Medidas técnicas y organizativas

Versión del 12 de noviembre de 2026 · Traducción a título informativo. La versión alemana es la vinculante.

Nota preliminar

Las medidas están estructuradas según los objetivos de protección del Modelo Estándar de Protección de Datos de las autoridades alemanas de control de protección de datos. SchuleVernetzt es desarrollado y operado por SavePaperwork como empresa unipersonal.

1. Minimización de datos

- El alumnado no tiene cuenta. Solo se conservan su nombre, apellidos y clase; no se guarda fecha de nacimiento, dirección, número de teléfono ni foto.
- El motivo de una enfermedad solo se pregunta si la escuela lo activa; la pregunta está desactivada por defecto. En las comunicaciones de ausencia del profesorado nunca se guarda un motivo.
- Las escuelas pueden desactivar la subida de justificantes médicos; para las escuelas de Renania del Norte-Westfalia, Brandeburgo y Berlín está desactivada por defecto.
- Las notificaciones contienen lo mínimo posible: el aviso de un mensaje nombra solo al remitente, no el asunto ni el texto; el recordatorio de un justificante médico en la pantalla de bloqueo no nombra a ningún niño ni niña.
- La cuenta de la entidad titular de la escuela (Schulträger) ve solo nombres de escuelas y cifras clave, ninguna persona.
- El enlace de clase y la pantalla del vestíbulo no muestran nombres del alumnado ni del profesorado ausente.
- Supresión por tipo de dato según los plazos del estado federado, una vez que la dirección de la escuela los ha confirmado.
- Las entradas de acceso de lectura en el registro de auditoría se suprimen a los 90 días (salvo las constancias de solicitudes de acceso atendidas) y los registros de la aplicación a los 14 días; el registro de auditoría de la escuela no guarda direcciones IP.
- El proveedor de alojamiento conserva los registros de acceso con la dirección IP completa hasta 90 días y los registros de errores hasta 7 días, para investigar incidencias y repeler usos abusivos.
- En las páginas de la escuela no se ejecutan servicios de análisis ni de seguimiento ni fuentes tipográficas de terceros, y tampoco en los correos electrónicos de la escuela.

2. Disponibilidad

- Operación en un centro de datos certificado según ISO 27001 en Fráncfort del Meno (según el proveedor de alojamiento).
- Copia de seguridad diaria por el proveedor de alojamiento, cifrada con AES-256, en un centro de datos independiente en Helsinki, conservada durante 90 días.
- Las nuevas versiones se activan de forma atómica; en cualquier momento es posible volver a la versión anterior. Los cambios en el esquema de la base de datos nunca se aplican automáticamente.
- Supervisión automática cada cinco minutos (base de datos, tareas en segundo plano, acumulaciones de errores) con alertas al teléfono del operador.
- El diario de clase puede seguir llevándose durante una caída de la red; las entradas se envían en cuanto el dispositivo vuelve a estar en línea.
- La escuela puede descargar por sí misma en cualquier momento una exportación completa de todos los datos, incluso después de terminar el contrato (garantía de exportación).
- El objetivo es una disponibilidad del 99,5 % como promedio anual, sin contar los mantenimientos anunciados.

3. Integridad

- Los contenidos cifrados usan cifrado autenticado; cualquier alteración se detecta al leer y nunca se acepta en silencio.
- El registro de auditoría anota quién creó, modificó o eliminó un registro y cuándo, con el valor antiguo y el nuevo; los valores sensibles aparecen ocultados.
- Los formularios están protegidos contra la falsificación de solicitudes entre sitios (CSRF); las entradas se validan en el servidor.
- Los archivos subidos se comprueban en cuanto a tipo y contenido (PDF, JPG, PNG, WebP, DOCX; máximo 10 MB; sin dobles extensiones) y se guardan con un nombre aleatorio.
- Cada cambio en el código pasa por pruebas automatizadas, incluidas pruebas de la separación entre escuelas.

4. Confidencialidad

- Roles y permisos: la dirección de la escuela lo ve todo; la secretaría solo lo que se le ha habilitado expresamente; el profesorado solo sus clases y asignaturas; las familias solo a sus propios hijos. Solo la dirección de la escuela, la secretaría y el tutor o la tutora de la clase pueden leer el motivo de una enfermedad, y cada acceso de lectura a él queda registrado.
- Separación de escuelas: todos los datos pertenecen a exactamente una escuela; cada consulta se limita a esa escuela.
- Cifrado en la aplicación (libsodium; XSalsa20-Poly1305 para campos, XChaCha20-Poly1305 para archivos) para los motivos de enfermedad, las calificaciones y sus comentarios, los textos de los boletines, las entradas del diario de clase sobre el alumnado, los mensajes y todos los archivos subidos. La clave se guarda solo en la configuración del servidor; el proveedor de almacenamiento de archivos recibe únicamente texto cifrado.
- Transmisión exclusivamente mediante HTTPS con HSTS; las cookies de sesión solo por HTTPS y no legibles por scripts.
- En las áreas de la escuela, una Content Security Policy solo permite los scripts propios de la plataforma; el navegador no ejecuta código inyectado y ningún otro sitio puede incrustar estas áreas.
- Contraseñas solo como hash (bcrypt o Argon2); las sesiones se cierran al cambiar la contraseña; los enlaces de restablecimiento de contraseña son válidos 24 horas y solo pueden usarse una vez.
- Protección contra ataques de adivinación: como máximo cinco intentos de inicio de sesión consecutivos, además de un problema de cálculo (ALTCHA) sin proveedor externo.
- Segundo factor (TOTP) obligatorio para la secretaría y la entidad titular de la escuela, disponible para la dirección de la escuela, además de passkeys. El profesorado y las familias también pueden activar el segundo factor; la escuela puede exigirlo a su profesorado. Las escuelas pueden configurar el inicio de sesión de la escuela (OIDC, por ejemplo Microsoft Entra, Google o un acceso de un estado federado) y usar su autenticación multifactor.
- Los archivos se guardan en un almacenamiento privado sin acceso público y solo se entregan a través de la aplicación tras una comprobación de permisos.
- Los registros de la aplicación solo puede leerlos el operador; un filtro elimina direcciones, parámetros, secretos y tokens antes de escribir nada.
- Las credenciales de acceso del servidor se guardan solo en un archivo de configuración protegido; los entornos de desarrollo y de prueba no pueden acceder al almacenamiento de producción.
- El operador accede a los datos de una escuela solo cuando lo exigen la operación, la resolución de fallos o una petición de la escuela; el operador está sujeto al deber de secreto conforme al § 203 StGB (Código Penal alemán). Si para ello inicia sesión como una persona de la escuela mediante la función «Cambiar de usuario», sus acciones aparecen en el registro de auditoría de la escuela como «Operador (SavePaperwork)» con su nombre, no como acciones de esa persona.

5. No vinculación (limitación de la finalidad)

- Los datos se tratan solo para la escuela: sin publicidad, sin elaboración de perfiles, sin cesión, sin entrenamiento de modelos de IA; en el producto escolar no hay integrados servicios de IA.
- Una red de escuelas no comparte nada hasta que cada escuela se une y da su consentimiento para cada ámbito (bolsa de sustituciones, cursos, materiales); la escuela solicitante ve los datos de contacto de un docente de sustitución solo después de que se hayan habilitado. Salir de la red bloquea el acceso de inmediato.
- Los datos de producción de las escuelas nunca se copian a entornos de desarrollo o de prueba; allí el operador trabaja con datos de muestra ficticios.

6. Transparencia

- En el registro de auditoría, la dirección de la escuela ve quién modificó qué datos y quién abrió qué listas con datos sensibles.
- El contrato, las medidas, los subencargados, los plazos de conservación por estado federado, las plantillas para la evaluación de impacto y el registro de actividades de tratamiento, y los avisos informativos para familias, personal y alumnado están disponibles públicamente.
- Los nuevos subencargados se anuncian con 30 días de antelación.

7. Intervenibilidad

- Acceso y portabilidad de datos: exportación de todos los datos de un alumno o de un progenitor con un clic; exportación de toda la escuela en cualquier momento.
- La propia escuela lleva a cabo en la aplicación la rectificación, la supresión y la limitación.
- La propia escuela determina los plazos de conservación, los ámbitos, la pregunta sobre el motivo de la enfermedad y la visibilidad para las familias; un enlace de clase puede renovarse o desactivarse en cualquier momento.
- Notificación de las violaciones de la seguridad de los datos a la escuela sin dilación indebida, por regla general en un plazo de 24 horas.

8. Organización

- SavePaperwork es una empresa unipersonal; el propietario desarrolla y opera la plataforma personalmente. Otras personas solo reciben acceso después de quedar obligadas a la confidencialidad y al § 203 StGB.
- Las nuevas versiones las despliega únicamente el propietario, a través de su propia conexión cifrada con el servidor.
- Actualmente no se ha designado ningún delegado de protección de datos; la persona de contacto es el propietario.
- Estas medidas se revisan con cada cambio sustancial de la plataforma y al menos una vez al año.