Środki techniczne i organizacyjne

Wersja z 12 listopada 2026 · Tłumaczenie informacyjne. Wiążąca jest wersja niemiecka.

Uwaga wstępna

Środki zostały uporządkowane według celów ochrony Standardowego Modelu Ochrony Danych niemieckich organów nadzorczych ds. ochrony danych. SchuleVernetzt jest rozwijane i prowadzone przez SavePaperwork jako jednoosobową działalność.

1. Minimalizacja danych

- Uczniowie nie mają konta. Przechowywane są wyłącznie imię, nazwisko i klasa; bez daty urodzenia, adresu, numeru telefonu i zdjęcia.
- O powód choroby pyta się tylko wtedy, gdy szkoła włączy tę opcję; domyślnie pytanie jest wyłączone. W przypadku zgłoszeń nieobecności nauczycieli powód nie jest nigdy zapisywany.
- Szkoły mogą wyłączyć przesyłanie zwolnień lekarskich; dla szkół w Nadrenii Północnej-Westfalii, Brandenburgii i Berlinie jest ono domyślnie wyłączone.
- Powiadomienia zawierają jak najmniej: powiadomienie o wiadomości wymienia tylko nadawcę, nie temat ani treść; przypomnienie o zwolnieniu lekarskim na ekranie blokady nie wymienia żadnego dziecka.
- Konto organu prowadzącego (Schulträger) widzi tylko nazwy szkół i wskaźniki, żadnych osób.
- Link klasy i ekran w holu nie pokazują nazwisk uczniów ani nieobecnych nauczycieli.
- Usuwanie według rodzajów danych zgodnie z okresami obowiązującymi w kraju związkowym, po ich potwierdzeniu przez dyrekcję szkoły.
- Wpisy o dostępie do odczytu w dzienniku zdarzeń są usuwane po 90 dniach (z wyjątkiem potwierdzeń zrealizowanych żądań dostępu), logi aplikacji po 14 dniach; dziennik zdarzeń szkoły nie przechowuje adresów IP.
- Dostawca hostingu przechowuje dzienniki dostępu z pełnym adresem IP do 90 dni, a dzienniki błędów do 7 dni, aby badać awarie i przeciwdziałać nadużyciom.
- Na stronach szkoły ani w e-mailach szkoły nie działają żadne usługi analityczne ani śledzące, ani czcionki podmiotów trzecich.

2. Dostępność

- Działanie w centrum danych w Frankfurcie nad Menem z certyfikatem ISO 27001 (według dostawcy hostingu).
- Codzienna kopia zapasowa wykonywana przez dostawcę hostingu, szyfrowana AES-256, w osobnym centrum danych w Helsinkach, przechowywana przez 90 dni.
- Nowe wersje są przełączane atomowo; powrót do poprzedniej wersji jest możliwy w każdej chwili. Zmiany schematu bazy danych nigdy nie są stosowane automatycznie.
- Automatyczny monitoring co pięć minut (baza danych, zadania w tle, nagromadzenia błędów) z alertami na telefon operatora.
- Dziennik lekcyjny można prowadzić także podczas awarii sieci; wpisy są przesyłane, gdy tylko urządzenie znów jest online.
- Szkoła może w każdej chwili samodzielnie pobrać pełny eksport wszystkich danych, także po zakończeniu umowy (gwarancja eksportu).
- Celem jest dostępność na poziomie 99,5% jako średnia roczna, z wyłączeniem zapowiedzianych prac konserwacyjnych.

3. Integralność

- Zaszyfrowane treści korzystają z szyfrowania uwierzytelnionego; każda zmiana zostaje wykryta przy odczycie i nigdy nie jest po cichu akceptowana.

- Dziennik zdarzeń rejestruje, kto i kiedy utworzył, zmienił lub usunął wpis, ze starą i nową wartością; wartości wrażliwe są w nim zaczernione.
- Formularze są chronione przed cross-site request forgery; dane wejściowe są walidowane na serwerze.
- Przesyłane pliki są sprawdzane pod względem typu i zawartości (PDF, JPG, PNG, WebP, DOCX; najwyżej 10 MB; bez podwójnych rozszerzeń) i zapisywane pod losową nazwą.
- Każda zmiana kodu przechodzi przez zautomatyzowane testy, w tym testy rozdzielenia szkół.

4. Poufność

- Role i uprawnienia: dyrekcja szkoły widzi wszystko; sekretariat tylko to, co zostało mu wyraźnie udostępnione; nauczyciele tylko swoje klasy i przedmioty; rodzice tylko własne dzieci. Powód choroby mogą odczytać wyłącznie dyrekcja szkoły, sekretariat i wychowawca, a każdy odczyt jest rejestrowany.
- Rozdzielenie szkół: wszystkie dane należą do dokładnie jednej szkoły; każde zapytanie jest ograniczone do tej szkoły.
- Szyfrowanie w aplikacji (libsodium; XSalsa20-Poly1305 dla pól, XChaCha20-Poly1305 dla plików) dla powodów choroby, wartości ocen i komentarzy, tekstów świadectw, wpisów w dzienniku lekcyjnym dotyczących uczniów, wiadomości i wszystkich przesłanych plików. Klucz jest przechowywany wyłącznie w konfiguracji serwera; dostawca przestrzeni dyskowej na pliki otrzymuje wyłącznie szyfrogram.
- Transmisja wyłącznie przez HTTPS z HSTS; pliki cookie sesji tylko przez HTTPS i nieodczytywalne przez skrypty.
- W obszarach szkoły Content Security Policy dopuszcza wyłącznie skrypty samej platformy; przeglądarka nie wykonuje wstrzykniętego kodu, a żadna inna witryna nie może osadzić tych obszarów.
- Hasła wyłącznie jako skrót (bcrypt lub Argon2); sesje są kończone po zmianie hasła; linki do resetu hasła są ważne 24 godziny i można ich użyć tylko raz.
- Ochrona przed atakami polegającymi na zgadywaniu: najwyżej pięć kolejnych prób logowania oraz zagadka obliczeniowa (ALTCHA) bez dostawcy zewnętrznego.
- Drugi składnik uwierzytelniania (TOTP) obowiązkowy dla sekretariatu i organu prowadzącego, dostępny dla dyrekcji szkoły, a ponadto klucze dostępu (passkeys). Nauczyciele i rodzice również mogą włączyć drugi składnik; szkoła może go wymagać od grona pedagogicznego. Szkoły mogą skonfigurować logowanie szkolne (OIDC, na przykład Microsoft Entra, Google lub logowanie kraju związkowego) i korzystać z jego uwierzytelniania wieloskładnikowego.
- Pliki są przechowywane w prywatnej przestrzeni dyskowej bez dostępu publicznego i są dostarczane wyłącznie przez aplikację po sprawdzeniu uprawnień.
- Logi aplikacji może odczytywać wyłącznie operator; filtr usuwa adresy, parametry, sekrety i tokeny, zanim cokolwiek zostanie zapisane.
- Dane dostępowe serwera są przechowywane wyłącznie w chronionym pliku konfiguracyjnym; środowiska deweloperskie i testowe nie mają dostępu do produkcyjnej przestrzeni dyskowej.
- Operator uzyskuje dostęp do danych szkoły tylko wtedy, gdy wymaga tego działanie systemu, usuwanie usterek albo prośba szkoły; operator jest zobowiązany do zachowania tajemnicy na podstawie § 203 StGB (niemiecki Kodeks karny). Jeśli w tym celu loguje się jako osoba ze szkoły za pomocą funkcji „Przełącz użytkownika”, jego działania pojawiają się w dzienniku zdarzeń szkoły jako „Operator (SavePaperwork)” wraz z jego nazwiskiem, a nie jako działania tej osoby.

5. Brak możliwości powiązania (ograniczenie celu)

- Dane są przetwarzane wyłącznie na rzecz szkoły: bez reklam, bez profilowania, bez ujawniania, bez trenowania modeli AI; w produkcie szkolnym nie są zintegrowane żadne usługi AI.
- Sieć szkół niczego nie udostępnia, dopóki każda szkoła nie przystąpi i nie wyrazi zgody dla każdego obszaru (pula zastępstw, kursy, materiały); szkoła zgłaszająca zapytanie widzi dane kontaktowe nauczyciela zastępującego dopiero po ich zwolnieniu. Opuszczenie sieci natychmiast blokuje dostęp.
- Dane produkcyjne szkół nigdy nie są kopiowane do środowisk deweloperskich ani testowych; tam operator pracuje na fikcyjnych danych przykładowych.

6. Przejrzystość

- W dzienniku zdarzeń dyrekcja szkoły widzi, kto zmienił które dane i kto otworzył które listy zawierające dane wrażliwe.
- Umowa, środki, podmioty podprzetwarzające, okresy przechowywania w poszczególnych krajach związkowych, wzory oceny skutków i rejestru czynności przetwarzania oraz informacje dla rodziców, pracowników i uczniów są publicznie dostępne.
- Nowe podmioty podprzetwarzające są ogłaszane z 30-dniowym wyprzedzeniem.

7. Możliwość interwencji

- Dostęp do danych i ich przenoszenie: eksport wszystkich danych ucznia lub rodzica jednym kliknięciem; eksport całej szkoły w każdej chwili.
- Sprostowanie, usunięcie i ograniczenie przetwarzania szkoła przeprowadza samodzielnie w aplikacji.
- Szkoła samodzielnie określa okresy przechowywania, obszary, pytanie o powód choroby i widoczność dla rodziców; link klasy można w każdej chwili odnowić lub wyłączyć.
- Zgłaszanie naruszeń ochrony danych szkole bez zbędnej zwłoki, co do zasady w ciągu 24 godzin.

8. Organizacja

- SavePaperwork jest jednoosobową działalnością; właściciel osobiście rozwija i prowadzi platformę. Inne osoby uzyskują dostęp dopiero po zobowiązaniu do poufności i do przestrzegania § 203 StGB.
- Nowe wersje wdraża wyłącznie właściciel, przez własne szyfrowane połączenie z serwerem.
- Obecnie nie wyznaczono inspektora ochrony danych; osobą kontaktową jest właściciel.
- Środki te są weryfikowane przy każdej istotnej zmianie platformy i co najmniej raz w roku.