ANLAGE 2 ZUM NUTZUNGS- BZW. LIZENZVERTRAG

Technische und organisatorische Maßnahmen

Art. 32 DSGVO

Anlage 2 zum Nutzungsvertrag bzw. Lizenzvertrag; beschreibt die Maßnahmen nach Ziffer 4 des Vertrags zur Auftragsverarbeitung **(Art. 28 Abs. 3 lit. c DSGVO)**. Zu jeder Maßnahme ist angegeben, wo sie im Programmcode umgesetzt ist. Ein automatischer Test vergleicht diese Angaben bei jeder Änderung mit dem Code; ändert sich eine der genannten Dateien, wird diese Anlage überprüft und neu veröffentlicht. Maßnahmen, die noch nicht umgesetzt sind, stehen als „geplant" darin.

1 Architektur in einem Satz

SchoolUP speichert keine Kursinhalte und keine Nutzerdaten auf eigenen Systemen. Das Suchverzeichnis liegt im Moodle der Schule, die Sitzung verschlüsselt im Browser, der Gesprächsverlauf nur auf dem Gerät. Personenbezogene Daten verarbeitet der Server nur für die Dauer einer Anfrage im Arbeitsspeicher; Kursmaterial ohne Personenbezug hält er höchstens 30 Minuten im Arbeitsspeicher, um schneller zu antworten, nie auf einem Datenträger. Das reduziert die meisten Risiken bereits durch die Bauweise (Datenschutz durch Technikgestaltung, Art. 25 DSGVO).

2 Vertraulichkeit

MASSNAHME	STAND
Alle Verbindungen über TLS (HTTPS), Zertifikate automatisch erneuert. `deploy/server/Caddyfile`	umgesetzt
Zugriff auf Kursmaterial nur mit einer Moodle-Rolle, die ausschließlich sichtbares Material lesen darf; Teilnehmer, Profile, Foren, Abgaben, Bewertungen und verborgene Inhalte sind verboten. Die Rollen gibt es als importierbare Datei mit Versionsnummer; SchoolUP prüft bei jedem Einlesen, ob sie vollständig eingerichtet sind. `packages/moodle/src/rollen.ts` · `deploy/testschule/rollen.php` · `go/einlesen/indexieren.go`	umgesetzt
Bei Anmeldung mit Passwort wird mit dem Zugang der fragenden Person geprüft, ob sie im Kurs eingeschrieben ist. Das Ergebnis gilt höchstens 5 Minuten (verschlüsselt im Sitzungs-Cookie); danach und für jeden Kurs außerhalb dieses Ergebnisses fragt SchoolUP Moodle erneut. `go/kurse/zugang.go` · `go/tutor/fragen.go`	umgesetzt
Anmeldung über Moodle nach LTI 1.3: Prüfung der Signatur (RS256) gegen die Schlüssel des Schul-Moodles, von Aussteller, Empfänger, Bereitstellung, Ablauf (höchstens 5 Minuten alt) und einer Einmal-Nonce. Nur das Moodle dieser Schule kann SchoolUP registrieren. Zugriff nur auf die von Moodle bestätigten	umgesetzt

MASSNAHME	STAND
Kurse und darin nur auf Dateien aus deren Manifest. Mit der optionalen Rolle „lesen + Kursliste“ fragt SchoolUP die Kurse der Person bei Moodle ab und übernimmt das Ergebnis höchstens 5 Minuten verschlüsselt in die Sitzung (Austragungen wirken spätestens nach 5 Minuten); ohne sie gilt die beim Start bestätigte Kursberechtigung für die Dauer der Sitzung (höchstens 8 Stunden). `go/anbindung/moodle/lti.go` · `go/kurse/zugang.go`	
Dokumente werden nur angezeigt, wenn sie im Manifest eines Kurses der Person stehen; das prüft SchoolUP bei jedem Abruf. Bei Anmeldung mit Passwort lädt SchoolUP sie bei jedem Abruf mit dem Zugang der Person, Moodle prüft die Berechtigung dann zusätzlich selbst. `go/http/kurse.go` · `go/kurse/zugang.go`	**umgesetzt**
Sicherheits-Header (HSTS, nosniff, Referrer-Policy, Permissions-Policy: Standort aus, Kamera und Mikrofon darf nur die App selbst nutzen, für den Gerätewechsel und zum Sprechen einer Frage, eingebettete fremde Seiten nie; Schutz vor Einbettung in fremde Seiten); eine Content-Security-Policy lässt in App und Verwaltung nur Skripte von SchoolUP selbst zu. `deploy/server/Caddyfile` · `go/http/server.go`	**umgesetzt**
Begrenzung der Anfragen je IP-Adresse am Webserver (Anmeldungen 60 je Minute; insgesamt 1.200–6.000 je Minute je nach Dienst, großzügig wegen Schulnetzen hinter einer Adresse). `deploy/server/Caddyfile` · `deploy/moodle/caddy/Dockerfile`	**umgesetzt**
Begrenzung in der App: Anmeldungen 60 je Minute und IP sowie 10 je Minute und Benutzername; Fragen (Übersetzungen, gesprochene Fragen und Vorlesen zählen mit) 20 je Minute und 300 je Tag und Person; Probeklausuren 8, Abgaben 20, Fotolesungen (Klausurbearbeitung und Aufgaben im Chat zusammen, jede Datei einzeln) 30 und Lernpakete 15 je Person und Tag; je Schule zusammen höchstens 400 Probeklausuren, 800 Abgaben und 2.000 Fotolesungen am Tag (Voreinstellungen, je Schule einstellbar). Für Sprechen und Vorlesen zusätzlich höchstens 3 Cent je Person und Tag (vorgelesen werden höchstens 2.000 Zeichen einer Antwort; nur Beträge im Arbeitsspeicher). Kostenschutz je Schule (KI-Kontingent): 70 % des monatlichen Entgelts ohne Umsatzsteuer, an einem Tag höchstens ein Zehntel davon (in Klausurphasen mal ihrem Faktor); ist ein Viertel verbraucht, pausiert das Vorlesen, bei 90 % Probeklausuren, Übungspakete und Sprechen, bei 100 % alles außer der Hilfe in einer Krise (gezählt nach den Preisen von Mistral; der Monat aus den Zählern im Moodle der Schule, nur Beträge). Je Person wird höchstens eine Probeklausur zur Zeit geschrieben; scheitert eine Arbeit, zählt sie nicht. In Klausurphasen, die die Schule festlegt, gelten die Tageskontingente mit einem Faktor von höchstens 5; die Grenze je Minute bleibt. Schreibende Anfragen nimmt die App nur von ihren eigenen Seiten an (Prüfung der Herkunft) und nur bis 1 MB, außer Fotos und Abgaben einer Probeklausur und dem Foto einer Aufgabe. `go/http/sicherheit.go` · `go/http/lernen.go` · `go/verzeichnis/lizenz.go` · `go/tutor/sprache.go` · `go/schulen/budget.go`	**umgesetzt**
Aktivierung durch die Eltern nur mit dem Elternpasswort der Schule (12 Zeichen, etwa 60 Bit, jederzeit erneuerbar), zeitkonstant geprüft und auf 10 Versuche je Minute und IP-Adresse begrenzt. Die Einwilligung wird erst mit der Anmeldung des Moodle-Kontos wirksam und gilt nur für genau dieses Konto: eingelöst wird sie nur bei der Anmeldung auf der Aktivierungsseite oder über den Knopf im Moodle-Kurs; eine gewöhnliche Anmeldung, das Abmelden und „Abbrechen“ verwerfen eine offene Einwilligung im Browser. Selbst einwilligen kann nur, wen die Schule dafür festlegt (Regel 2: alle, Globale Gruppen oder niemand; Standard niemand), und jede Lehrkraft; angemeldet, mit ausdrücklicher Zustimmung. Ohne gültige Aktivierung beantwortet SchoolUP keine Anfrage. `go/schulen/einwilligung.go` · `go/http/aktivierung.go` · `go/schulen/aktivierung_test.go` · `go/anbindung/moodle/lti_test.go`	**umgesetzt**
Die Verwaltung von SchoolUP (Schulen, Lizenzen, Zugänge der Dienstkonten) ist nur unter eigener Adresse und nur mit Passkey erreichbar (WebAuthn mit Bestätigung am Gerät, kein Passwort). Der erste Zugang braucht einen Einrichtungscode, weitere nur eine einmalige Einladung eines Admins. Sitzungen enden nach 8 Stunden; Änderungen werden nur von der eigenen Adresse angenommen. Jede Änderung wird mit Person, Zeit und geänderten Feldern protokolliert; Passwörter erscheinen dort nie und werden auch der Oberfläche nicht ausgeliefert. Passkeys lassen sich entfernen, der letzte eines Admins nicht. Exporte als CSV entschärfen Zellen, die eine Tabellenformel auslösen könnten.	**umgesetzt**

MASSNAHME	STAND
go/verwaltung/anmeldung.go · go/verwaltung/routen.go · go/http/verwaltung_test.go	
Der Erwartungshorizont einer Probeklausur wird mit AES-256-GCM versiegelt und an Kurs, Person und den unveränderten Bogen gebunden. Vor der Abgabe kann ihn niemand lesen; ein veränderter Bogen oder ein fremdes Siegel wird abgelehnt. Inhalte der Abgabe gelten gegenüber dem Sprachmodell als Daten, nicht als Anweisungen. go/klausur/erzeugen.go · go/klausur/bewerten.go · go/klausur/klausur_test.go	umgesetzt
Moodle der Testschule sperrt ein Konto nach 10 Fehlversuchen für 30 Minuten; Passwörter mindestens 10 Zeichen; Cookies nur über HTTPS und HttpOnly. deploy/server/haerten.sh	umgesetzt
Server-Zugang ausschließlich per SSH-Schlüssel (Ed25519); Passwort-Anmeldung abgeschaltet; höchstens 3 Versuche je Verbindung. deploy/server/haerten.sh	umgesetzt
Firewall: von außen nur SSH, HTTP und HTTPS erreichbar; alle internen Dienste (Datenbank, Suchmodell, Umwandlung, App) ohne öffentlichen Port. deploy/server/haerten.sh · deploy/server/docker-compose.yml · deploy/moodle/docker-compose.yml	umgesetzt
fail2ban sperrt IP-Adressen nach 5 fehlgeschlagenen SSH-Anmeldungen (1 Stunde, bei Wiederholung bis 1 Woche). deploy/server/haerten.sh	umgesetzt
Zugangsdaten und Schlüssel der Betreiber liegen verschlüsselt im Schlüsselbund des Betreiber-Rechners, nicht im Klartext; Geheimnisse auf dem Server nur für root lesbar. deploy/server/haerten.sh	umgesetzt

3 Trennung

MASSNAHME	STAND
Jede Schule ist von den anderen getrennt: eigenes Dienstkonto, Ablage im eigenen Moodle, Sitzung, Kontingente und versiegelte Probeklausuren an die Schule gebunden. Eine Anmeldung über Moodle wird gegen den Aussteller genau dieser Schule geprüft; die Schule steht versiegelt im Anmeldezustand. Moodle-Kennungen gelten nur innerhalb ihrer Schule. go/schulen/kontext.go · go/anbindung/moodle/lti.go · go/verzeichnis/datei_test.go	umgesetzt
Dokumentumwandlung in eigenem Container, Arbeitsdateien nur im RAM (tmpfs), keine Abrufe externer Ressourcen. deploy/server/docker-compose.yml	umgesetzt

4 Datenminimierung

MASSNAHME	STAND
SchoolUP liest und beantwortet nur Kurse im lizenzierten Umfang der Schule (ganze Schule, Kursbereiche wie „Oberstufe“ oder einzelne Kurse). Kurse außerhalb werden nicht eingelesen; ihre Ablage wird gelöscht. SchoolUP läuft an einer Schule erst, wenn der unterschriebene Vertrag (mit AVV) eingetragen ist, und nach dem letzten Vertragstag nicht weiter; danach wird die Ablage beim nächsten Lauf gelöscht. In Ruhezeiten, die die Schule festlegt (z. B. Ferien), ist SchoolUP pausiert: keine Anfragen, kein Einlesen. Beschränkt die Schule die Nutzung oder einzelne Funktionen auf Globale Gruppen ihres Moodle, gilt das nur für deren	umgesetzt

MASSNAHME	STAND
Mitglieder; Lehrkräfte immer. Die Gruppen fragt SchoolUP über einen eigenen Webservice der Schule ab, der nur die beiden Gruppen-Funktionen enthält; die gelieferte Liste der Kontonummern prüft SchoolUP nur auf die angemeldete Person, im Arbeitsspeicher, und verwirft sie sofort. `go/verzeichnis/lizenz.go` · `go/einlesen/indexieren.go` · `go/kurse/zugang.go` · `go/schulen/kontext.go` · `go/anbindung/moodle/lti_test.go`	
SchoolUP ruft in Moodle nur eine abschließende Liste von Funktionen auf (Material, eigene Ablage, Kursliste der angemeldeten Person, öffentliche Einstellungen) – keine Teilnehmerlisten, keine Profile. Durch automatischen Test erzwungen. `packages/moodle/src/rollen.ts` · `packages/recht/src/recht.test.ts`	umgesetzt
Keine Datenbank mit Kursinhalten oder Nutzerdaten bei SchoolUP. Kursmaterial ohne Personenbezug (Suchverzeichnis, Textabschnitte, angezeigte Dateien) hält die App höchstens 30 Minuten im Arbeitsspeicher, um schneller zu antworten, nie auf einem Datenträger; personenbezogene Daten nur für die Dauer einer Anfrage (und die Kursbestätigung im verschlüsselten Sitzungs-Cookie). `go/tutor/fragen.go` · `go/einlesen/indexieren.go` · `go/kurse/ablage/zwischenspeicher.go`	umgesetzt
Von den Rollen, die Moodle beim Start übermittelt, behält SchoolUP nur ein Merkmal: ob die Person im Kurs des Starts lehrt (Kursrolle „Instructor“). Es öffnet allein die Seite „Kursstatus“ dieses Kurses, die nur Angaben über das Kursmaterial zeigt und nichts über Schülerinnen und Schüler. Die Seite ist ohne Aktivierung erreichbar, weil sie keine Daten über Personen enthält; Einschreibung und Lizenzumfang gelten wie überall. Bei Anmeldung mit Passwort fragt SchoolUP Moodle mit dem Zugangsschlüssel der Person nur, was sie selbst in ihren Kursen darf (Lehrrechte ja/nein), nicht nach anderen Personen; das Ergebnis liegt höchstens 5 Minuten im Arbeitsspeicher. Durch automatischen Test erzwungen. `go/anbindung/moodle/lti.go` · `go/http/kursstatus.go` · `go/http/server.go` · `packages/recht/src/recht.test.ts`	umgesetzt
Krisen-Schutz im Chat: Schreibt jemand, dass es ihm selbst ernsthaft schlecht geht, zeigt die App Hilfsangebote statt Unterricht. Erkannt wird im Code, bevor irgendetwas den Server verlässt; die Nachricht geht nicht an das Sprachmodell (auch nicht später im Verlauf oder Lernzettel), wird nicht protokolliert, nicht gemeldet und auf dem Gerät nicht im Verlauf gespeichert. Was die Muster nicht erkennen, fängt eine Regel im Auftrag an das Sprachmodell auf (Hilfe statt Unterricht). `go/tutor/krise.go` · `go/tutor/fragen.go` · `go/tutor/lernzettel.go` · `apps/web/src/seiten/Chat.tsx` · `packages/recht/src/recht.test.ts`	umgesetzt
Gesprächsverlauf nur auf dem Gerät; beim Abmelden gelöscht. `apps/web/src/daten/verlauf.ts` · `apps/web/src/App.tsx`	umgesetzt
Betriebsprotokolle ohne Inhalte und Kennungen (durch automatischen Test erzwungen). `go/basis/log.go` · `packages/recht/src/recht.test.ts`	umgesetzt
Texterkennung nur für Seiten mit Bildinhalt; abschaltbar je Instanz (OCR_AKTIV=0). `go/einlesen/lesen.go` · `go/basis/konfig.go`	umgesetzt

5 Integrität

MASSNAHME	STAND
Automatische Sicherheitsupdates des Betriebssystems täglich, Neustart bei Bedarf nachts; Kernel-Netzwerkschutz (SYN-Cookies, keine Redirects, kein Source-Routing). `deploy/server/haerten.sh`	umgesetzt
Versuche, den Tutor über eine Eingabe umzuprogrammieren („Ignoriere alle Anweisungen …“), beantwortet der Code selbst, ohne Sprachmodell. Der Auftrag an das Sprachmodell legt fest, dass Eingaben, Verlauf und Kursmaterial Daten sind, keine Anweisungen, und dass es nichts für Kinder und Jugendliche Ungeeignetes schreibt, auch nicht als Rollenspiel.	umgesetzt

MASSNAHME	STAND
go/tutor/schutz.go · go/ki/sprachmodell.go	
Änderungen werden über ein Ausroll-Skript eingespielt, das Typprüfung, Tests und die Prüfung der Rechtsdokumente voraussetzt; antwortet danach eine Hauptadresse nicht, geht es automatisch auf den vorherigen Stand zurück. Ausgerollt wird nur ein in der Versionsverwaltung festgehaltener Stand; seine Kennung meldet der Server danach selbst. deploy/server/ausrollen.sh	umgesetzt

6 Pseudonymisierung und Verschlüsselung

MASSNAHME	STAND
Sitzung als verschlüsseltes Cookie (AES-256-GCM); auf dem Server keine Sitzungsdaten. go/basis/sitzung.go	umgesetzt
An das Sprachmodell gehen keine Namen, Kennungen oder Zugangsdaten. go/ki/sprachmodell.go	umgesetzt

7 Verfügbarkeit und Belastbarkeit

MASSNAHME	STAND
Dienste starten nach Ausfall automatisch neu; Kursinhalte liegen im Moodle der Schule und lassen sich jederzeit neu einlesen. deploy/server/docker-compose.yml	umgesetzt
Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c DSGVO): Der Server hält keine Daten über Schülerinnen und Schüler. Suchverzeichnis und Einlesestand liegen im Moodle der Schule; einziger Zustand auf dem Server ist das verschlüsselte Schulverzeichnis mit den Geschäftsdaten von SchoolUP (Schulen, Verträge, Lizenzen, Anfragen von Schulen), das täglich gesichert wird; nach einer Neuinstallation genügen die Zugangsdaten, und der Dienst übernimmt den vorhandenen Stand ohne erneutes Einlesen. Erprobt am 18.10.2026: vollständige Neuinstallation in unter vier Minuten, keine Datei neu gelesen, angemeldete Sitzungen blieben gültig. go/einlesen/indexieren.go · go/kern/ablage.go · deploy/server/docker-compose.yml	umgesetzt
Tägliche Sicherung von Konfiguration, Schlüsseln und Moodle-Testschule auf dem Server (7 Tage) und verschlüsselt (AES-256) außerhalb des Servers beim Betreiber (30 Sicherungen). Jede abgeholte Sicherung wird probeweise entschlüsselt und entpackt; fehlt eine aktuelle Sicherung, meldet sich der Betreiber-Rechner. Er meldet jede Abholung dem Server; liegt die letzte länger als 2 Tage zurück, warnt die Verwaltung. deploy/server/haerten.sh · deploy/server/sichern.sh	umgesetzt
Statusseite (/status) und Prüfadresse (/api/status): Erreichbarkeit von App, Suche, Umwandlung und Sprachmodell, höchstens einmal je Minute geprüft, ohne Inhalte und ohne Personendaten. Die Prüfadresse meldet eine Störung mit Status 503. go/basis/zustand.go · go/http/statusseite.go	umgesetzt
Externer Wächter ruft die Prüfadresse jede Minute auf und alarmiert den Betreiber bei einer Störung. –	geplant

8 Überprüfung

MASSNAHME	STAND
Automatischer Abgleich dieser Angaben mit dem Code bei jedem Ausrollen; Fingerabdrücke aller rechtlich relevanten Dateien. `packages/recht/src/recht.test.ts`	umgesetzt

9 Organisatorische Maßnahmen

- Zugriff auf Server und Schlüssel haben nur die beiden Gesellschafter; sie sind auf Vertraulichkeit verpflichtet.
- Zugangsdaten (Dienstkonto, Sitzungsschlüssel, API-Schlüssel) liegen nur in der Umgebung des Servers, nicht im Programmcode.
- Sicherheitsvorfälle werden nach Ziffer 7 des AVV binnen 24 Stunden an die Schule gemeldet.
- Jede Änderung des Programms durchläuft vor dem Ausrollen die automatischen Tests einschließlich des Abgleichs dieser Unterlagen.
- Betriebsprotokolle: Die Protokolle jedes Dienstes werden rotiert: höchstens 3 Dateien zu je 10 MB, ältere Einträge werden überschrieben. Ein Zugriffsprotokoll des Webservers wird nicht geführt. Das Systemprotokoll des Servers (u. a. Anmeldeversuche am Administrationszugang) wird nach 14 Tagen gelöscht.

10 Verfahren zur Überprüfung

Die Wirksamkeit der Maßnahmen wird bei jeder Änderung automatisch geprüft (Art. 32 Abs. 1 lit. d DSGVO): Der Test `packages/recht/src/recht.test.ts` stellt u. a. sicher, dass der Code nur mit den genannten Diensten spricht, keine weiteren Cookies oder Speicher im Browser nutzt, keine Inhalte oder Kennungen protokolliert und die genannten Fristen einhält. Darüber hinaus überprüfen die Gesellschafter die Maßnahmen mindestens jährlich.

Hübner/Eßer GbR · Elias Eßer und Sean Hübner · Süchtelner Straße 33, 47877 Willich-Anrath · kontakt@school-up.de · +49 157 89160932
Diese Fassung (Version 1.94 vom 09.11.2026) ist Teil der Unterlagen unter school-up.de/recht. Dort stehen auch der Änderungsverlauf und die jeweils aktuelle Fassung.