



Ausbildung24

☎ +49 1516 5070397
✉ info@ausbildung24.com
🏠 Beethovenallee 24
33175 Bad Lippspringe

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Anlage zur AVV

Stand: 22.06.2026



Die folgenden Maßnahmen beschreiben den derzeit vorgesehenen Basisschutz. Ausbildung24 macht bewusst keine Zusage zu Funktionen, die nicht sicher bestätigt sind. Insbesondere wird keine allgemeine MFA-Pflicht für sämtliche Endnutzer vertraglich zugesichert. Zusätzliche Anforderungen können bei Enterprise-Kunden gesondert vereinbart werden.

1. Maßnahmenübersicht

Schutzziel / Bereich	Umsetzung
Organisation und Verantwortlichkeit	Zugriffe werden auf autorisierte Personen beschränkt. Rollen und Zuständigkeiten werden dokumentiert; Beschäftigte und Auftragnehmer werden auf Vertraulichkeit verpflichtet.
Zutrittskontrolle	Die produktive Infrastruktur wird bei Cloud-Anbietern betrieben. Physische Zutrittskontrollen liegen in deren zertifizierten Rechenzentren; Ausbildung24 betreibt keine eigenen Serverräume für Produktivdaten.
Zugangskontrolle	Persönliche Benutzerkonten, passwortgeschützte Anmeldung, Zurücksetzung bei Verdacht auf Kompromittierung und Sperrung ausgeschiedener oder nicht mehr berechtigter Nutzer.
Berechtigungskontrolle	Rollen- und mandantenbezogene Berechtigungen; Zugriff nur nach dem Need-to-know-Prinzip. Administrative Zugriffe sind auf einen kleinen Personenkreis beschränkt.
Mandantentrennung	Kundendaten werden logisch nach Unternehmen und Berechtigungen getrennt. Unternehmensnutzer erhalten nur Zugriff auf den jeweils zugeordneten Bereich.
Übertragungsschutz	Transportverschlüsselung über aktuelle HTTPS/TLS-Verbindungen. Datenübertragungen erfolgen nur über vorgesehene Schnittstellen und autorisierte Empfänger.
Speicherschutz	Cloudseitige Verschlüsselungs- und Schutzmechanismen für gespeicherte Daten werden genutzt. Besonders sensible Daten sollen nicht unnötig erhoben werden.
Protokollierung	Sicherheits- und Administrationsereignisse werden im technisch verfügbaren Umfang protokolliert und mindestens 90 Tage aufbewahrt. Protokolle werden nur berechtigten Personen zugänglich gemacht und vor unbefugter Veränderung geschützt.
Verfügbarkeit und Wiederherstellung	Nutzung skalierbarer Cloud-Dienste mit täglichen Datensicherungen entsprechend der eingesetzten Cloud-Anbieter-Defaults; Wiederherstellbarkeit wird regelmäßig überprüft. Wiederherstellungs- und Exportmöglichkeiten stehen entsprechend der eingesetzten Plattformkomponenten zur Verfügung.
Änderungs- und Entwicklungsprozess	Änderungen werden kontrolliert bereitgestellt. Sicherheitsrelevante Fehler werden priorisiert; Zugriffe auf Produktionsdaten zu Testzwecken werden vermieden oder minimiert.
Schwachstellen und Updates	Abhängigkeiten und Plattformkomponenten werden regelmäßig aktualisiert. Kritische Sicherheitslücken werden nach Risiko priorisiert.
Datenschutzvorfälle	Interner Meldeweg, Bewertung, Eindämmung, Dokumentation und unverzügliche Information betroffener Kunden gemäß AVV.
Löschung und Rückgabe	Account- und Bewerbungsdaten werden auf Anforderung oder nach Vertragsende nach den vereinbarten Fristen gelöscht oder exportiert. Backups werden im regulären Überschreibzyklus entfernt.
Dienstleisterkontrolle	Auftragsverarbeiter werden anhand ihrer Datenschutz- und Sicherheitsunterlagen ausgewählt und vertraglich verpflichtet. Änderungen werden nach AVV kommuniziert.



Schutzziel / Bereich	Umsetzung
Datensparsamkeit	Es werden nur für den jeweiligen Zweck erforderliche Daten erhoben. Besondere Kategorien werden nicht gezielt im Berufsprofil-Test abgefragt.

2. Technische Plattformkomponenten

- Google Firebase / Google Cloud für Authentifizierung, Datenbank, Hosting/Storage und Push-Funktionen. Firestore-Datenbank und Hosting: Region Frankfurt (europe-west1). Dienste ohne konfigurierbare EU-Region (z. B. Firebase Cloud Messaging) werden auf Grundlage der Google Cloud DPA / EU-Standardvertragsklauseln betrieben; weitere Angaben in der Unterauftragnehmerliste.
- Microsoft Azure OpenAI Service für KI-gestützte Funktionen in einer EU-Region. Eingaben und Ausgaben werden nicht zum Training der zugrunde liegenden Basismodelle verwendet, soweit dies nach den geltenden Microsoft-Produktbedingungen erfolgt.
- Resend für transaktionalen E-Mail-Versand (USA-basiert; Transfermechanismus: EU-Standardvertragsklauseln gemäß Resend Data Processing Agreement; weitere Angaben in der Unterauftragnehmerliste).
- Microsoft 365 für interne Kommunikation, Dokumentation und Support.
- Nach aktuellem Projektstand werden keine zusätzlichen Analyse- oder Werbettrackingdienste eingesetzt.

3. Nicht als Standard zugesicherte Maßnahmen

- Multi-Faktor-Authentifizierung für sämtliche Unternehmens- und Schülerkonten.
- Eine bestimmte Zertifizierung von Ausbildung24 selbst.
- Eine garantierte Wiederherstellungszeit oder ein garantierter maximaler Datenverlust ohne gesonderte SLA.
- Kundeneigene Verschlüsselungsschlüssel oder dedizierte Infrastruktur.

4. Aktualisierung

Ausbildung24 überprüft die Maßnahmen bei wesentlichen Produkt- oder Infrastrukturänderungen. Gleichwertige oder stärkere Maßnahmen können ohne Vertragsänderung eingesetzt werden, sofern das Gesamtschutzniveau nicht sinkt.