kontakt@school-up.de · +49 157 89160932
school-up.de

Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: 30. August 2026

Diese Darstellung beschreibt die tatsächlich umgesetzten Maßnahmen des Auftragsverarbeiters SchoolUP, gegliedert nach den Gewährleistungszielen des Standard-Datenschutzmodells (SDM). Noch nicht umgesetzte, aber sinnvolle Maßnahmen sind ausdrücklich als **„geplant“** gekennzeichnet. Physische Maßnahmen im Rechenzentrum obliegen dem Unterauftragsverarbeiter STRATO AG (Standort Deutschland) und sind bei diesem nachzuweisen; es werden hier keine Zertifizierungen behauptet, die nicht durch Nachweise belegt sind.

1. Vertraulichkeit

1.1 Zutrittskontrolle (physisch)

- Der physische Serverbetrieb erfolgt in einem Rechenzentrum der STRATO AG in Deutschland. Zutrittsschutzmaßnahmen (Gebäudesicherung, Zugangskontrolle) liegen im Verantwortungsbereich des Unterauftragsverarbeiters und sind vertraglich abgesichert; entsprechende Nachweise sind beim Unterauftragsverarbeiter einzuholen.
- SchoolUP betreibt keine eigenen Server mit Klardaten außerhalb dieser Infrastruktur.

1.2 Zugangskontrolle (Systemzugang)

- Verschlüsselte Transportwege durchgängig über TLS/HTTPS; HTTP wird automatisch auf HTTPS umgeleitet.
- Reverse Proxy (Caddy) mit automatischem HTTPS sowie gesetzten Sicherheits-Headern: `Strict-Transport-Security` (zwei Jahre, inkl. Subdomains), `X-Content-Type-Options: nosniff`, `X-Frame-Options: DENY`, `Referrer-Policy: strict-origin-when-cross-origin` sowie eine Content-Security-Policy mit `frame-ancestors 'none'`, `object-src 'none'` und `base-uri 'self'`. Die Server-Kennung wird entfernt.
- TLS-Zertifikate werden nur für die eigene Domain und für tatsächlich registrierte, aktive Schul-Subdomains ausgestellt; für unbekannte Hostnamen wird die Ausstellung verweigert.
- Authentifizierung der nutzende Personen über das schulische Moodle; das Moodle-Passwort wird zu keinem Zeitpunkt gespeichert.
- Schulleitungskonten mit scrypt-gehashten Passwörtern (zufälliger Salt je Konto, Vergleich in konstanter Zeit).
- Signierte, zustandslose Sitzungstoken (HMAC-SHA256, Vergleich in konstanter Zeit) mit Ablaufzeit und Zwecktrennung. Vor *jedem* Zugriff auf den Lernbereich, also vor jeder Frage an den Tutor, jeder Übung und jedem Abruf von Kursinhalten, wird zusätzlich geprüft, ob die Nutzungseinwilligung weiterhin gilt und die Schule aktiv ist; ein Widerruf wirkt damit sofort und nicht erst mit Ablauf des Tokens. Bewusst nicht hinter dieser Prüfung liegen genau die drei Wege, die einer Person auch nach dem Widerruf offenstehen müssen: die Selbstauskunft, der Widerruf selbst und die Abfrage des eigenen Einwilligungsstands.
- Begrenzung der Anmeldeversuche auf allen Anmelde-Endpunkten, mit zwei Grenzen nebeneinander: höchstens **fünf Fehlversuche je Konto** (Schule und Benutzername) und höchstens **60 Fehlversuche je Absender** (IP-Adresse und Schule), jeweils innerhalb von zehn Minuten. Gezählt werden nur Fehlversuche; weitere Versuche werden mit einer Wartezeit abgewiesen. Der Betreiberzugang hat eine eigene, engere Grenze.
- Restriktives CORS: Anfragen aus dem Browser werden nur für die eigene Domain `school-up.de` und deren Schul-Subdomains `*.school-up.de` zugelassen (in Produktion ausschließlich über HTTPS); fremde Herkünfte erhalten keine Freigabe.

- Die Zuordnung einer Anfrage zur jeweiligen Schule erfolgt in Produktion ausschließlich anhand des vom Reverse Proxy übergebenen Hostnamens; eine Übersteuerung per Parameter ist dort ausgeschlossen.
- Validierung der sicherheitsrelevanten Pflicht-Secrets beim Start (Mindestlänge des Signaturschlüssels, korrekte Schlüssellänge für die Verschlüsselung); ohne gültige Secrets nimmt der Dienst den Betrieb nicht auf.
- Automatisierte Tests sichern die vorstehenden Zusagen zu Passwort-Hashing, Verschlüsselung, Sitzungstoken, Mandantenzuordnung, Herkunftsprüfung und Anmeldebegrenzung bei jeder Änderung ab.
- **Geplant:** Zwei-Faktor-Authentifizierung für Schulleitungskonten.

1.3 Zugriffskontrolle (Berechtigungen)

- Zugriff auf Klardaten (Name, Moodle-Benutzername, Geburtsdatum, Name der erziehungsberechtigten Person, Unterschrift) nur für die schulbezogen berechtigte Schulleitung sowie, auf das Erforderliche beschränkt, für die Betreiber. Ein Wohnsitz wird nicht erhoben.
- Die Zweckbindung der Sitzungstoken begrenzt die aufrufbaren Funktionen: ein Token des Lernbereichs eröffnet keinen Zugang zum Schulleitungs- oder Betreiberbereich.
- Der Betreiberbereich (Anlegen, Ändern und Deaktivieren von Schulen) ist durch einen gesonderten Schlüssel geschützt und ohne diesen nicht nutzbar.
- Kein Tracking, keine Werbeprofile, keine Weitergabe zu Werbezwecken. Die Lern-Notizen des KI-Tutors (je Kurs, pseudonym, max. 40 Stichpunkte) dienen ausschließlich der Anpassung der Erklärungen an die lernende Person, sind für sie einsehbar und jederzeit löschbar.
- **Geplant:** feingranulares, protokolliertes Rollen-/Rechtekonzept mit dokumentierter Vergabe/Entzug von Berechtigungen der Betreiber.

1.4 Trennungskontrolle

- Mandantentrennung pro Schule: Jede Schule erhält eine eigene Subdomain; die Zuordnung erfolgt an einer einzigen, zentralen Stelle im System und ausschließlich anhand des vom Reverse Proxy übergebenen Hostnamens. Jede Datenbankabfrage zu personenbezogenen Daten ist zusätzlich an die Kennung der jeweiligen Schule gebunden. Diese Bindung steht heute in jeder einzelnen Abfrage und wird durch eine automatische Prüfung über den gesamten Quelltext abgesichert, die vor jeder Auslieferung läuft; sie wird nicht von der Datenbank selbst erzwungen. Eine Absicherung auf Datenbankebene (Row Level Security) ist vorgesehen.
- Zweckgetrennte Verarbeitung (Anmeldung, Einwilligung, Lernbereich, Schulleitung, Betrieb) mit jeweils eigenen, zweckgebundenen Sitzungstoken.

2. Integrität

2.1 Weitergabekontrolle

- Übertragung ausschließlich verschlüsselt (TLS/HTTPS), auch zu den Unterauftragsverarbeitern.
- **Regionale Bindung der Modellausführung.** Alle Aufrufe an das Sprachmodell und an die Texterkennung gehen an den EU-Regionalendpunkt `api.eu.mistral.ai`. Die Ausführung ist damit technisch auf die Europäische Union festgelegt. Der Unterauftragsverarbeiter hält daneben einen US-Endpunkt vor; er wird nicht aufgerufen. Der Endpunkt ist an einer Stelle im Quelltext gesetzt, wird von keinem Aufrufer überschrieben und von einer automatischen Prüfung gehalten, die umfällt, sobald irgendwo der allgemeine Endpunkt als Voreinstellung auftaucht.

- Verarbeitung innerhalb der EU (STRATO: Deutschland, für Server, Datenbank und Objektspeicher; Mistral AI: Frankreich, Aufruf über den EU-Regionalendpunkt). Der Auftragsverarbeiter selbst übermittelt keine Daten in ein Drittland. Mistral AI erklärt, die Daten lägen voreingestellt in der EU und könnten je nach genutzter Funktion vorübergehend außerhalb der EU verarbeitet werden; dafür sagt Mistral AI geeignete Garantien nach Art. 46 DSGVO und eine Sicherheitsprüfung der beteiligten Unterauftragsverarbeiter zu (Wo speichert Mistral die Daten?).
- **Dateien werden vor der Übertragung verschlüsselt.** Eine abgegebene Übungsklausur und die nächtliche Sicherung beider Datenbanken gehen ausschließlich als AES-256-GCM-Chiffrat in den Objektspeicher; der Schlüssel bleibt auf dem Server des Auftragsverarbeiters. Es geht dabei um die Handschrift Minderjähriger, und der Unterauftragsverarbeiter kann sie nicht zur Kenntnis nehmen.
- **Verfügbarkeit: nächtliche Sicherung.** Beide Datenbanken werden täglich verschlüsselt in den Objektspeicher gesichert (Aufbewahrung 30 Tage, ältere werden automatisch entfernt). Der Weg zurück ist im Quelltext hinterlegt und geprüft; eine Sicherung, die niemand zurückgespielt hat, ist keine.
- Vertragliche Bindung der Unterauftragsverarbeiter (AVV); Ausschluss der Nutzung zu Trainings-/Eigenzwecken ist sicherzustellen.

2.1a Ausgehende Abrufe (verlinkte Webseiten)

- Abgerufen werden ausschließlich Adressen, die eine Lehrkraft im Kurs verlinkt hat. Weiterführenden Links wird nicht gefolgt.
- Vor jedem Abruf wird die Zieladresse geprüft: nur `http` / `https`; private, lokale und Metadaten-Adressbereiche sind gesperrt. Geprüft wird auch die **aufgelöste IP-Adresse**, damit ein öffentlicher Name nicht auf ein internes System zeigen kann (Schutz vor Server Side Request Forgery). Weiterleitungen werden bei jedem Schritt erneut geprüft, höchstens dreimal.
- Begrenzungen je Abruf: 12 Sekunden Zeitgrenze, 2 MB Übertragungsgrenze, nur HTML-Inhalte, höchstens 20.000 Zeichen gespeicherter Text.
- Der maschinenlesbare Nutzungsvorbehalt (`robots.txt`, `X-Robots-Tag`, `noai` / `noindex`, `tdm-reservation`) wird vor dem Speichern ausgewertet; liegt er vor, wird nichts gespeichert. Die `robots.txt` wird schon vor dem Abruf geprüft. Die Prüfung geschieht bei jedem Aufbereiten eines Kurses erneut, wirkt damit aber nach vorn: **ein später erklärter Vorbehalt verhindert jeden weiteren Abruf, entfernt bereits gespeicherten Text jedoch nicht von allein.** Dafür gibt es den Weg über eine formlose Nachricht, siehe Abschnitt 4a der Datenschutzerklärung.
- Video- und Übungsplattformen sind vom Abruf ausgenommen.
- Der Abruf trägt eine eindeutige Kennung (`SchoolUP-Ingest`) mit Verweis auf unsere Rechtstexte und überträgt keine Daten der nutzende Personen.

2.2 Eingabekontrolle / Nachvollziehbarkeit

- Zu jeder Einwilligung werden der Zeitpunkt der Einreichung, der Prüfstatus (eingereicht, angenommen, abgelehnt, widerrufen), der Zeitpunkt der Entscheidung, ein optionaler Prüfvermerk der Schulleitung sowie die Fassung des Einwilligungstextes gespeichert. Damit ist nachvollziehbar, wer wann in welche Fassung eingewilligt hat und wie darüber entschieden wurde.
- Deduplizierung von Kursmaterialien über SHA-256-Hash sichert Datenkonsistenz und verhindert Mehrfachverarbeitung.
- Der Gesprächsverlauf liegt auf dem Endgerät und wird mit jeder neuen Frage mitgeschickt. Damit ein Gerät dem Tutor keine Vorgeschichte unterschieben kann, die es nie gegeben hat, versieht der Server jede ausgelieferte Antwort mit einer Prüfsumme (HMAC-SHA256), die an Schule, Kurs und Person gebunden ist. Gesprächsschritte ohne gültige Prüfsumme werden verworfen und gezählt.
- **Geplant:** durchgängiges, manipulationsgeschütztes Zugriffs-/Änderungs-Logging auch für administrative Zugriffe auf Klardaten.

2.3 Speicherbegrenzung und Nachweis der Löschung

- Ein **täglicher Löschlauf** setzt die Fristen des Löschkonzepts ohne Zutun eines Menschen durch. Er läuft einmal je Nacht um 03:15 UTC und führt seit dem 14. August 2026 **zwei** Regeln aus: widerrufene Einwilligungen nach Ablauf der Nachweisfrist, und die Lern-Notizen des KI-Tutors nach zwölf Monaten ohne Nutzung. Die zwei Regeln für die Übungsdaten sind gestrichen, weil die zugehörigen Tabellen abgeschafft sind (siehe 2.3a).
- Er führt **ausschließlich Fristen aus, für die ein Rechtsdokument eine Fundstelle nennt.** Eine Regel ohne Fundstelle wird gezählt und berichtet, aber nicht ausgeführt. Betroffen ist heute keine mehr: die Frist für die Lern-Notizen ist am 14. August 2026 in das Löschkonzept aufgenommen worden, und erst danach hat der Lauf sie übernommen. Diese Reihenfolge ist die Maßnahme: eine Prüfung im Quelltext liest die ausgelieferten Rechtsdokumente und hält sie gegen die Regeln des Laufs, damit weder ein Dokument eine Löschung zusagt, die niemand ausführt, noch der Lauf etwas löscht, das kein Dokument nennt.
- Zwei Obergrenzen, die vor der ersten Löschung greifen: höchstens 500 Zeilen je Lauf, und Abbruch, wenn eine einzelne Regel ab zehn fälligen Zeilen mehr als ein Viertel des Bestands ihrer Tabelle träfe. Greift eine davon, löscht der Lauf in dieser Nacht gar nichts und hält den Abbruchgrund fest.
- **Löschprotokoll.** Jeder Lauf schreibt in die Datenbank, nicht in ein Container-Protokoll: je Schule und Tag den Zustand des Laufs, die je Datenart wirklich gelöschten Zeilen, die fällig gewesenen und die bewusst verschonten. Die Spur enthält keine Kennung einer Person, keinen Kurs und keinen Text. Sie überlebt eine Auslieferung und lässt sich über die normale Schnittstelle des Dienstes nicht fälschen.
- Der Lauf läuft genau einmal je Tag, auch bei mehreren Instanzen oder Neustarts: der erste Lauf beansprucht den Tag in der Datenbank, jeder weitere findet ihn vergeben. Ohne die Datenbank, die dieses Protokoll trägt, startet der Lauf gar nicht.
- Der Widerruf einer Nutzungseinwilligung löscht sofort und in einem Zug: beide Unterschriften, Geburtsdatum, Namen der erziehungsberechtigten Person und sämtliche Lern-Notizen über alle Kurse. Für Web und App ist das derselbe Weg im System, nicht zwei Fassungen. Nimmt die Schulleitung eine Bestätigung zurück, greift derselbe Weg für die Lern-Notizen; die Unterschrift bleibt dann als Nachweis nach Art. 7 Abs. 1 DSGVO stehen.
- Für die anlassbezogene Löschung eines ganzen Kurses (Abmeldung, Vertragsende) besteht eine Funktion, die Material, Einbettungen, Themen sowie die Lern-Notizen aller Lernenden dieses Kurses in einem Zug entfernt. Sie wird auf Anforderung der Schule ausgeführt und bestätigt; **geplant:** ihre Auslösung unmittelbar aus dem Leitungsportal.

2.3a Datenvermeidung: der Bestand, den es nicht mehr gibt

Die wirksamste Maßnahme zur Speicherbegrenzung ist keine Frist, sondern der Verzicht auf die Erhebung (Art. 5 Abs. 1 lit. c DSGVO). Am **14. August 2026** ist der gespeicherte Lernstand vollständig abgeschafft worden.

- Drei Tabellen sind entfallen: der **Lernstand je Thema** (Punkte, getragene Übungsformen, gleitender Stärkewert, Wiederholungsfach, Fälligkeit), die **Übungszahlen je Kurs** und die **Abgabeschlüssel**, mit denen doppelte Meldungen erkannt wurden. Alle drei waren personenbezogen.
- Sie werden nicht nur nicht mehr beschrieben. Beim nächsten Start der Anwendung werden sie **gelöscht, einschließlich der Zeilen, die bereits darin stehen**. Eine stehen gelassene Tabelle wäre nicht leer, sondern voll mit Bewertungen ohne Zweck.
- Aus dem Selbst-Üben entsteht seither ausschließlich eine **personenfreie Zählung**: Schulnummer, Kurs, Tag, Art der Übung. Keine Kennung einer Person, kein Ergebnis. Sie misst, was benutzt wird, nicht, was jemand kann.
- Zwei automatische Prüfungen im Quelltext, eine je Anwendung, verhindern die Rückkehr dieser Anzeigen und Felder. Sie prüfen den Quelltext selbst, weil hier nicht ein Verhalten abgesichert werden soll, sondern dass eine ganze Klasse von Verhalten nicht wieder entsteht.

- **Noch nicht beobachtet:** die Löschung der drei Tabellen ist gegen die Produktionsdatenbank noch nicht gelaufen. Vor der Auslieferung gehört eine frische Sicherung ins Haus und danach eine Kontrolle, dass die Tabellen wirklich weg sind.

3. Verfügbarkeit und Belastbarkeit

- Die Einwilligungs-Datenbank wird **täglich um 03:30 UTC gesichert**, zusätzlich von Hand vor jedem Eingriff am laufenden System. Die Sicherungen sind mit AES-256 verschlüsselt und werden nach 30 Tagen rollierend verworfen; eine gelöschte Zeile ist damit spätestens 30 Tage nach der Löschung auch aus der letzten Sicherung verschwunden. Die Unterschriften bleiben darin in ihrer verschlüsselten Form (AES-256-GCM), eine Sicherung enthält also zu keinem Zeitpunkt Unterschriften im Klartext.
- Die Sicherungen liegen bislang auf **demselben gemieteten Server** wie das Produktivsystem. Sie schützen damit gegen einen fehlerhaften Eingriff und gegen einen Datenbankschaden, nicht gegen den Verlust der Maschine. Das ist bewusst so benannt und nicht beschönigt; die Abhilfe steht unten als geplant.
- Der Wissensspeicher (verarbeitetes Kursmaterial, Embeddings, Lernthemen) ist bewusst wiederherstellbar ausgelegt: Er lässt sich jederzeit vollständig aus den freigegebenen Moodle-Kursen neu aufbauen und ist daher nicht auf Sicherungen angewiesen.
- Unterbrochene Verarbeitungsvorgänge (Texterkennung, Einbettung) werden im nächsten Durchlauf automatisch erneut aufgenommen; ein Abbruch führt nicht zu unvollständigem Kursmaterial.
- Begrenzung der Anmeldeversuche und vorgelagerter Reverse Proxy erhöhen die Widerstandsfähigkeit gegen Überlast und missbräuchliche Zugriffe.
- Begrenzung der KI-Nutzung auf zwei Ebenen: höchstens **20 Fragen je Person innerhalb von zehn Minuten** und ein **Tageskontingent je Schule** für den Verbrauch des Sprachmodells. Beides schützt vor Überlast und vor einer einzelnen Person, die den Dienst für ihre ganze Schule ausbremst.
- Anhänge zu einer Chatfrage sind auf 12 MB und auf Formate begrenzt, aus denen sich Text gewinnen lässt. Die Datei wird nicht gespeichert; der erkannte Text liegt höchstens 30 Minuten im Arbeitsspeicher, an Schule, Kurs und Person gebunden, und berührt keine Festplatte.
- Der Dienst bleibt bei Einzelfehlern verfügbar: unbehandelte asynchrone Fehler führen nicht zum Absturz, sondern werden protokolliert.
- **Geplant:** automatisierte, verschlüsselte Sicherung an einen zweiten, räumlich getrennten Speicherort; formalisierter Notfall- und Wiederanlaufplan (BCM) mit definierten Wiederherstellungszeiten (RTO/RPO); regelmäßige Verfügbarkeitsauswertung.

4. Pseudonymisierung und Verschlüsselung

- Verschlüsselung ruhender sensibler Daten mit AES-256-GCM: Moodle-Webservice-Token, Unterschriften-Bilder und der Text der Lern-Notizen des KI-Tutors.
- Passwörter der Schulleitung als scrypt-Hash (nicht umkehrbar) gespeichert.
- Moodle-Passwort wird nicht gespeichert; Token wird bei jedem Login erneuert (Reduktion des Missbrauchsfensters).
- Transportverschlüsselung durchgängig (TLS/HTTPS).
- **Hinweis:** Eine Pseudonymisierung der Klaridentitäten ist funktionsbedingt (Einwilligungsnachweis) nur eingeschränkt möglich; die Datenminimierung erfolgt über Erforderlichkeitsprüfung und Löschfristen.

5. Trennung

- Getrennte Verarbeitung nach Mandanten (Schulen) und nach Zwecken (siehe 1.4).
- Kursbezogene OCR-Daten sind von personenbezogenen Einwilligungsdaten funktional getrennt.

6. Wiederherstellbarkeit

- Aus den Sicherungen der Einwilligungs-Datenbank lässt sich der Stand vor jeder Änderung vollständig wiederherstellen; das Vorgehen ist in einem Betriebshandbuch schriftlich festgehalten.
- Der Wissensspeicher wird bei Verlust durch erneutes Einlesen der freigegebenen Kurse wiederhergestellt.
- Unterbrochene Verarbeitungsvorgänge werden selbsttätig fortgesetzt.
- **Geplant:** dokumentierte, regelmäßige Wiederherstellungstests (Restore-Tests) mit Protokollierung.

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d)

- Sicherheitsrelevante Konfigurationen (Pflicht-Secrets, Herkunftsprüfung, TLS) werden beim Start validiert; automatisierte Tests prüfen die zugesagten Schutzmaßnahmen bei jeder Änderung.
- Dieses TOM-Dokument sowie das Löschkonzept werden bei wesentlichen Änderungen des Dienstes aktualisiert.
- **Geplant:** festgelegter Überprüfungszyklus (mindestens jährliche Review der TOM); Verpflichtung der handelnden Personen auf Vertraulichkeit in dokumentierter Form; regelmäßige Schwachstellen-/Sicherheitsprüfungen (z. B. Penetrationstests, Dependency-Scans); Benennung fester Verantwortlichkeiten für das Datenschutz- und Informationssicherheitsmanagement; Verfahren zur Behandlung von Datenschutzvorfällen (nach Art. 33/34) formal dokumentiert.

Auftragskontrolle (Unterauftragsverarbeiter): Die **STRATO AG**, Otto-Ostrowski-Straße 7, 10249 Berlin (Konzerngesellschaft der IONOS SE; die IP-Adressbereiche des Rechenzentrums sind auf die IONOS SE registriert, wer die Serveradresse nachschlägt, findet deshalb diesen Namen), und die **Mistral AI SAS**, 15 Rue des Halles, 75001 Paris, Frankreich, sind über Verträge zur Auftragsverarbeitung eingebunden; ihre Maßnahmen sind Bestandteil des Gesamtschutzniveaus und bei den jeweiligen Anbietern nachzuweisen. Weitere Dienste Dritter werden nicht eingebunden: kein Tracking, keine Analyse-, Werbe-, Karten-, Schriftarten- oder Auslieferungsdienste, kein Versanddienst für E-Mail oder Push-Nachrichten, kein Dienst zur Fehlerübermittlung. Die einzigen ausgehenden Verbindungen des Servers gehen an das Moodle der jeweiligen Schule, an `api.mistral.ai`, an den Objektspeicher `s3.hidrive.strato.com` (nur Chiffrat, siehe Nr. 2.1b) und an die im Kurs verlinkten Webseiten (Nr. 2.1a).