Technische und organisatorische Maßnahmen (TOM)

Fassung vom 12.11.2026

Vorbemerkung

Die Maßnahmen sind nach den Gewährleistungszielen des Standard-Datenschutzmodells der deutschen Datenschutzaufsichtsbehörden gegliedert. SchuleVernetzt wird von SavePaperwork als Ein-Personen-Betrieb entwickelt und betrieben.

1. Datenminimierung

- Schülerinnen und Schüler haben kein Konto. Von ihnen werden nur Vorname, Nachname und Klasse geführt; kein Geburtsdatum, keine Anschrift, keine Telefonnummer, kein Foto.
- Ein Krankheitsgrund wird nur abgefragt, wenn die Schule das einschaltet; ab Werk ist die Abfrage aus. Bei Ausfallmeldungen von Lehrkräften wird nie ein Grund gespeichert.
- Schulen können den Attest-Upload abschalten; für Schulen in Nordrhein-Westfalen, Brandenburg und Berlin ist er voreingestellt aus.
- Benachrichtigungen enthalten so wenig wie möglich: eine Nachricht nennt nur den Absender, nicht Betreff oder Text; eine Attest-Erinnerung auf dem Sperrbildschirm nennt kein Kind.
- Das Trägerkonto sieht nur Schulnamen und Kennzahlen, keine Personen.
- Klassenlink und Foyer-Bildschirm zeigen keine Namen von Schülerinnen und Schülern und keine abwesenden Lehrkräfte.
- Fristenlöschung je Datenart nach den Fristen des Bundeslandes, nachdem die Schulleitung sie bestätigt hat.
- Lesezugriffe im Protokoll werden nach 90 Tagen gelöscht (Nachweise erfüllter Auskunftsanfragen ausgenommen), Anwendungsprotokolle nach 14 Tagen; das Protokoll der Schule speichert keine IP-Adressen.
- Der Hoster speichert Zugriffsprotokolle mit vollständiger IP-Adresse bis zu 90 Tage und Fehlerprotokolle bis zu 7 Tage, um Störungen zu untersuchen und Missbrauch abzuwehren.
- Auf den Seiten der Schule laufen keine Analyse- oder Tracking-Dienste und keine fremden Schriften, auch nicht in den E-Mails der Schule.

2. Verfügbarkeit

- Betrieb in einem nach ISO 27001 zertifizierten Rechenzentrum in Frankfurt am Main (Angabe des Hosters).
- Tägliche Sicherung durch den Hoster, AES-256-verschlüsselt in einem getrennten Rechenzentrum in Helsinki, 90 Tage aufbewahrt.
- Neue Versionen werden atomar umgeschaltet; ein Rückweg auf die vorige Version ist jederzeit möglich. Änderungen am Datenbankschema werden nie automatisch eingespielt.
- Automatische Überwachung alle fünf Minuten (Datenbank, Hintergrundaufgaben, Fehlerhäufung) mit Alarm auf das Telefon des Betreibers.
- Das Klassenbuch lässt sich bei Netzausfall weiterführen; Einträge werden nachgereicht, sobald das Gerät wieder online ist.
- Die Schule kann jederzeit selbst einen vollständigen Export aller Daten ziehen, auch nach Vertragsende (Exportgarantie).
- Ziel ist eine Verfügbarkeit von 99,5 % im Jahresmittel außerhalb angekündigter Wartungen.

3. Integrität

- Verschlüsselte Inhalte sind authentifiziert verschlüsselt; eine Veränderung wird beim Lesen erkannt und nie stillschweigend akzeptiert.

- Das Protokoll hält fest, wer wann einen Datensatz angelegt, geändert oder gelöscht hat, mit altem und neuem Wert; sensible Werte werden darin geschwärzt.
- Formulare sind gegen Cross-Site-Request-Forgery geschützt; Eingaben werden serverseitig geprüft.
- Hochgeladene Dateien werden auf Typ und Inhalt geprüft (PDF, JPG, PNG, WebP, DOCX; höchstens 10 MB; keine doppelten Endungen) und unter einem zufälligen Namen gespeichert.
- Jede Änderung am Code durchläuft automatische Tests, darunter Tests der Trennung zwischen Schulen.

4. Vertraulichkeit

- Rollen und Rechte: Die Schulleitung sieht alles; das Sekretariat nur, was ihm ausdrücklich freigegeben ist; Lehrkräfte nur ihre Klassen und Fächer; Eltern nur ihre eigenen Kinder. Den Krankheitsgrund lesen nur Schulleitung, Sekretariat und die Klassenleitung, und jeder Lesezugriff darauf wird protokolliert.
- Trennung der Schulen: Alle Daten gehören genau einer Schule; jede Abfrage ist auf diese Schule begrenzt.
- Verschlüsselung in der Anwendung (libsodium; XSalsa20-Poly1305 für Felder, XChaCha20-Poly1305 für Dateien) für Krankheitsgründe, Notenwerte und -kommentare, Zeugnistexte, Klassenbuch-Einträge über Schülerinnen und Schüler, Nachrichten und alle hochgeladenen Dateien. Der Schlüssel liegt nur in der Server-Konfiguration; der Speicheranbieter für Dateien erhält nur Chiffretext.
- Übertragung ausschließlich per HTTPS mit HSTS; Sitzungs-Cookies nur über HTTPS, nicht für Skripte lesbar.
- In den Bereichen der Schule lässt eine Content-Security-Policy nur Skripte der Plattform selbst zu; eingeschleuster Code wird vom Browser nicht ausgeführt, und keine fremde Seite kann diese Bereiche einbetten.
- Passwörter nur als Hash (bcrypt bzw. Argon2); Sitzungen werden bei einer Passwortänderung beendet; Links zum Zurücksetzen gelten 24 Stunden und nur einmal.
- Schutz vor Rateversuchen: höchstens fünf Anmeldeversuche in Folge, dazu ein Rechenrätsel (ALTCHA) ohne Drittanbieter.
- Zweiter Faktor (TOTP) Pflicht für Sekretariat und Träger, verfügbar für die Schulleitung, dazu Passkeys. Lehrkräfte und Eltern können den zweiten Faktor ebenfalls einschalten; die Schule kann ihn für das Kollegium verlangen. Schulen können den Schul-Login (OIDC, etwa Microsoft Entra, Google oder einen Landes-Login) einrichten und dessen Mehr-Faktor-Anmeldung nutzen.
- Dateien liegen in einem privaten Speicher ohne öffentlichen Zugriff und werden nur über die Anwendung nach Rechteprüfung ausgeliefert.
- Anwendungsprotokolle sind nur für den Betreiber lesbar; ein Filter entfernt Adressen, Parameter, Geheimnisse und Token, bevor etwas geschrieben wird.
- Zugangsdaten des Servers liegen nur in einer geschützten Konfigurationsdatei; Entwicklungs- und Testumgebungen erreichen den Produktionsspeicher nicht.
- Der Betreiber greift auf Daten einer Schule nur zu, soweit Betrieb, Fehlerbehebung oder eine Anfrage der Schule es erfordern; er ist nach § 203 StGB zur Geheimhaltung verpflichtet. Meldet er sich dafür über die Funktion „Benutzer wechseln“ als Person der Schule an, erscheinen seine Handlungen im Protokoll der Schule als „Betreiber (SavePaperwork)“ mit seinem Namen, nicht als Handlungen dieser Person.

5. Nichtverkettung (Zweckbindung)

- Die Daten werden nur für die Schule verarbeitet: keine Werbung, keine Profilbildung, keine Weitergabe, kein Training von KI-Modellen; im Schulprodukt sind keine KI-Dienste eingebunden.
- Ein Schulverbund teilt nichts, bis jede Schule beitritt und je Bereich (Vertretungspool, Kurse, Material) zustimmt; Kontaktdaten einer Aushilfslehrkraft sieht die anfragende Schule erst nach Freigabe. Ein Austritt sperrt sofort.
- Produktionsdaten von Schulen werden nie in Entwicklungs- oder Testumgebungen kopiert; dort arbeitet der Betreiber mit erfundenen Beispieldaten.

6. Transparenz

- Die Schulleitung sieht im Protokoll, wer welche Daten geändert hat und wer welche Listen mit sensiblen Daten aufgerufen hat.
- Vertrag, Maßnahmen, Unterauftragnehmer, Fristen je Bundesland, Muster für Folgenabschätzung und Verarbeitungsverzeichnis sowie Informationstexte für Eltern, Personal und Schülerinnen und Schüler sind öffentlich abrufbar.
- Neue Unterauftragnehmer werden 30 Tage vorher angekündigt.

7. Intervenierbarkeit

- Auskunft und Datenübertragbarkeit: Export aller Daten einer Schülerin, eines Schülers oder eines Elternteils mit einem Klick; Export der ganzen Schule jederzeit.
- Berichtigung, Löschung und Einschränkung setzt die Schule selbst in der Anwendung um.
- Die Schule bestimmt Fristen, Bereiche, die Abfrage des Krankheitsgrundes und die Sichtbarkeit für Eltern selbst; ein Klassenlink lässt sich jederzeit erneuern oder abschalten.
- Meldung von Datenschutzverletzungen an die Schule unverzüglich, in der Regel binnen 24 Stunden.

8. Organisation

- SavePaperwork ist ein Ein-Personen-Betrieb; der Inhaber entwickelt und betreibt die Plattform selbst. Weitere Personen erhalten Zugang nur nach Verpflichtung auf Vertraulichkeit und § 203 StGB.
- Neue Versionen spielt nur der Inhaber aus seiner eigenen, verschlüsselten Verbindung zum Server ein.
- Ein Datenschutzbeauftragter ist derzeit nicht benannt; Ansprechpartner ist der Inhaber.
- Diese Maßnahmen werden bei jeder wesentlichen Änderung der Plattform und mindestens einmal im Jahr überprüft.