Technische en organisatorische maatregelen (TOM's)

Versie van 12 november 2026 · Vertaling ter informatie. De Duitse versie is bindend.

Voorafgaande opmerking

De maatregelen zijn gestructureerd volgens de beschermingsdoelen van het Standaard-Datenschutzmodell van de Duitse toezichthoudende autoriteiten voor gegevensbescherming. SchuleVernetzt wordt door SavePaperwork ontwikkeld en geëxploiteerd als eenmanszaak.

1. Minimale gegevensverwerking

- Leerlingen hebben geen account. Alleen hun voornaam, achternaam en klas worden bewaard; geen geboortedatum, geen adres, geen telefoonnummer, geen foto.
- Naar een ziekteoorzaak wordt alleen gevraagd als de school dit inschakelt; de vraag staat standaard uit. Bij afwezigheidsmeldingen van leerkrachten wordt nooit een reden opgeslagen.
- Scholen kunnen het uploaden van doktersbriefjes uitschakelen; voor scholen in Noordrijn-Westfalen, Brandenburg en Berlijn staat het standaard uit.
- Meldingen bevatten zo weinig mogelijk: een berichtmelding noemt alleen de afzender, niet het onderwerp of de tekst; een herinnering aan een doktersbriefje op het vergrendelscherm noemt geen kind.
- Het account van het schoolbestuur (Schulträger) ziet alleen schoolnamen en kerncijfers, geen personen.
- De klaslink en het foyerscherm tonen geen namen van leerlingen en geen afwezige leerkrachten.
- Wissing per soort gegevens volgens de termijnen van de deelstaat, zodra de schoolleiding deze heeft bevestigd.
- Vermeldingen van leestoegang in het auditlog worden na 90 dagen gewist (behalve bewijzen van afgehandelde inzageverzoeken), applicatielogs na 14 dagen; het auditlog van de school slaat geen IP-adressen op.
- De hostingaanbieder bewaart toegangslogs met het volledige IP-adres tot 90 dagen en foutlogs tot 7 dagen, om storingen te onderzoeken en misbruik af te weren.
- Op de pagina’s van de school draaien geen analyse- of trackingdiensten en geen lettertypen van derden, ook niet in de e-mails van de school.

2. Beschikbaarheid

- Exploitatie in een ISO 27001-gecertificeerd datacenter in Frankfurt am Main (volgens de hostingaanbieder).
- Dagelijkse back-up door de hostingaanbieder, AES-256-versleuteld, in een apart datacenter in Helsinki, 90 dagen bewaard.
- Nieuwe versies worden atomair omgeschakeld; een terugkeer naar de vorige versie is op elk moment mogelijk. Wijzigingen aan het databaseschema worden nooit automatisch doorgevoerd.
- Automatische bewaking elke vijf minuten (database, achtergrondtaken, opeenhopingen van fouten) met meldingen op de telefoon van de exploitant.
- Het klassenboek kan bij een netwerkstoring gewoon worden bijgehouden; vermeldingen worden verzonden zodra het apparaat weer online is.
- De school kan op elk moment zelf een volledige export van alle gegevens downloaden, ook na het einde van het contract (exportgarantie).
- Het streven is een beschikbaarheid van 99,5 % als jaargemiddelde, aangekondigd onderhoud niet meegerekend.

3. Integriteit

- Versleutelde inhoud gebruikt geauthenticeerde versleuteling; elke wijziging wordt bij het lezen opgemerkt en nooit stilzwijgend geaccepteerd.

- Het auditlog legt vast wie een gegeven wanneer heeft aangemaakt, gewijzigd of verwijderd, met de oude en de nieuwe waarde; gevoelige waarden worden daarin onleesbaar gemaakt.
- Formulieren zijn beschermd tegen cross-site request forgery; invoer wordt op de server gevalideerd.
- Geüploade bestanden worden gecontroleerd op type en inhoud (PDF, JPG, PNG, WebP, DOCX; maximaal 10 MB; geen dubbele extensies) en onder een willekeurige naam opgeslagen.
- Elke wijziging van de code doorloopt geautomatiseerde tests, inclusief tests van de scheiding tussen scholen.

4. Vertrouwelijkheid

- Rollen en rechten: de schoolleiding ziet alles; het secretariaat alleen wat uitdrukkelijk voor hem is vrijgegeven; leerkrachten alleen hun klassen en vakken; ouders alleen hun eigen kinderen. Alleen de schoolleiding, het secretariaat en de mentor kunnen de ziekteoorzaak lezen, en elke leestoegang daartoe wordt gelogd.
- Scheiding van scholen: alle gegevens behoren tot precies één school; elke zoekopdracht is tot die school beperkt.
- Versleuteling in de applicatie (libsodium; XSalsa20-Poly1305 voor velden, XChaCha20-Poly1305 voor bestanden) voor ziekteoorzaken, cijferwaarden en opmerkingen, rapporttekst, vermeldingen in het klassenboek over leerlingen, berichten en alle geüploade bestanden. De sleutel staat alleen in de serverconfiguratie; de aanbieder van de bestandsopslag ontvangt uitsluitend versleutelde gegevens.
- Verzending uitsluitend via HTTPS met HSTS; sessiecookies alleen via HTTPS en niet leesbaar voor scripts.
- In de omgevingen van de school staat een Content Security Policy alleen de eigen scripts van het platform toe; geïnjecteerde code wordt door de browser niet uitgevoerd en geen andere site kan deze omgevingen insluiten.
- Wachtwoorden alleen als hash (bcrypt of Argon2); sessies worden beëindigd wanneer een wachtwoord wordt gewijzigd; links voor het opnieuw instellen van het wachtwoord zijn 24 uur geldig en kunnen maar één keer worden gebruikt.
- Bescherming tegen raadpogingen: maximaal vijf opeenvolgende inlogpogingen, plus een rekenpuzzel (ALTCHA) zonder externe aanbieder.
- Tweede factor (TOTP) verplicht voor het secretariaat en het schoolbestuur, beschikbaar voor de schoolleiding, plus passkeys. Leerkrachten en ouders kunnen de tweede factor ook inschakelen; de school kan hem voor het lerarenteam verplicht stellen. Scholen kunnen de schoolinlog (OIDC, bijvoorbeeld Microsoft Entra, Google of een inlog van een deelstaat) instellen en de multifactorauthenticatie daarvan gebruiken.
- Bestanden worden bewaard in privéopslag zonder openbare toegang en uitsluitend via de applicatie afgeleverd na een rechtencontrole.
- Applicatielogs kunnen alleen door de exploitant worden gelezen; een filter verwijdert adressen, parameters, geheimen en tokens voordat er iets wordt weggeschreven.
- De toegangsgegevens van de server worden alleen bewaard in een beschermd configuratiebestand; ontwikkel- en testomgevingen kunnen de productieopslag niet bereiken.
- De exploitant raadpleegt de gegevens van een school alleen als exploitatie, het oplossen van storingen of een verzoek van de school dat vereist; de exploitant is gebonden aan geheimhouding volgens § 203 StGB (Duits wetboek van strafrecht). Meldt de exploitant zich daarvoor via de functie “Van gebruiker wisselen” aan als iemand van de school, dan verschijnen diens handelingen in het auditlog van de school als “Exploitant (SavePaperwork)” met diens naam, niet als handelingen van die persoon.

5. Niet-koppelbaarheid (doelbinding)

- De gegevens worden uitsluitend voor de school verwerkt: geen reclame, geen profilering, geen verstrekking, geen training van AI-modellen; in het schoolproduct zijn geen AI-diensten geïntegreerd.
- Een schoolnetwerk deelt niets totdat elke school zich aansluit en per gedeelte toestemming geeft (vervangingspool, cursussen, materialen); de aanvragende school ziet de contactgegevens van een

invalleerkracht pas nadat ze zijn vrijgegeven. Het verlaten van het netwerk blokkeert de toegang onmiddellijk.
- Productiegegevens van scholen worden nooit gekopieerd naar ontwikkel- of testomgevingen; daar werkt de exploitant met fictieve voorbeeldgegevens.

6. Transparantie

- In het auditlog ziet de schoolleiding wie welke gegevens heeft gewijzigd en wie welke lijsten met gevoelige gegevens heeft geopend.
- De overeenkomst, de maatregelen, de subverwerkers, de bewaartermijnen per deelstaat, sjablonen voor de effectbeoordeling en het register van verwerkingsactiviteiten, en informatieverklaringen voor ouders, medewerkers en leerlingen zijn openbaar beschikbaar.
- Nieuwe subverwerkers worden 30 dagen van tevoren aangekondigd.

7. Ingrijpbaarheid

- Inzage en gegevensoverdraagbaarheid: export van alle gegevens van een leerling of een ouder met één klik; export van de hele school op elk moment.
- De school voert rectificatie, wissing en beperking zelf uit in de applicatie.
- De school bepaalt zelf bewaartermijnen, gedeelten, de vraag naar de ziekteoorzaak en de zichtbaarheid voor ouders; een klaslink kan op elk moment worden vernieuwd of uitgeschakeld.
- Melding van inbreuken op persoonsgegevens aan de school onverwijld, in de regel binnen 24 uur.

8. Organisatie

- SavePaperwork is een eenmanszaak; de eigenaar ontwikkelt en exploiteert het platform persoonlijk. Andere personen krijgen pas toegang nadat zij tot vertrouwelijkheid en tot § 203 StGB zijn verplicht.
- Nieuwe versies worden alleen door de eigenaar uitgerold, via zijn eigen versleutelde verbinding met de server.
- Er is momenteel geen functionaris voor gegevensbescherming aangewezen; de contactpersoon is de eigenaar.
- Deze maatregelen worden bij elke wezenlijke wijziging van het platform en minstens eenmaal per jaar getoetst.