Datenschutz-Folgenabschätzung (Vorlage)

Fassung vom 18.11.2026

So nutzen Sie dieses Muster

Die Folgenabschätzung führt die Schule als Verantwortliche durch (Art. 35 DSGVO); SavePaperwork liefert als Auftragsverarbeiter die Angaben zur Plattform (Art. 28 Abs. 3 Buchst. f DSGVO). Alles, was die Plattform betrifft, ist vorausgefüllt. Felder in eckigen Klammern wie [Name der Schule] füllt die Schule aus; Bewertungen passt sie an ihre Lage an, vor allem an die Bereiche, die sie tatsächlich nutzt.

Das Muster ersetzt nicht die Beratung durch den Datenschutzbeauftragten der Schule. Zum Bearbeiten gibt es eine Word-Fassung.

1. Beschreibung der Verarbeitung

1.1 Verantwortliche und Beteiligte

Angabe	Eintrag
Verantwortliche	[Name und Anschrift der Schule], vertreten durch [Name der Schulleitung]
Bundesland und Schulform	[Bundesland], [Schulform], [Zahl der Schülerinnen und Schüler]
Datenschutzbeauftragte(r) der Schule	[Name, Kontakt]
Personalvertretung	[zuständiger Personalrat, etwa an der Schule oder beim Schulamt]
Auftragsverarbeiter	SavePaperwork, Inhaber Andreas Gerum, Höfatsstraße 16, 86163 Augsburg; support@schulevernetzt.org. Vertrag zur Auftragsverarbeitung abgeschlossen am [Datum].
Genutzte Bereiche	[Bereiche aus 1.3 übernehmen; nicht genutzte Bereiche streichen]
Erstellt von, am	[Name, Funktion], [Datum]

1.2 Gegenstand

SchuleVernetzt ist eine Schulplattform für Unterricht, Organisation und Kommunikation, die im Browser genutzt wird. Schülerinnen und Schüler haben kein eigenes Konto; sie sind nur Betroffene. Konten haben Schulleitung, Sekretariat, Lehrkräfte, Erziehungsberechtigte und, falls vorhanden, der Schulträger. Die Schule schaltet die Bereiche einzeln ein; verarbeitet werden nur die Daten der Bereiche, die sie nutzt. Im Schulprodukt sind keine KI-Dienste eingebunden, und auf den Seiten der Schule laufen keine Analyse- oder Tracking-Dienste.

1.3 Bereiche, Daten und Betroffene

Bereich	Daten	Betroffene	Schutzbedarf
Schülerliste und Klassen	Vorname, Nachname, Klasse, Zeitraum einer Attestpflicht; Zuordnung zu Erziehungsberechtigten. Kein Geburtsdatum, keine Anschrift, keine Telefonnummer, kein Foto.	Schülerinnen und Schüler	normal
Klassenbuch und Anwesenheit	Anwesenheit je Stunde (anwesend, fehlt, verspätet, entschuldigt), Stundenthema, Hausaufgabe; Einträge über ein Kind (Hausaufgabe vergessen, Material fehlt, Lob, Tadel, Sonstiges) mit Text, für Eltern nie	Schülerinnen und Schüler, Lehrkräfte	hoch (Verhalten von Kindern)

Bereich	Daten	Betroffene	Schutzbedarf
	sichtbar; Kurse mit Einschreibung und Kurs-Anwesenheit.		
Krankmeldungen	Zeitraum, Status, meldende Person, Zeitpunkt des Attest-Eingangs, hochgeladenes ärztliches Attest; Krankheitsgrund (Freitext) nur, wenn die Schule die Abfrage einschaltet.	Schülerinnen und Schüler, Erziehungsberechtigte	sehr hoch (Gesundheitsdaten von Kindern, Art. 9 DSGVO)
Noten und Zeugnisse	Fach, Notenwert, Datum, Gewichtung, Kommentar; Zeugnisse mit Fachnoten, Texten, Bemerkungen und Rückfragen; für Eltern nicht sichtbar.	Schülerinnen und Schüler, Lehrkräfte	hoch
Rundschreiben und Schwarzes Brett	Titel, Text, Übersetzungen, Anhänge, Empfängerkreis; je Empfänger Lesezeitpunkt, Bestätigung, Antwort und Antwortweg; Aushänge, Dokumente und Material mit Autor.	Erziehungsberechtigte, Lehrkräfte, Schulpersonal	normal
Nachrichten	Betreff, Text, Teilnehmende, Bezug zu einem Kind oder einer Klasse, Lesestand.	Erziehungsberechtigte, Lehrkräfte, Schülerinnen und Schüler (Bezug)	hoch (Freitext)
Stunden- und Vertretungsplan	Lehrkraft, Kürzel, Klasse, Fach, Raum, Zeit, Vertretung; keine Schülernamen. Ausfallmeldungen von Lehrkräften nur mit Zeitraum, nie mit Grund.	Lehrkräfte	normal
Sprechtag und Sprechstunde	Termin, Lehrkraft, Elternteil, Kind; bei öffentlicher Buchung ohne Konto Name, E-Mail und Notiz der buchenden Person.	Erziehungsberechtigte, buchende Personen, Lehrkräfte	normal
Konten und Benachrichtigungen	Name, E-Mail, Passwort nur als Hash, Rolle, Sprache, Einladungs- und Anmeldezeitpunkte, optional zweiter Faktor, Verknüpfung mit dem Schul-Login; Push-Abonnements.	Schulleitung, Sekretariat, Lehrkräfte, Erziehungsberechtigte, Trägerpersonal	normal
Protokoll	Wer wann welchen Datensatz angelegt, geändert oder gelöscht hat; tageweise zusammengefasste Lesezugriffe auf Listen mit sensiblen Daten; keine IP-Adressen.	alle Nutzerinnen und Nutzer, vor allem Beschäftigte	hoch (Beschäftigtendaten)
Schulverbund	Vertretungspool mit Name und Kontakt einer Aushilfslehrkraft nach Freigabe ihrer Schule; schulübergreifende Kurse mit Schülerinnen und Schülern einer Partnerschule; geteiltes Material.	Lehrkräfte, Schülerinnen und Schüler	normal
Trägerübersicht	Nur Schulnamen und Kennzahlen (Klassen, Schülerzahl, Fehlquote, Unterrichtsausfall); keine Personen.	—	gering

1.4 Empfänger und Zugriff

- **Innerhalb der Schule** nach Rollen: Die Schulleitung sieht alles; das Sekretariat nur, was ihm ausdrücklich freigegeben ist (Noten lesen, Zeugnisse drucken, Krankheitsgrund, Klassenbuch-Einträge lesen); Lehrkräfte nur ihre Klassen und Fächer. Den Krankheitsgrund lesen nur Schulleitung, Sekretariat und die Klassenleitung.
- **Erziehungsberechtigte** sehen nur ihre eigenen Kinder und weder Noten noch Zeugnisse.
- **Schulträger** sehen nur Schulnamen und Kennzahlen, keine Personen.

- **Ohne Anmeldung** zeigen Klassenlink und Foyer-Bildschirm nur Stundenplan, veröffentlichte Vertretungen, Hausaufgaben und schulweite Aushänge, keine Namen von Schülerinnen und Schülern und keine abwesenden Lehrkräfte.
- **Partnerschulen im Verbund** erhalten nur, was die Schule je Bereich freigibt.
- **Auftragsverarbeiter** SavePaperwork mit den Unterauftragnehmern nach Anlage 2: Hoster in Frankfurt am Main (Anwendung, Datenbank, E-Mail-Versand, Sicherung) und ein Speicheranbieter für Dateien, der nur Chiffretext erhält.
- **Weitere Empfänger** nach Anlage 3: der Push-Dienst des Browsers, wenn eine Person Push einschaltet (verschlüsselte Nachricht), die E-Mail-Anbieter der Empfängerinnen und Empfänger und, falls die Schule ihn einrichtet, ihr Schul-Login.

1.5 Speicherorte

- Anwendung und Datenbank: Rechenzentrum in Frankfurt am Main; tägliche Sicherung des Hosters AES-256-verschlüsselt in Helsinki (Finnland), 90 Tage.
- Hochgeladene Dateien (Atteste, Anhänge): privater Speicher in Frankfurt am Main, vor dem Speichern in der Anwendung verschlüsselt.
- Endgeräte: Sitzungs- und Anmelde-Cookies im Browser; im Offline-Klassenbuch liegen noch nicht gesendete Einträge bis zur Übertragung unverschlüsselt im Browser der Lehrkraft.
- E-Mails: in den Postfächern der Empfängerinnen und Empfänger. Eine Nachricht wird dort ohne Betreff und Text angekündigt; Rundschreiben mit Titel und Auszug, ohne Anhänge.

1.6 Aufbewahrung und Löschung

- Klassenbuch und Anwesenheit, Krankmeldungen einschließlich Attest, Lesebestätigungen von Rundschreiben, Ausfallmeldungen und das Schwarze Brett löscht die Plattform automatisch nach der Frist, die die Schulleitung bestätigt hat; vorgeschlagen sind die Fristen des Bundeslandes. Vor der Bestätigung wird nichts gelöscht.
- Noten, Zeugnisse, Nachrichten, Rundschreiben, Schülerlisten und Konten löscht die Schule selbst. Termine von Sprechtag und Sprechstunde löscht die Plattform nach der bestätigten Frist (Voreinstellung zwölf Monate nach dem Termin, die die Schule ändern kann), Kurs-Anwesenheit mit der Klassenbuch-Frist.
- Lesezugriffe im Protokoll werden nach 90 Tagen gelöscht, Anwendungsprotokolle des Betreibers nach 14 Tagen.
- Nach Vertragsende bleiben die Daten sechs Monate lesbar und exportierbar; danach löscht der Auftragnehmer sie binnen 30 Tagen, Sicherungen laufen spätestens nach 90 Tagen ab (AVV § 10).

2. Schwellwertprüfung: Ist eine Folgenabschätzung erforderlich?

Eine Folgenabschätzung ist nötig, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen hat (Art. 35 Abs. 1 DSGVO). Geprüft wird in zwei Schritten: Steht die Verarbeitung auf der Muss-Liste der zuständigen Aufsichtsbehörde (Art. 35 Abs. 4)? Und erfüllt sie mindestens zwei der neun Kriterien der Leitlinien zur Folgenabschätzung (WP 248 rev. 01, vom Europäischen Datenschutzausschuss bestätigt)?

2.1 Kriterien der Leitlinien WP 248

Kriterium	Erfüllt?	Begründung
1. Bewerten oder Einstufen	nein	Noten vergeben Lehrkräfte; die Plattform rechnet nur Durchschnitte und bildet keine Profile.
2. Automatisierte Entscheidung mit Rechtswirkung	nein	Die Plattform trifft keine Entscheidungen über Personen.

Kriterium	Erfüllt?	Begründung
3. Systematische Überwachung	teilweise	Anwesenheit wird je Stunde erfasst; das Protokoll hält Lesezugriffe von Beschäftigten auf sensible Listen fest.
4. Vertrauliche oder höchstpersönliche Daten	ja	Gesundheitsdaten in Krankmeldungen und Attesten (Art. 9 DSGVO); Leistungs- und Verhaltensdaten von Kindern.
5. Umfangreiche Verarbeitung	ja	Alle Schülerinnen und Schüler der Schule über mehrere Schuljahre: [Zahl eintragen].
6. Abgleichen oder Zusammenführen von Datensätzen	nein	Importe aus Stundenplan-Programmen und Tabellen übernehmen nur eigene Daten der Schule.
7. Daten schutzbedürftiger Betroffener	ja	Kinder und Jugendliche; Beschäftigte im Verhältnis zu ihrem Dienstherrn.
8. Innovative Nutzung neuer Technologien	nein	Übliche Webanwendung ohne KI-Dienste.
9. Hindert Betroffene an der Ausübung eines Rechts	nein	Sofern die Schule den bisherigen Weg für Krankmeldungen und Mitteilungen offenhält: [bestätigen].

2.2 Muss-Listen der Aufsichtsbehörden

Land	Liste und Eintrag	Ergebnis
Bayern	BayLfD, öffentlicher Bereich (Stand 01.03.2019), Nr. 16, Beispiel „Umfangreiche Verarbeitung personenbezogener Daten von minderjährigen Schülerinnen und Schülern im Rahmen der Schulverwaltung“	Folgenabschätzung erforderlich
Hamburg	HmbBfDI, öffentlicher Bereich (v2.0a, 08.04.2021), Nr. 8 „Umfangreiche Verarbeitung von Daten über Kinder“, Beispiel Schulverwaltungsprogramme	Folgenabschätzung erforderlich
Bremen	LfDI Bremen, öffentlicher Bereich (Stand 25.03.2021), Nr. 8, ebenso, Beispiel Schulverwaltungsprogramme	Folgenabschätzung erforderlich
Brandenburg	LDA Brandenburg, öffentlicher Bereich, Nr. 2 „Umfangreiche Verarbeitung von Daten schutzbedürftiger Personen“, Beispiel „Zentrale Schulverwaltungs-Software“	Folgenabschätzung erforderlich; die gemeinsame Liste gilt dort zusätzlich
alle Länder	Gemeinsame Liste der Datenschutzkonferenz (Version 1.1): Nr. 16 (besondere Kategorien über mobile Anwendungen) und Nr. 8 (Verhaltensdaten Beschäftigter zur Bewertung)	Nr. 16 grenzwertig; Nr. 8 nur, wenn das Protokoll zur Bewertung von Lehrkräften genutzt werden könnte (Risiko R7)
übrige Länder	Liste der zuständigen Aufsichtsbehörde (Verzeichnis der Datenschutzkonferenz): [Liste und Eintrag]	Prüfung nach 2.1 genügt

2.3 Ergebnis

Eine Folgenabschätzung ist erforderlich, jedenfalls für den Bereich Krankmeldungen: Er verarbeitet Gesundheitsdaten von Kindern und erfüllt damit die Kriterien 4 und 7. In Bayern, Hamburg, Bremen und Brandenburg folgt die Pflicht schon aus der Muss-Liste. Diese Abschätzung erfasst alle Bereiche gemeinsam, weil sie dieselbe Plattform, dieselben Konten und dieselben Maßnahmen teilen (Art. 35 Abs. 1 Satz 2 DSGVO).

Eine Schule, die nur Stunden- und Vertretungsplan, Rundschreiben und Termine nutzt, kann zu einem anderen Ergebnis kommen. Sie hält die Begründung hier fest: [Begründung].

3. Notwendigkeit und Verhältnismäßigkeit

3.1 Zwecke

- Unterricht dokumentieren: Anwesenheit, Stundenthemen, Hausaufgaben, pädagogische Einträge.
- Fehlzeiten entschuldigen und eine Attestpflicht nachhalten.
- Leistungen bewerten und Zeugnisse erstellen.
- Eltern und Kollegium informieren, Rückmeldungen einholen, Gespräche führen und Termine vergeben.
- Unterricht und Vertretungen planen.
- Ordnungsgemäße Verarbeitung nachweisen (Protokoll).
- Mit Partnerschulen zusammenarbeiten, wenn die Schule einem Verbund beitritt.

3.2 Rechtsgrundlagen

Verarbeitung	Rechtsgrundlage
Schülerdaten in Unterricht und Organisation	Art. 6 Abs. 1 Buchst. e, Abs. 3 DSGVO in Verbindung mit den Datenschutzvorschriften des Schulgesetzes und den Verordnungen des Landes: [Norm, etwa Art. 85 BayEUG mit Anlage 1 BaySchO, § 120 SchulG NRW mit VO-DV I, §§ 83 ff. HSchG mit SchDSV]
Gesundheitsdaten in Krankmeldungen	Art. 9 Abs. 2 Buchst. g DSGVO in Verbindung mit dem Landesschulrecht zur Schulpflicht und zur Entschuldigung von Fehlzeiten: [Norm]
Kommunikation mit Eltern (Rundschreiben, Nachrichten, Termine, Elternkonto)	Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit dem Landesschulrecht; in Bayern Anlage 1 Abschnitt 3 BaySchO. Das Elternkonto ist ein Angebot der Schule; der bisherige Weg bleibt offen.
Beschäftigtendaten (Konten, Stundenplan, Ausfallmeldungen, Protokoll)	Art. 6 Abs. 1 Buchst. b, c und e, Art. 88 DSGVO in Verbindung mit dem Beschäftigtendatenschutz des Landes: [Norm]; für das Protokoll zusätzlich Art. 5 Abs. 2 und Art. 32 DSGVO.
Schulverbund	Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit den Vorschriften des Landes über die Zusammenarbeit von Schulen: [Norm]

3.3 Datenminimierung

- Schülerinnen und Schüler haben kein Konto; geführt werden nur Vorname, Nachname und Klasse.
- **Der Krankheitsgrund ist ab Werk aus.** Für die Entschuldigung einer Fehlzeit genügt in der Regel, dass das Kind krank ist; der Grund ist eine Gesundheitsangabe, die die Schule nur im Einzelfall braucht. Wer die Abfrage einschaltet, begründet das in Abschnitt 5 (S2).
- Schulen können den Attest-Upload abschalten; für Schulen in Nordrhein-Westfalen, Brandenburg und Berlin ist er voreingestellt aus.
- Ausfallmeldungen von Lehrkräften speichern nie einen Grund.
- Benachrichtigungen enthalten so wenig wie möglich: Eine Nachricht nennt nur den Absender, eine Attest-Erinnerung kein Kind.
- Der Schulträger sieht keine Personen; Klassenlink und Foyer-Bildschirm zeigen keine Namen von Schülerinnen und Schülern.
- Das Protokoll speichert keine IP-Adressen und fasst Lesezugriffe tageweise zusammen.
- In Freitextfeldern fragt die Plattform keine Gesundheitsangaben ab; was dort steht, bestimmt die Schule (AVV § 2 Abs. 4).

3.4 Speicherbegrenzung

Die Fristen nach 1.6 bestätigt die Schulleitung in den Einstellungen für ihr Land. Für die Daten ohne automatische Löschung legt die Schule ein eigenes Verfahren fest: [etwa Noten und Nachrichten eines Schuljahres zum Ende des folgenden Schuljahres löschen; Konten beim Ausscheiden entfernen]. Verlangt das Landesrecht, Unterlagen vor der Vernichtung einem Archiv anzubieten, exportiert die Schule sie vorher.

3.5 Transparenz

Die Schule informiert mit den Mustern für Eltern, Beschäftigte und Schülerinnen und Schüler (Art. 13, 14 DSGVO). Die Schulleitung sieht im Protokoll, wer Daten geändert und wer Listen mit sensiblen Daten

aufgerufen hat. Vertrag, Maßnahmen, Unterauftragnehmer und Fristen sind öffentlich.

3.6 Rechte der Betroffenen

Auskunft und Datenübertragbarkeit setzt die Schule mit dem Export je Schülerin, Schüler oder Elternteil um, den Gesamtexport kann sie jederzeit ziehen. Berichtigung, Löschung und Einschränkung nimmt sie selbst in der Anwendung vor. Anfragen, die beim Auftragnehmer eingehen, leitet er an die Schule weiter (AVV § 9).

3.7 Auftragsverarbeitung und Drittländer

Grundlage ist der Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO; der Auftragnehmer ist zusätzlich nach § 203 StGB zur Geheimhaltung verpflichtet. Alle Speicherorte liegen in der EU. Der Speicheranbieter für Dateien ist eine Gesellschaft mit Sitz in den USA; für einen Zugriff aus den USA gelten Standardvertragsklauseln, und er erhält nur Chiffretext. Push-Dienste der Browser sind keine Unterauftragnehmer und erhalten nur nach dem Web-Push-Standard verschlüsselte Nachrichten.

3.8 Besonderheiten einzelner Länder

Diese Vorgaben haben wir im Text des Landes gelesen; maßgeblich ist die jeweils geltende Fassung. Sie können den Einsatz einzelner Bereiche ausschließen.

Land	Vorgabe	Folge für den Einsatz
Berlin	SchuldatenV vom 07.08.2023: Auftragsverarbeitung nur im Europäischen Wirtschaftsraum, Zugriff nur mit dienstlichem Gerät, Zwei-Faktor-Anmeldung (§ 6 Abs. 5 Nr. 1, 3, 4); unterjährige Zwischennoten nur lokal auf dienstlichen Geräten (§ 10 Abs. 4); Kommunikation nur über Dienste, die die Schulaufsicht bereitstellt oder genehmigt (§ 18 Abs. 2, 3); Gesundheitsdaten nur Ende-zu-Ende-verschlüsselt (§ 18 Abs. 4).	Rundschreiben, Nachrichten und Krankmeldungen erst nach Genehmigung der Schulaufsicht. Die Verschlüsselung von SchuleVernetzt bei Übertragung und Speicherung ist nach unserer Einschätzung keine Ende-zu-Ende-Verschlüsselung; Krankmeldungen deshalb bis zu einer Klärung nicht nutzen. Zwischennoten nicht in SchuleVernetzt führen. Lehrkräfte nur über den Schul-Login mit zweitem Faktor und von dienstlichen Geräten. Für Ersatzschulen gelten §§ 17, 18 nicht (§ 1 Abs. 4).
Brandenburg	Datenschutzverordnung Schulwesen (DSV), Anlage 1: Für Angaben zu gesundheitlichen Beeinträchtigungen (Nr. 1.8) „Eine automatisierte Verarbeitung ist unzulässig." Für Belege über Schulversäumnisse wegen Krankheit (Nr. 1.6), den Nachweis der Unterrichtsversäumnisse (Nr. 2.3) und weitere Daten: Verarbeitung außerhalb der Schule unzulässig, außer in zentralen Fachverfahren mit Vereinbarung nach Art. 28 Abs. 3 DSGVO. Die Schulleitung regelt die Freigabe verbindlich (§ 4 Abs. 2).	Krankheitsgrund nie einschalten. Ob SchuleVernetzt als zentrales Fachverfahren gelten kann, ist zweifelhaft; vor dem Einsatz von Krankmeldungen und Anwesenheit mit dem Schulamt oder dem Ministerium klären. Die Freigabe in Abschnitt 7 festhalten.
Nordrhein-Westfalen	VO-DV I (BASS 10-44 Nr. 2.1), Fußnote zu den Anlagen 1 bis 3: „Medizinische Gutachten und Atteste sind hiervon ausgenommen und dürfen nicht automatisiert verarbeitet werden." Private Geräte nur mit Genehmigung der Schulleitung und nur für die Daten der Anlage 3 (§ 2 Abs. 2).	Keine Atteste hochladen lassen: Atteste auf Papier entgegennehmen und in SchuleVernetzt nur ihren Eingang vermerken. Krankmeldungen ohne Attest-Datei bleiben möglich.
Bayern	Anlage 1 BaySchO lässt Auftragsverarbeiter ausdrücklich zu (Abschnitt 2 Nr. 4.1), auch für die Kommunikation mit Lesebestätigung (Abschnitt 3). Verwaltungsdaten führt die Schule im staatlichen Schulverwaltungsprogramm (Art. 85 Abs. 1 BayEUG).	Einsatz zulässig. SchuleVernetzt ergänzt das Schulverwaltungsprogramm, ersetzt es nicht. Private Geräte vor der ersten Nutzung der Schule anzeigen.
Hessen	SchDSV: Gesundheitsdaten verschlüsselt versenden und speichern, Zugriffsrechte dokumentieren (§ 8 Abs. 5); Schulen sollen das Schulportal Hessen	Verschlüsselung von Krankheitsgrund und Attesten und das Protokoll erfüllen die technische Seite; die Schule dokumentiert die vergebenen Rollen (S1).

Land	Vorgabe	Folge für den Einsatz
	nutzen (§ 10 Abs. 1); private Geräte nur mit schriftlicher Genehmigung (§ 20).	Nutzt sie SchuleVernetzt neben oder statt des Schulportals, hält sie die Gründe fest: [Begründung].
Sachsen	VwV Schuldatenschutz III.12: nur Cloud-Dienste, auf die das Recht der EU Anwendung findet; Unteranbieter und Rechenzentren sind anzugeben.	Hoster und Speicherorte liegen in der EU (Anlage 2). Ob der Speicheranbieter für Dateien als US-Gesellschaft mit reinem Chiffretext genügt, prüft die Schule mit ihrem Datenschutzbeauftragten.
übrige Länder	Auftragsverarbeitung nach Art. 28 DSGVO ist, soweit wir die Vorschriften gelesen haben, zulässig. Die Volltexte für Bremen, Hamburg, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben wir nicht abschließend geprüft.	Die Schule prüft das Landesrecht: [Ergebnis].

4. Risiken und Maßnahmen

Bewertet werden die Risiken für die Betroffenen, nicht für die Schule. Eintrittswahrscheinlichkeit und Schwere werden in vier Stufen geschätzt (geringfügig, überschaubar, substanziell, groß), angelehnt an das Kurzpapier Nr. 18 der Datenschutzkonferenz; daraus ergibt sich ein geringes, mittleres oder hohes Risiko. „TOM“ verweist auf die Abschnitte der technischen und organisatorischen Maßnahmen (Anlage 1 zum AVV), „S“ auf die Maßnahmen der Schule in Abschnitt 5. Die Schule prüft jede Bewertung für ihre Lage.

Nr.	Risiko und Bereich	Ausgangsrisiko	Maßnahmen	Restrisiko
R1	**Unbefugter Zugriff auf Gesundheitsdaten.** Unberechtigte innerhalb oder außerhalb der Schule lesen Krankheitsgründe oder Atteste. Bereich: Krankmeldungen.	Eintritt überschaubar, Schwere groß: hoch	Krankheitsgrund ab Werk nicht abgefragt (TOM 1). Grund lesen nur Schulleitung, Sekretariat und Klassenleitung, jeder Aufruf wird protokolliert (TOM 4, 6). Grund und Atteste in der Anwendung verschlüsselt, der Speicheranbieter hält nur Chiffretext; Auslieferung nur nach Rechteprüfung (TOM 4). Fristenlöschung einschließlich Attest (TOM 1). Schule: S1, S2, S3.	gering
R2	**Übergriff zwischen Schulen.** Durch einen Programmfehler werden Daten einer Schule für Nutzer einer anderen sichtbar. Bereich: alle.	Eintritt überschaubar, Schwere groß: hoch	Jeder Datensatz gehört genau einer Schule, jede Abfrage ist auf sie begrenzt, Downloads nur mit Schulbindung (TOM 3, 4). Automatische Tests der Trennung bei jeder Änderung (TOM 3). Die Trennung ist logisch in der Anwendung, nicht durch getrennte Datenbanken.	gering
R3	**Zugriff durch den Betreiber.** Der Betreiber ist ein Ein-Personen-Betrieb mit technischem Vollzugriff; ein Missbrauch oder ein kompromittierter Betreiberzugang legt Daten offen. Bereich: alle.	Eintritt überschaubar, Schwere groß: hoch	Zugriff nur, soweit Betrieb, Fehlerbehebung oder eine Anfrage der Schule es erfordern; Geheimhaltung nach § 203 StGB (TOM 4, 8; AVV § 4a). Ein Zugriff über „Benutzer wechseln“ erscheint im Protokoll der Schule als „Betreiber (SavePaperwork)“ mit Namen (TOM 4). Verwaltungsbereich nur mit Administratorrolle, Server nur über die verschlüsselte Verbindung des Inhabers (TOM 8). Die Verschlüsselung in der Anwendung schützt gegen Speicheranbieter und Datenbankabzug, nicht gegen den Betreiber selbst. Schule: S13.	mittel; Zugriffe über die Anwendung stehen im Protokoll der Schule, Zugriffe direkt auf Server und Datenbank nicht

Nr.	Risiko und Bereich	Ausgangsrisiko	Maßnahmen	Restrisiko
R4	**Offenlegung auf dem Sperrbildschirm oder in der Mailvorschau.** Dritte sehen Benachrichtigungen mit Namen oder Inhalten. Bereiche: Krankmeldungen, Nachrichten, Rundschreiben.	Eintritt substanziell, Schwere überschaubar: mittel	Push ist freiwillig; eine Nachricht nennt nur den Absender, der Vertretungsplan einen festen Text, die Attest-Erinnerung kein Kind (TOM 1). Mails zu Nachrichten ohne Betreff und Auszug, Anhänge von Rundschreiben nie in der Mail (TOM 1). Rundschreiben-Mails enthalten Titel und Auszug. Schule: S6, S9.	gering
R5	**Verlust oder Nichtverfügbarkeit.** Daten gehen durch Fehler, Angriff oder Ausfall verloren oder sind zeitweise nicht erreichbar. Bereich: alle.	Eintritt überschaubar, Schwere substanziell: mittel	Tägliche verschlüsselte Sicherung des Hosters in einem getrennten Rechenzentrum, 90 Tage; Überwachung alle fünf Minuten; neue Versionen mit Rückweg; Offline-Klassenbuch (TOM 2). Gesamtexport jederzeit (TOM 2, 7). Schule: S11.	mittel; durch den Export der Schule begrenzt
R6	**Zugriff aus einem Drittland auf Dateien.** Der Speicheranbieter ist eine US-Gesellschaft; US-Behörden könnten Herausgabe verlangen. Bereiche: Atteste und Anhänge.	Eintritt geringfügig, Schwere groß: mittel	Speicherort Frankfurt am Main, privater Speicher (TOM 4). Jede Datei wird vor dem Speichern in der Anwendung verschlüsselt, der Anbieter erhält nur Chiffretext unter zufälligem Namen und nie den Schlüssel; Standardvertragsklauseln (TOM 4, Anlage 2). Sichtbar bleiben Größe und Zeitpunkt. Schule: S14.	gering
R7	**Überwachung von Lehrkräften durch das Protokoll.** Das Protokoll zeigt, wer Datensätze geändert und sensible Listen aufgerufen hat, und ist objektiv geeignet, Verhalten und Leistung zu überwachen. Bereich: Protokoll.	Eintritt überschaubar, Schwere substanziell: mittel	Lesezugriffe nur tageweise je Person und Liste und nach 90 Tagen gelöscht; keine IP-Adressen; sensible Werte geschwärzt (TOM 1, 3). Zweck ist der Nachweis ordnungsgemäßer Verarbeitung, keine Leistungs- oder Verhaltenskontrolle. Änderungen bleiben gespeichert, solange das Schulkonto besteht. Schule: S7.	gering mit Dienstvereinbarung, sonst mittel
R8	**Unverschlüsselte Daten auf dem Gerät der Lehrkraft.** Noch nicht gesendete Einträge des Offline-Klassenbuchs liegen unverschlüsselt im Browser. Bereich: Klassenbuch.	Eintritt überschaubar, Schwere überschaubar: mittel	Die Daten liegen nur bis zur nächsten Übertragung auf dem Gerät (TOM 2). Schule: S6.	gering mit Geräteregel
R9	**Übernahme von Konten ohne zweiten Faktor.** Ein erratenes, wiederverwendetes oder abgefischtes Passwort öffnet ein Eltern- oder Lehrkraftkonto. Eltern sehen nur ihre Kinder und keine Noten; ein Lehrkraftkonto sieht die Daten seiner Klassen. Bereiche: Konten und alle Bereiche dahinter.	Eintritt substanziell, Schwere substanziell: hoch	Passwörter nur als Hash, höchstens fünf Versuche, Rechenrätsel ohne Drittanbieter, Rücksetz-Links 24 Stunden und einmalig, Sitzungen enden bei Passwortwechsel (TOM 4). Zweiter Faktor Pflicht für Sekretariat und Träger, verfügbar für Schulleitung, Lehrkräfte und Eltern; die Schule kann ihn für das Kollegium verlangen oder über den Schul-Login sicherstellen (TOM 4). Eine Content-Security-Policy lässt in den Bereichen der Schule nur Skripte der Plattform selbst zu (TOM 4). Schule: S5, S9.	Eltern gering; Lehrkräfte gering mit zweitem Faktor (eigener oder über den Schul-Login), sonst mittel
R10	**Zu lange oder zu kurze Aufbewahrung.** Daten bleiben länger als erlaubt oder werden gelöscht,	Eintritt substanziell, Schwere	Fristen je Land mit Norm vorgeschlagen; Löschung erst nach Bestätigung, Vorschau 14 Tage vorher; wo ein Land ab Schulabgang rechnet, ein längerer	gering, wenn die Schule Fristen bestätigt und ein

Nr.	Risiko und Bereich	Ausgangsrisiko	Maßnahmen	Restrisiko
	solange die Schule sie noch braucht. Bereich: alle.	überschaubar: mittel	Ersatzwert (TOM 1). Gesamtexport vor der Löschung (TOM 7). Keine automatische Löschung für Noten, Zeugnisse, Nachrichten und Konten (AVV Anlage 5). Nach Vertragsende werden die Daten nach der Lesephase von sechs Monaten automatisch gelöscht, angekündigt vier Wochen und eine Woche vorher (AVV § 10). Schule: S4.	Löschverfahren festlegt
R11	**Fehlversand von E-Mails.** Eine Einladung oder Benachrichtigung geht an eine falsche Adresse. Eine Einladung nennt die Kinder; wer sie annimmt, kann Zugang zum Elternportal eines fremden Kindes erhalten. Bereiche: Konten, Rundschreiben, Nachrichten.	Eintritt überschaubar, Schwere substanziell: mittel	Mails zu Nachrichten ohne Betreff und Auszug; Anhänge von Rundschreiben nie in der Mail, sondern nur nach Anmeldung (TOM 1, 4). Schule: S9, S10.	gering bei geprüften Adressen
R12	**Offenlegung im Schulverbund.** Daten werden einer Partnerschule zugänglich, ohne dass die Schule es will, oder bleiben nach einem Austritt sichtbar. Bereich: Verbund.	Eintritt geringfügig, Schwere überschaubar: gering	Der Verbund teilt nichts, bis die Schule beitritt und je Bereich zustimmt; Kontaktdaten einer Aushilfslehrkraft erst nach Freigabe; ein Austritt sperrt sofort (TOM 5). Schule: S12.	gering
R13	**Sensible Angaben in Freitexten.** In Klassenbuch-Einträge, Nachrichten oder Notenkommentare geraten Gesundheits- oder Familienangaben. Bereiche: Klassenbuch, Nachrichten, Noten.	Eintritt substanziell, Schwere substanziell: hoch	Diese Freitexte sind in der Anwendung verschlüsselt (TOM 4); Klassenbuch-Einträge sind für Eltern nie sichtbar; die Plattform fragt dort keine Gesundheitsangaben ab (AVV § 2 Abs. 4). Schule: S9.	gering mit Einweisung

5. Maßnahmen der Schule

Diese Maßnahmen liegen bei der Schule. Die Bewertungen in Abschnitt 4 setzen sie voraus.

Nr.	Maßnahme	Risiko	Erledigt am, durch
S1	Rollen vergeben und festhalten: Schulleitung, Sekretariat mit sparsamen Freigaben, Klassenleitungen, Lehrkräfte; Konten ausscheidender Personen sofort entfernen.	R1, R9	[Datum, Name]
S2	Krankheitsgrund nur einschalten, wenn die Schule ihn braucht, und den Grund hier festhalten: [Begründung]. In Brandenburg nie einschalten.	R1	[Datum, Name]
S3	Eine Attestpflicht nur eintragen, wo das Landesrecht oder die Schulordnung sie vorsieht. In Nordrhein-Westfalen Atteste auf Papier entgegennehmen und nur den Eingang vermerken.	R1	[Datum, Name]
S4	Aufbewahrungsfristen prüfen und bestätigen; für Noten, Zeugnisse, Nachrichten und Konten ein Löschverfahren festlegen; vor einer Löschung das Archivangebot des Landes beachten.	R10	[Datum, Name]
S5	Den Schul-Login mit Mehr-Faktor-Anmeldung für Lehrkräfte einrichten, wo die Schule einen hat; den zweiten Faktor für die Schulleitung einschalten.	R9	[Datum, Name]
S6	Geräteregel: dienstliche Geräte oder private Geräte nach Genehmigung bzw. Anzeige gemäß Landesrecht; Bildschirmsperre, aktuelle Software, keine Mitbenutzung; Push-Inhalte auf dem	R4, R8	[Datum, Name]

Nr.	Maßnahme	Risiko	Erledigt am, durch
	Sperrbildschirm ausblenden.		
S7	Die Personalvertretung beteiligen und eine Dienstvereinbarung zum Protokoll schließen: nur zur Datenschutzkontrolle, Einsicht nur bei konkretem Anlass und im Vier-Augen-Prinzip, keine Leistungs- oder Verhaltenskontrolle, Löschfrist. Ein Muster enthält das Infoblatt für den Personalrat von SavePaperwork. Zuständig: [Personalrat an der Schule, beim Schulamt oder bei der Bezirksregierung].	R7	[Datum, Name]
S8	Eltern, Beschäftigte und Schülerinnen und Schüler mit den Datenschutzhinweisen informieren.	—	[Datum, Name]
S9	Nutzerinnen und Nutzer einweisen: keine Gesundheits- oder Familienangaben in Freitexte, keine sensiblen Inhalte in Titel von Rundschreiben, sorgfältiger Umgang mit E-Mail-Adressen, Abmelden auf geteilten Geräten.	R4, R9, R11, R13	[Datum, Name]
S10	E-Mail-Adressen der Eltern aus verlässlicher Quelle übernehmen, Einladungen vor dem Versand prüfen und die Zuordnung von Eltern zu Kindern kontrollieren.	R11	[Datum, Name]
S11	Regelmäßig den Gesamtexport ziehen, etwa zum Halbjahr, und geschützt in der Schule ablegen; einen Notfallweg bei Ausfall festlegen, etwa ein Papier-Klassenbuch.	R5	[Datum, Name]
S12	Einem Verbund nur nach Absprache mit den Partnerschulen beitreten; festlegen, wer Kontaktdaten freigibt.	R12	[Datum, Name]
S13	Festlegen, ob der Betreiber Zugriffe auf Daten der Schule vorher ankündigen oder nachträglich in Textform mitteilen soll, und das als Weisung erteilen (AVV § 3 Abs. 2).	R3	[Datum, Name]
S14	Das Landesrecht nach 3.8 prüfen und, wo nötig, die Genehmigung der Schulaufsicht einholen.	R6	[Datum, Name]
S15	Den Vertrag zur Auftragsverarbeitung abschließen und die Einträge des Verarbeitungsverzeichnisses übernehmen.	—	[Datum, Name]
S16	Diese Folgenabschätzung jährlich und bei wesentlichen Änderungen überprüfen, etwa wenn ein Bereich hinzukommt oder Anlage 1 sich ändert (Art. 35 Abs. 11 DSGVO).	alle	[Datum, Name]

6. Restrisiko und Ergebnis

Mit den Maßnahmen der Plattform und der Schule sind die meisten Restrisiken gering. Mittel bleiben der Zugriff durch den Betreiber (R3), die Verfügbarkeit, die an einem Hoster hängt (R5), und Lehrkraftkonten ohne zweiten Faktor (R9). Ein hohes Restrisiko bleibt nach unserer Einschätzung nicht.

Eine vorherige Konsultation der Aufsichtsbehörde (Art. 36 DSGVO) ist nur nötig, wenn nach den Maßnahmen ein hohes Restrisiko bleibt, das die Schule nicht weiter senken kann. Dann legt sie diese Abschätzung vor Beginn der Verarbeitung ihrer Aufsichtsbehörde vor. Für Berlin, Brandenburg und Nordrhein-Westfalen gilt das Ergebnis nur mit den Einschränkungen nach 3.8.

Ergebnis der Schule (zutreffendes ankreuzen):

- [ ] Die Restrisiken sind vertretbar; die Verarbeitung wird mit den Maßnahmen nach Abschnitt 4 und 5 durchgeführt.
- [ ] Vor Beginn sind weitere Maßnahmen nötig: [Maßnahmen, Frist].
- [ ] Es bleibt ein hohes Restrisiko; die Aufsichtsbehörde wird nach Art. 36 DSGVO konsultiert.

7. Beteiligung und Freigabe

Schritt	Eintrag
Stellungnahme des Datenschutzbeauftragten der Schule (Art. 35 Abs. 2 DSGVO)	[Datum, Ergebnis, Name]

Schritt	Eintrag
Standpunkt der Betroffenen oder ihrer Vertretung, etwa Schulkonferenz, Elternvertretung, Schülervertretung (Art. 35 Abs. 9 DSGVO)	[Gremium, Datum, Ergebnis]
Beteiligung der Personalvertretung (Mitbestimmung bei technischen Einrichtungen, etwa Art. 75a Abs. 1 Nr. 1 BayPVG, § 72 Abs. 3 Nr. 2 LPVG NRW)	[Personalrat, Datum der Zustimmung oder der Dienstvereinbarung]
Genehmigung oder Freigabe nach Landesrecht, etwa Schulaufsicht in Berlin, Schulleitung in Brandenburg	[Stelle, Datum, Aktenzeichen]
Freigabe durch die Schulleitung	[Ort, Datum, Name, Unterschrift]
Nächste Überprüfung	[Datum, spätestens in einem Jahr]

Die Angaben zur Plattform geben den Stand vom 12.11.2026 wieder. SavePaperwork kündigt Änderungen an, die diese Abschätzung berühren: neue Unterauftragnehmer 30 Tage vorher (AVV § 6), wesentliche Änderungen der Maßnahmen in Anlage 1 (AVV § 4 Abs. 3).