregrad.
- Sensible Metadaten werden vor Protokollierung redigiert.
- Administrative und sicherheitsrelevante Vorgänge werden nur für berechtigte Rollen zugänglich gemacht.

7. Verfügbarkeitskontrolle und Wiederherstellung

Tägliche Datenbanksicherungen werden mit AES-256-GCM verschlüsselt und per FTPS zu ALL-INKL übertragen. Für das Remote-Verzeichnis fehlt derzeit eine automatische Löschrotation; diese ist vor Produktivfreigabe umzusetzen.

Restore-Tests sind eingerichtet. Die Restore-Test-Datenbank befindet sich in der Railway-Region EU West (Amsterdam, Niederlande). Nach jedem Wiederherstellungstest ist die Testdatenbank automatisch zu leeren.

Festgelegtes RTO und RPO betragen jeweils 24 Stunden. Ein dokumentierter Wiederherstellungstest ist vierteljährlich durchzuführen.

8. Trennungsgebot

- Trennung der Schulmandanten über school_id und rollenbezogene Autorisierung.
- Trennung von Web-Frontend, API/Backend, Datenbank und Dateiablage.
- Umgebungsabhängige Konfigurationen und Geheimnisse werden außerhalb des Quellcodes verwaltet.

9. Auftragskontrolle und Dienstleister

Aktive Unterauftragsverarbeiter werden dokumentiert und über Datenschutzverträge gebunden. Änderungen werden Vertragsschulen entsprechend dem AVV mitgeteilt.

10. Datenschutzfreundliche Voreinstellungen

- Keine Tracking- oder Marketing-Cookies im derzeit geprüften Web-Code.
- Nicht öffentliche Datei-Buckets und kurzlebige Abruflinks.
- Erhebung und Sichtbarkeit von Daten werden rollen- und funktionsbezogen begrenzt.

11. Incident Response

1. Vorfall erkennen, Erstmaßnahmen treffen und Beweismittel sichern.
2. Betroffene Systeme, Datenkategorien, Schulen, Personen und Zeiträume bestimmen.
3. Zugänge sperren, Schlüssel oder Tokens rotieren und Schwachstelle eindämmen.
4. Verantwortliche Schule unverzüglich mit den verfügbaren Informationen informieren.
5. Ursache beheben, Systeme kontrolliert wiederherstellen und Wirksamkeit prüfen.
6. Vorfall, Entscheidungen, Kommunikation und Verbesserungsmaßnahmen dokumentieren.

12. Überprüfung

Diese TOMs werden mindestens halbjährlich und zusätzlich bei wesentlichen System-, Anbieter- oder Risikoveränderungen überprüft. Berechtigungs- und Wiederherstellungsprüfungen erfolgen vierteljährlich. Abweichungen zwischen dokumentiertem und tatsächlichem Betrieb sind zu korrigieren; nicht nachgewiesene Prozesse werden nicht als bestehende Zusicherung dargestellt.