Misure tecniche e organizzative

Versione del 12 novembre 2026 · Traduzione a scopo informativo. Fa fede la versione tedesca.

Premessa

Le misure sono strutturate secondo gli obiettivi di protezione dello Standard-Datenschutzmodell delle autorità tedesche di controllo per la protezione dei dati. SchuleVernetzt è sviluppato e gestito da SavePaperwork come impresa individuale.

1. Minimizzazione dei dati

- Gli alunni non hanno un account. Vengono conservati solo nome, cognome e classe; nessuna data di nascita, nessun indirizzo, nessun numero di telefono, nessuna foto.
- Il motivo della malattia viene chiesto solo se la scuola attiva questa opzione; la domanda è disattivata per impostazione predefinita. Per le segnalazioni di assenza dei docenti non viene mai memorizzato un motivo.
- Le scuole possono disattivare il caricamento dei certificati medici; per le scuole della Renania Settentrionale-Vestfalia, del Brandeburgo e di Berlino è disattivato per impostazione predefinita.
- Le notifiche contengono il minimo indispensabile: la notifica di un messaggio indica solo il mittente, non l'oggetto né il testo; il promemoria di un certificato medico sulla schermata di blocco non indica alcun bambino.
- L'account dell'ente gestore (Schulträger) vede solo i nomi delle scuole e indicatori chiave, nessuna persona.
- Il link di classe e lo schermo dell'atrio non mostrano alcun nome di alunni né docenti assenti.
- Cancellazione per tipo di dati secondo i termini del Land, una volta che la dirigenza scolastica li ha confermati.
- Le voci di accesso in lettura nell'audit log vengono cancellate dopo 90 giorni (tranne le prove delle richieste di accesso evase), i log dell'applicazione dopo 14 giorni; l'audit log della scuola non memorizza indirizzi IP.
- Il fornitore di hosting conserva i log di accesso con l'indirizzo IP completo fino a 90 giorni e i log degli errori fino a 7 giorni, per analizzare i guasti e contrastare gli abusi.
- Nelle pagine della scuola, né nelle e-mail della scuola, non è in funzione alcun servizio di analisi o di tracciamento né alcun font di terzi.

2. Disponibilità

- Gestione in un data center certificato ISO 27001 a Francoforte sul Meno (secondo il fornitore di hosting).
- Backup giornaliero da parte del fornitore di hosting, cifrato con AES-256, in un data center separato a Helsinki, conservato per 90 giorni.
- Le nuove versioni vengono attivate in modo atomico; un ritorno alla versione precedente è possibile in qualsiasi momento. Le modifiche allo schema del database non vengono mai applicate automaticamente.
- Monitoraggio automatico ogni cinque minuti (database, processi in background, accumuli di errori) con avvisi sul telefono del gestore.
- Il registro di classe può essere compilato anche durante un'interruzione di rete; le annotazioni vengono trasmesse non appena il dispositivo torna online.
- La scuola può scaricare autonomamente in qualsiasi momento un'esportazione completa di tutti i dati, anche dopo la fine del contratto (garanzia di esportazione).
- L'obiettivo è una disponibilità del 99,5% come media annuale, escluse le manutenzioni annunciate.

3. Integrità

- I contenuti cifrati utilizzano una cifratura autenticata; qualsiasi alterazione viene rilevata in lettura e non viene mai accettata in silenzio.

- L'audit log registra chi ha creato, modificato o cancellato un record e quando, con il valore precedente e quello nuovo; i valori sensibili vi sono oscurati.
- I moduli sono protetti contro la falsificazione di richieste tra siti (cross-site request forgery); l'input viene convalidato sul server.
- I file caricati vengono verificati per tipo e contenuto (PDF, JPG, PNG, WebP, DOCX; al massimo 10 MB; nessuna doppia estensione) e archiviati con un nome casuale.
- Ogni modifica al codice passa attraverso test automatizzati, compresi i test sulla separazione tra le scuole.

4. Riservatezza

- Ruoli e autorizzazioni: la dirigenza scolastica vede tutto; la segreteria solo ciò che le è stato espressamente reso accessibile; i docenti solo le proprie classi e materie; i genitori solo i propri figli. Solo la dirigenza scolastica, la segreteria e il coordinatore di classe possono leggere il motivo della malattia, e ogni accesso in lettura ad esso viene registrato.
- Separazione delle scuole: tutti i dati appartengono a una sola scuola; ogni interrogazione è limitata a tale scuola.
- Cifratura nell'applicazione (libsodium; XSalsa20-Poly1305 per i campi, XChaCha20-Poly1305 per i file) per i motivi di malattia, i valori e i commenti dei voti, i testi delle pagelle, le annotazioni sul registro di classe riguardanti gli alunni, i messaggi e tutti i file caricati. La chiave è conservata solo nella configurazione del server; il fornitore di archiviazione dei file riceve solo testo cifrato.
- Trasmissione esclusivamente tramite HTTPS con HSTS; cookie di sessione solo tramite HTTPS e non leggibili dagli script.
- Nelle aree della scuola una Content Security Policy consente solo gli script della piattaforma stessa; il browser non esegue codice iniettato e nessun altro sito può incorporare queste aree.
- Password solo come hash (bcrypt o Argon2); le sessioni vengono terminate quando si cambia la password; i link per reimpostare la password sono validi per 24 ore e utilizzabili una sola volta.
- Protezione contro gli attacchi a tentativi: al massimo cinque tentativi di accesso consecutivi, più un rompicapo computazionale (ALTCHA) senza fornitore terzo.
- Secondo fattore (TOTP) obbligatorio per la segreteria e l'ente gestore, disponibile per la dirigenza scolastica, oltre alle passkey. Anche insegnanti e genitori possono attivare il secondo fattore; la scuola può renderlo obbligatorio per il corpo docente. Le scuole possono configurare l'accesso scolastico (OIDC, ad esempio Microsoft Entra, Google o un login del Land) e utilizzarne l'autenticazione a più fattori.
- I file sono conservati in uno spazio di archiviazione privato senza accesso pubblico e vengono consegnati solo tramite l'applicazione dopo un controllo dei permessi.
- I log dell'applicazione possono essere letti solo dal gestore; un filtro rimuove indirizzi, parametri, segreti e token prima che venga scritto qualcosa.
- Le credenziali di accesso del server sono conservate solo in un file di configurazione protetto; gli ambienti di sviluppo e di test non possono raggiungere l'archiviazione di produzione.
- Il gestore accede ai dati di una scuola solo quando l'esercizio, la risoluzione di problemi o una richiesta della scuola lo richiedono; il gestore è vincolato al segreto ai sensi del § 203 StGB (codice penale tedesco). Se a tal fine accede come una persona della scuola tramite la funzione «Cambia utente», le sue azioni compaiono nell'audit log della scuola come «Gestore della piattaforma (SavePaperwork)» con il suo nome, non come azioni di quella persona.

5. Non correlabilità (limitazione della finalità)

- I dati vengono trattati solo per la scuola: nessuna pubblicità, nessuna profilazione, nessuna comunicazione a terzi, nessun addestramento di modelli di IA; nel prodotto scolastico non sono integrati servizi di IA.
- Una rete di scuole non condivide nulla finché ogni scuola non vi aderisce e non acconsente per ciascun ambito (pool di supplenze, corsi, materiali); la scuola richiedente vede i dati di contatto di un supplente solo dopo che sono stati rilasciati. L'uscita dalla rete blocca immediatamente l'accesso.
- I dati di produzione delle scuole non vengono mai copiati negli ambienti di sviluppo o di test; lì il gestore lavora con dati di esempio fittizi.

6. Trasparenza

- Nell'audit log la dirigenza scolastica vede chi ha modificato quali dati e chi ha aperto quali elenchi contenenti dati sensibili.
- Il contratto, le misure, i sub-responsabili, i termini di conservazione per Land, i modelli per la valutazione d'impatto e per il registro delle attività di trattamento, nonché le informative per genitori, personale e alunni sono pubblicamente disponibili.
- I nuovi sub-responsabili vengono annunciati con 30 giorni di anticipo.

7. Intervenibilità

- Accesso e portabilità dei dati: esportazione di tutti i dati di un alunno o di un genitore con un clic; esportazione dell'intera scuola in qualsiasi momento.
- La scuola esegue autonomamente rettifica, cancellazione e limitazione nell'applicazione.
- La scuola stabilisce autonomamente i termini di conservazione, gli ambiti, la domanda sul motivo della malattia e la visibilità per i genitori; un link di classe può essere rinnovato o disattivato in qualsiasi momento.
- Notifica delle violazioni dei dati alla scuola senza ingiustificato ritardo, di norma entro 24 ore.

8. Organizzazione

- SavePaperwork è un'impresa individuale; il titolare sviluppa e gestisce personalmente la piattaforma. Altre persone ottengono l'accesso solo dopo essere state vincolate alla riservatezza e al § 203 StGB.
- Le nuove versioni vengono distribuite solo dal titolare, tramite la propria connessione cifrata al server.
- Al momento non è stato nominato alcun responsabile della protezione dei dati; il referente è il titolare.
- Queste misure vengono riesaminate a ogni modifica sostanziale della piattaforma e almeno una volta all'anno.