eduBITES GmbH

Technische und organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO

Version	2.0
Stand	11.05.2026
Klassifizierung	Zur Weitergabe an Geschäftspartner und Kunden
Verantwortlich	eduBITES GmbH, Geschäftsführung

Hinweis

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, die die eduBITES GmbH zur Sicherstellung eines dem Risiko angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten gemäß Art. 32 DSGVO implementiert hat. Die Maßnahmen gelten für sämtliche Verarbeitungen personenbezogener Daten durch eduBITES GmbH, insbesondere im Rahmen der eduBITES Learner Experience Platform (LXP).

eduBITES GmbH betreibt eine vollständig cloudbasierte Architektur in AWS Frankfurt (Region eu-central-1). Es bestehen keine eigenen Server am Bürostandort. Die physische Infrastruktursicherheit wird durch die ISO 27001 / SOC 2 Type II zertifizierten AWS-Rechenzentren gewährleistet; am Bürostandort Berlin werden keine personenbezogenen Kundendaten lokal gespeichert oder verarbeitet.

Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt; die Angaben beziehen sich auf Angehörige aller Geschlechter.

Präambel

eduBITES GmbH hat geeignete technische und organisatorische Maßnahmen zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme implementiert. Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen besteht und wird gemäß ISMS-Vorgaben durchgeführt.

Der allgemeine Teil (Grundsätzliche Maßnahmen) beschreibt Maßnahmen, die unabhängig von einzelnen Dienstleistungen, Services oder Kunden gelten. Die nachfolgenden Abschnitte beschreiben Maßnahmen für die acht klassischen Kontrollkategorien sowie die regelmäßige Überprüfung und den Zertifizierungs-Status.

1. Grundsätzliche Maßnahmen

- Es besteht ein dokumentiertes Informationssicherheits-Managementsystem (ISMS), dessen Einhaltung systematisch überwacht und mindestens jährlich im Rahmen interner Audits evaluiert wird.

- Es besteht ein Konzept zur unverzüglichen und gesetzeskonformen Behandlung von Datenschutzverletzungen (Prüfung, Dokumentation, Meldung an die Aufsichtsbehörde gemäß Art. 33 DSGVO innerhalb von 72 Stunden, Benachrichtigung der betroffenen Personen gemäß Art. 34 DSGVO bei hohem Risiko).
- Es besteht ein Konzept zur Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch) innerhalb der gesetzlichen Fristen.
- Berechtigungen, Schlüssel und Zugangsdaten von Mitarbeitenden werden bei Ausscheiden bzw. Funktionswechsel gemäß dokumentiertem Berechtigungskonzept unverzüglich entzogen.
- Auftragsverarbeiter werden sorgfältig ausgewählt; mit allen Unterauftragnehmern bestehen DSGVO-konforme Vereinbarungen zur Auftragsverarbeitung (AVV). Bei Drittlandstransfers werden die Anforderungen des Kapitels V DSGVO eingehalten (insbesondere EU-Standardvertragsklauseln und ggf. Transfer Impact Assessment).
- Mitarbeitende werden im Rahmen des Onboardings und mindestens einmal jährlich zum Datenschutz und zur Informationssicherheit geschult und auf die Vertraulichkeit (Verpflichtung auf das Datengeheimnis) verpflichtet.
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) ist in den Entwicklungsprozess der eduBITES LXP integriert (Privacy by Design, Privacy by Default).
- Software und Sicherheitskomponenten werden über automatisierte Update-Prozesse aktuell gehalten.

2. Zutrittskontrolle

Hinweis: eduBITES GmbH betreibt eine cloudbasierte Architektur. Personenbezogene Kundendaten werden ausschließlich in AWS Frankfurt (eu-central-1) verarbeitet. Die nachfolgenden physischen Maßnahmen beziehen sich auf den Bürostandort Berlin sowie auf die durch AWS bereitgestellten Rechenzentren.

AWS-Rechenzentren (Auftragsverarbeiter)

- Mehrschichtige physische Zugangskontrollen
- 24/7 Sicherheitspersonal und Videoüberwachung
- Biometrische Zugangskontrollen
- Perimeterschutz und Besuchermanagement
- Nachweis: AWS ISO 27001, SOC 2 Type II Berichte

Bürostandort Berlin (Leipziger Straße 126)

- Schlüsselbasierter Zutritt zu den Büroräumen
- Schlüsselausgabe nur an autorisierte Mitarbeitende, Erfassung im Asset-Register
- Besucherbegleitung durch Mitarbeitende
- Keine lokale Speicherung oder Verarbeitung von Kundendaten am Bürostandort
- Mobile Endgeräte verlassen das Büro nur mit Festplattenverschlüsselung (Full Disk Encryption)

3. Zugangskontrolle / Zugriffskontrolle

Authentifizierung

- Benutzer-Authentifizierung über Amazon Cognito User Pools mit starken Passwortrichtlinien
- Account Lockout nach mehreren Fehlversuchen
- Session-Timeout bei Inaktivität
- Single Sign-On (SSO) über Google Workspace für interne Werkzeuge
- Multi-Faktor-Authentifizierung (MFA) verpflichtend für administrative Zugänge

Autorisierung und Rechtevergabe

- Rollenbasierte Zugriffskontrolle (RBAC) in allen Systemen
- Prinzip der minimalen Rechtevergabe (Least Privilege) bei sämtlichen Benutzer- und Service-Accounts
- Dokumentiertes Berechtigungskonzept
- Berechtigungen werden bei Rollenwechsel innerhalb von 5 Geschäftstagen angepasst
- Berechtigungen werden bei Ausscheiden unverzüglich entzogen
- Minimale Anzahl administrativer Accounts; getrennte Verwaltung administrativer Rechte

Endgerätesicherheit

- Festplattenverschlüsselung auf allen Mitarbeiter-Geräten (FileVault / BitLocker)
- Automatische Bildschirmsperre bei Inaktivität
- Stets aktuelle Software, Virenschutz und Sicherheitsupdates
- Richtlinie zu USB-Geräten und Wechselmedien

Verschlüsselung

- Daten im Ruhezustand (Data at Rest): AES-256 (AWS S3, Datenbank, Backups)
- Daten in der Übertragung (Data in Transit): TLS 1.2 oder höher
- Schlüsselverwaltung über AWS KMS mit automatischer Schlüsselrotation
- Datenbankverbindungen über SSL/TLS verschlüsselt

Logging

- Protokollierung administrativer Zugriffe (AWS CloudTrail)
- Protokollierung von Anwendungszugriffen (Eingabe, Änderung, Löschung von Daten)
- Mindestens 12 Monate Aufbewahrung der Protokolle
- Manipulationsgeschützte Speicherung (Append-only, beschränkte Zugriffsrechte)

4. Weitergabekontrolle

- Sämtliche Datenübertragungen zwischen Systemen erfolgen verschlüsselt über TLS 1.2 oder höher.
- Personenbezogene Daten werden ausschließlich an autorisierte Empfänger weitergegeben; eine Übermittlung erfolgt grundsätzlich nur auf Basis einer Rechtsgrundlage gemäß Art. 6 DSGVO und – sofern erforderlich – auf Basis einer AVV (Art. 28 DSGVO) bzw. einer Vereinbarung über gemeinsame Verantwortung (Art. 26 DSGVO).
- VPN-Pflicht für administrative Zugriffe auf die Produktivinfrastruktur.

- API-zu-API-Kommunikation wird über API-Schlüssel und Token authentifiziert.
- Personenbezogene Daten werden nicht über unverschlüsselte Kanäle (z. B. unverschlüsseltes E-Mail oder FTP) übertragen.
- Bei Drittlandsübermittlungen werden EU-Standardvertragsklauseln (SCC, Module 2 bzw. 3) abgeschlossen und ggf. ein Transfer Impact Assessment durchgeführt; sämtliche Unterauftragnehmer sind auf der Trust-Center-Seite gelistet.

5. Eingabekontrolle

- Protokollierung von Dateneingaben, Änderungen und Löschungen mit Zeitstempel.
- Nachvollziehbarkeit über individuelle Benutzerkennungen (keine Sammel- oder Gruppen-Logins für regelmäßige Tätigkeiten).
- Rechtevergabe für Eingabe, Änderung und Löschung auf Basis des Berechtigungskonzepts.
- Klare Zuständigkeiten für Löschungen.
- Administratoren- und Stellvertreterkonzept.
- Input-Validierung an allen API-Endpunkten und Benutzeroberflächen, parametrisierte Datenbankabfragen, Content Security Policy (CSP) Header, Validierung von Datei-Uploads.

6. Auftragskontrolle

- Auswahl von Auftragsverarbeitern unter Berücksichtigung der Anforderungen an Datenschutz und Informationssicherheit (Art. 28 Abs. 1 DSGVO).
- Abschluss DSGVO-konformer Auftragsverarbeitungsverträge mit allen Unterauftragnehmern; bei Drittlandsbezug ergänzende EU-Standardvertragsklauseln (SCC).
- Verpflichtung der Mitarbeitenden des Auftragsverarbeiters auf das Datengeheimnis.
- Regelung zum Einsatz weiterer Unterauftragnehmer (Genehmigungspflicht oder vorherige Information).
- Vereinbarung von Kontroll- und Auditrechten zugunsten der Verantwortlichen.
- Schriftliche Weisungsbefugnis des Auftraggebers im Rahmen der AVV.
- Sicherstellung der Löschung oder Rückgabe personenbezogener Daten nach Beendigung des Auftrags.
- Jährliche Überprüfung der eingesetzten Auftragsverarbeiter.

Aktuelle Unterauftragnehmer (Auszug; vollständige Liste mit DPAs unter edubites.com/trust-center):

Dienstleister	Zweck	Verarbeitungsort
Amazon Web Services (AWS)	Kerninfrastruktur, Speicherung, Authentifizierung (Cognito)	Frankfurt (eu-central-1)
Supabase	Produktivdatenbank	EU
Google Workspace	Interne Zusammenarbeit, CRM	EU
Azure OpenAI	Textgenerierung (kein Training mit Kundendaten)	EU / US (SCC)
Azure Speech	Sprachausgabe und Transkription	EU / US (SCC)
Sonix	Transkription (Löschung nach Verarbeitung)	US (SCC)

Dienstleister	Zweck	Verarbeitungsort
Replicate	Generierung visueller Inhalte	US (SCC)
Elai	Videoverarbeitung	AWS Frankfurt
Monday.com	Projektadministration	EU / US

7. Verfügbarkeitskontrolle / Integrität

Backup und Recovery

- Automatisierte Datenbank-Backups alle 30 Minuten
- Backups werden mit AES-256 verschlüsselt und in einer separaten AWS-Region gespeichert (geografische Redundanz)
- Monatliche Tests der Backup-Wiederherstellung; Ergebnisse dokumentiert
- Aufbewahrungsfristen gemäß Backup-Konzept

Notfallmanagement (Business Continuity / Disaster Recovery)

- Dokumentierter BC/DR-Plan mit Failover-Verfahren für kritische Systeme
- Recovery Time Objective (RTO): 4 Stunden (Ziel)
- Recovery Point Objective (RPO): 30 Minuten (Ziel)
- Multi-Availability-Zone-Deployment in AWS Frankfurt
- Jährliche Simulationsübung zur DR

Integrität der Verarbeitung

- Versionierte Infrastruktur (Infrastructure as Code)
- CI/CD-Pipeline mit automatisierten Tests und Code-Review-Pflicht vor Produktiv-Deployment
- Dokumentierte und getestete Rollback-Verfahren

Vorfall- und Incident-Management

Stufe	Beschreibung	Reaktionszeit
P1 Kritisch	Bestätigter Datenvorfall, vollständiger Ausfall, aktive Ausnutzung	15 Minuten
P2 Hoch	Vermuteter Datenvorfall, Teil-Ausfall, unbefugter Zugriff	1 Stunde
P3 Mittel	Policy-Verletzung, abgewehrter Angriff, Phishing	4 Stunden
P4 Niedrig	Geringe Abweichung, informatorischer Vorfall	1 Geschäftstag

- Zentrale Meldestelle: security@edubites.com
- Incident-Commander für P1/P2-Vorfälle
- Post-Incident-Review innerhalb von 5 Geschäftstagen
- Quartalsweise Auswertung des Incident-Logs

8. Gewährleistung des Zweckbindungs- und Trennungsgebotes

- Getrennte Entwicklungs-, Test- und Produktivumgebungen mit jeweils eigenen Zugangsdaten und Berechtigungen.
- Produktivdaten werden nicht in Entwicklungs- oder Testumgebungen verwendet.
- Steuerung der Datenzugriffe über das dokumentierte Berechtigungskonzept.
- Mandantentrennung: Daten werden auf Datenbankebene über eine Organisations-Kennung (organization_id) je Kunde getrennt; die Trennung wird durch Row Level Security (RLS) auf Datenbankebene durchgesetzt. Ein Zugriff auf Daten anderer Mandanten ist auf Anwendungs- und Datenbankebene technisch ausgeschlossen.
- API-Antworten sind auf den authentifizierten Mandanten-Kontext beschränkt (Scoping).
- Datenbankseitige Festlegung von Berechtigungen auf Tabellen- und Zeilenebene.

9. Regelmäßige Überprüfung, Bewertung und Evaluierung

- Mindestens jährliche Überprüfung der TOM im Rahmen der internen ISMS-Audits sowie des Datenschutz-Audit-Programms.
- Anlassbezogene Überprüfung bei wesentlichen Änderungen an Verarbeitungstätigkeiten, Infrastruktur oder Unterauftragnehmern.
- Erkenntnisse aus Sicherheitsvorfällen und Datenschutzverletzungen fließen in die Risiko- und Maßnahmenbewertung ein.
- Korrekturmaßnahmen aus Audits und Vorfällen werden bis zur Umsetzung nachverfolgt.

10. Zertifizierungen und Audits

eduBITES GmbH befindet sich derzeit in Vorbereitung der ISO 27001 Zertifizierung in Abstimmung mit dem Konzern-CISO der Amadeus Fire Group. Eine Zertifizierung liegt zum Stand dieses Dokumentes **nicht** vor.

Verfügbare Nachweise:

- AWS ISO 27001 / SOC 2 Type II Berichte (für die genutzte Infrastruktur in Frankfurt)
- Berichte und Testate der Unterauftragnehmer (auf Anfrage)

11. Ansprechpartner

eduBITES GmbH	Leipziger Straße 126, 10117 Berlin
Allgemeiner Kontakt	hello@edubites.com
Security-Vorfälle	security@edubites.com
Externer DSB	simply Legal GmbH (Sebastian Schenk), Würzburg

Hinweis: Im Rahmen der Übernahme der DSB-Funktion durch die Amadeus Fire Group ab dem 03.07.2026 wird der Konzern-Datenschutzbeauftragte der AF Group die Funktion übernehmen. Aktualisierte Kontaktdaten werden zu diesem Zeitpunkt veröffentlicht.

Unterschriften

Berlin, den _____

_____

Marc Drüner

Geschäftsführer, eduBITES GmbH

Eine Gegenzeichnung durch den Auftraggeber ist im Rahmen des jeweiligen AVV vorgesehen.

Dokumenten-Historie

Version	Datum	Beschreibung
1.0	08.07.2025	Initialfassung (BDSG §9-Struktur, allgemeines Template)
2.0	11.05.2026	Vollständige Überarbeitung auf Basis ISMS POL-30: konkrete Verschlüsselungs-, Backup- und Incident-Response-Parameter; Liste der Unterauftragnehmer; Bereinigung nicht zutreffender physischer Kontrollen; aktualisierter Zertifizierungs-Status.