Mesures techniques et organisationnelles (MTO)

Version du 12 novembre 2026 · Traduction à titre informatif. Seule la version allemande fait foi.

Remarque préliminaire

Les mesures sont structurées selon les objectifs de protection du modèle standard de protection des données (Standard-Datenschutzmodell) des autorités allemandes de contrôle de la protection des données. SchuleVernetzt est développé et exploité par SavePaperwork en tant qu'entreprise unipersonnelle.

1. Minimisation des données

- Les élèves n'ont pas de compte. Seuls leur prénom, leur nom et leur classe sont conservés ; ni date de naissance, ni adresse, ni numéro de téléphone, ni photo.
- Un motif de maladie n'est demandé que si l'école active cette option ; la question est désactivée par défaut. Pour les signalements d'absence des enseignants, aucun motif n'est jamais enregistré.
- Les écoles peuvent désactiver le téléversement de certificats médicaux ; pour les écoles de Rhénanie-du-Nord-Westphalie, du Brandebourg et de Berlin, il est désactivé par défaut.
- Les notifications contiennent le strict minimum : une notification de message ne nomme que l'expéditeur, ni l'objet ni le texte ; un rappel de certificat médical sur l'écran de verrouillage ne nomme aucun enfant.
- Le compte de l'organisme gestionnaire (Schulträger) ne voit que les noms des écoles et des chiffres clés, aucune personne.
- Le lien de classe et l'écran du hall n'affichent ni noms d'élèves ni enseignants absents.
- Suppression par type de données selon les durées du Land, une fois que la direction de l'école les a confirmées.
- Les entrées d'accès en lecture du journal d'audit sont supprimées après 90 jours (à l'exception des preuves de demandes d'accès traitées), les journaux de l'application après 14 jours ; le journal d'audit de l'école n'enregistre aucune adresse IP.
- L'hébergeur conserve les journaux d'accès avec l'adresse IP complète jusqu'à 90 jours et les journaux d'erreurs jusqu'à 7 jours, afin d'analyser les incidents et de parer aux abus.
- Aucun service d'analyse ou de suivi et aucune police de caractères tierce ne s'exécute sur les pages de l'école, ni dans les e-mails de l'école.

2. Disponibilité

- Exploitation dans un centre de données certifié ISO 27001 à Francfort-sur-le-Main (selon l'hébergeur).
- Sauvegarde quotidienne par l'hébergeur, chiffrée en AES-256, dans un centre de données distinct à Helsinki, conservée pendant 90 jours.
- Les nouvelles versions sont basculées de manière atomique ; un retour à la version précédente est possible à tout moment. Les modifications du schéma de la base de données ne sont jamais appliquées automatiquement.
- Surveillance automatique toutes les cinq minutes (base de données, tâches en arrière-plan, accumulations d'erreurs) avec alertes sur le téléphone de l'exploitant.
- Le cahier de classe peut continuer à être tenu pendant une coupure de réseau ; les entrées sont transmises dès que l'appareil est de nouveau en ligne.
- L'école peut elle-même télécharger à tout moment un export complet de toutes les données, même après la fin du contrat (garantie d'export).
- L'objectif est une disponibilité de 99,5 % en moyenne annuelle, hors maintenance annoncée.

3. Intégrité

- Les contenus chiffrés utilisent un chiffrement authentifié ; toute altération est détectée à la lecture et jamais acceptée silencieusement.

- Le journal d'audit enregistre qui a créé, modifié ou supprimé un enregistrement et quand, avec l'ancienne et la nouvelle valeur ; les valeurs sensibles y sont masquées.
- Les formulaires sont protégés contre la falsification de requêtes intersites ; les saisies sont validées côté serveur.
- Les fichiers téléversés sont contrôlés quant au type et au contenu (PDF, JPG, PNG, WebP, DOCX ; 10 Mo au maximum ; pas de double extension) et enregistrés sous un nom aléatoire.
- Chaque modification du code passe par des tests automatisés, y compris des tests de la séparation entre les écoles.

4. Confidentialité

- Rôles et autorisations : la direction de l'école voit tout ; le secrétariat uniquement ce qui lui a été expressément ouvert ; les enseignants uniquement leurs classes et leurs matières ; les parents uniquement leurs propres enfants. Seuls la direction de l'école, le secrétariat et le professeur principal peuvent lire le motif de maladie, et chaque accès en lecture à celui-ci est journalisé.
- Séparation des écoles : toutes les données appartiennent à exactement une école ; chaque requête est limitée à cette école.
- Chiffrement dans l'application (libsodium ; XSalsa20-Poly1305 pour les champs, XChaCha20-Poly1305 pour les fichiers) pour les motifs de maladie, les valeurs et commentaires de notes, les textes de bulletins, les entrées du cahier de classe concernant les élèves, les messages et tous les fichiers téléversés. La clé n'est conservée que dans la configuration du serveur ; le prestataire de stockage des fichiers ne reçoit que du texte chiffré.
- Transmission exclusivement via HTTPS avec HSTS ; cookies de session uniquement via HTTPS et illisibles par des scripts.
- Dans les espaces de l'école, une Content Security Policy n'autorise que les scripts propres à la plateforme ; le navigateur n'exécute pas de code injecté et aucun autre site ne peut intégrer ces espaces.
- Mots de passe uniquement sous forme de hachage (bcrypt ou Argon2) ; les sessions sont terminées lors d'un changement de mot de passe ; les liens de réinitialisation du mot de passe sont valables 24 heures et ne peuvent être utilisés qu'une seule fois.
- Protection contre les attaques par essais successifs : cinq tentatives de connexion consécutives au maximum, plus une énigme de calcul (ALTCHA) sans prestataire tiers.
- Second facteur (TOTP) obligatoire pour le secrétariat et l'organisme gestionnaire, disponible pour la direction de l'école, ainsi que des clés d'accès (passkeys). Les enseignants et les parents peuvent eux aussi activer le second facteur ; l'école peut l'exiger de son équipe enseignante. Les écoles peuvent mettre en place la connexion de l'école (OIDC, par exemple Microsoft Entra, Google ou une connexion d'un Land) et utiliser son authentification multifacteur.
- Les fichiers sont conservés dans un stockage privé sans accès public et ne sont remis que par l'application après vérification des autorisations.
- Les journaux de l'application ne peuvent être lus que par l'exploitant ; un filtre supprime les adresses, paramètres, secrets et jetons avant toute écriture.
- Les identifiants d'accès du serveur ne sont conservés que dans un fichier de configuration protégé ; les environnements de développement et de test ne peuvent pas atteindre le stockage de production.
- L'exploitant n'accède aux données d'une école que lorsque l'exploitation, le dépannage ou une demande de l'école l'exige ; l'exploitant est tenu au secret en vertu du § 203 StGB (Code pénal allemand). S'il se connecte à cette fin en tant que personne de l'école via la fonction « Changer d'utilisateur », ses actions apparaissent dans le journal d'audit de l'école sous « Exploitant (SavePaperwork) » avec son nom, et non comme des actions de cette personne.

5. Non-chaînage (limitation des finalités)

- Les données ne sont traitées que pour l'école : ni publicité, ni profilage, ni communication à des tiers, ni entraînement de modèles d'IA ; aucun service d'IA n'est intégré dans le produit scolaire.

- Un réseau d'écoles ne partage rien tant que chaque école n'a pas adhéré et consenti pour chaque domaine (pool de remplacements, cours, supports) ; l'école demandeuse ne voit les coordonnées d'un enseignant remplaçant qu'après leur validation. Quitter le réseau bloque immédiatement l'accès.
- Les données de production des écoles ne sont jamais copiées dans des environnements de développement ou de test ; l'exploitant y travaille avec des données d'exemple fictives.

6. Transparence

- Dans le journal d'audit, la direction de l'école voit qui a modifié quelles données et qui a ouvert quelles listes contenant des données sensibles.
- Le contrat, les mesures, les sous-traitants ultérieurs, les durées de conservation par Land, les modèles d'analyse d'impact et de registre des activités de traitement, ainsi que les notices d'information pour les parents, le personnel et les élèves sont accessibles publiquement.
- Les nouveaux sous-traitants ultérieurs sont annoncés 30 jours à l'avance.

7. Possibilité d'intervention

- Accès et portabilité des données : export de toutes les données d'un élève ou d'un parent en un clic ; export de toute l'école à tout moment.
- L'école effectue elle-même la rectification, l'effacement et la limitation dans l'application.
- L'école détermine elle-même les durées de conservation, les domaines, la question du motif de maladie et la visibilité pour les parents ; un lien de classe peut être renouvelé ou désactivé à tout moment.
- Notification des violations de données à l'école dans les meilleurs délais, en règle générale dans les 24 heures.

8. Organisation

- SavePaperwork est une entreprise unipersonnelle ; le propriétaire développe et exploite lui-même la plateforme. D'autres personnes ne reçoivent un accès qu'après avoir été tenues à la confidentialité et au § 203 StGB.
- Les nouvelles versions ne sont déployées que par le propriétaire, via sa propre connexion chiffrée au serveur.
- Aucun délégué à la protection des données n'est actuellement désigné ; la personne de contact est le propriétaire.
- Ces mesures sont réexaminées à chaque modification importante de la plateforme et au moins une fois par an.