Ranzen

Datenschutz-Folgenabschätzung: Ranzen

Entwurf für die Einrichtung nach Art. 35 DSGVO · Fassung vom 28. September 2026

Vorlage der Zeitreise-Manufaktur. Die Folgenabschätzung verantwortet die Einrichtung; ihr Datenschutzbeauftragter ist zu beteiligen (Art. 35 Abs. 2 DSGVO). Mehrere Länder verlangen sie ausdrücklich für digitale Klassen- und Notenbücher oder für die Verarbeitung von Daten Minderjähriger (etwa Baden-Württemberg, Mecklenburg-Vorpommern, Niedersachsen). Keine Rechtsberatung.

1. Beschreibung der Verarbeitung

Die Einrichtung nutzt die Web-App **Ranzen** für Kommunikation und Organisation mit Familien und im Team. **Ranzen** läuft als Auftragsverarbeitung auf einem Server in Nürnberg. Eingeschaltete Module: [ankreuzen: Krankmeldung · Elternbriefe · Nachrichten · Stundenplan · Hausaufgaben · Klassenbuch · Noten · Sprechtag · Hort]. Personen, Daten, Empfänger und Fristen: siehe Verzeichnis der Verarbeitungstätigkeiten.

2. Notwendigkeit und Verhältnismäßigkeit

- **Zweck:** schnellere, verlässliche Information und weniger Papier bei Aufgaben, die das Schul- bzw. Kita-Recht der Einrichtung zuweist.
- **Datenminimierung:** Module, die nicht gebraucht werden, bleiben aus. Beim Anlegen sind landesrechtlich unklare Module ausgeschaltet. Die Krankmeldung braucht keinen Freitext; ein Grund nur als feste Auswahl, wenn das Land ihn verlangt.
- **Freiwilligkeit:** Eltern können ohne App teilnehmen (Papier, Telefon). Ihnen entstehen keine Nachteile.
- **Speicherbegrenzung:** automatische Löschfristen (Verzeichnis Nr. 7).
- **Transparenz:** Information nach Art. 13 DSGVO mit der Vorlage „Information und Einwilligung“.

3. Risiken für Betroffene und Maßnahmen

Risiko	Wie wahrscheinlich, wie schwer	Maßnahmen in Ranzen und in der Einrichtung	Rest
Unbefugte sehen Daten eines Kindes (falsche Zuordnung, weitergegebener Link)	möglich, mittel	Anmeldelink gilt 15 Minuten und einmal; Anmeldebrief nur an berechtigte Person; Eltern sehen nur eigene Kinder; Rollenmodell; Einrichtung prüft Zuordnungen beim Import	gering
Übernahme eines Kontos von Leitung oder Verwaltung	selten, schwer	Zwei-Faktor-Anmeldung (Code-App), für Leitung und Verwaltung als Pflicht schaltbar; Begrenzung von Anmeldeversuchen; Sicherheitsprotokoll	gering
Gesundheitsdaten werden zu breit sichtbar	möglich, schwer	Atteste nur für Sekretariat, Leitung, Klassenleitung; Attest-Upload schaltbar und in vielen Ländern aus; kein Freitext bei Krankmeldung; Löschung nach 1 Jahr	gering

Daten bleiben auf privaten Geräten der Lehrkräfte	möglich, mittel	Ranzen speichert für Beschäftigte nichts für die Offline-Nutzung; beim Abmelden wird der Zwischenspeicher gelöscht; Einrichtung regelt Dienstgeräte bzw. Genehmigung privater Geräte nach Landesrecht	mittel, organisatorisch
Verlust von Daten (Ausfall, Fehler)	selten, mittel	tägliche verschlüsselte Sicherung, zusätzlich täglich außer Haus in einem zweiten Rechenzentrum (Falkenstein) mit Snapshots; Export jederzeit	gering
Zugriff des Anbieters auf Inhalte	selten, mittel	Support-Zugang nur nach Freigabe je Anliegen, befristet und protokolliert; keine Nutzung für eigene Zwecke; KI-gestützte Wartung technisch ohne Zugriff auf personenbezogene Daten	gering
Übermittlung in Drittländer	möglich, gering	nur bei eingeschalteten Push-Benachrichtigungen, Inhalt verschlüsselt; Einrichtung kann Push abschalten oder auf Hinweis ohne Inhalt beschränken	gering
Profilbildung, Verhaltens- oder Leistungskontrolle	selten, mittel	keine Analyse- oder Werbedienste; keine Aktivitätsstatistik über Beschäftigte; Frühwarnung bei Fehlzeiten schaltbar und nur als Hinweis an die Leitung	gering
Fehlende Ende-zu-Ende-Verschlüsselung	–	Nachrichten sind verschlüsselt übertragen und im Rechenzentrum geschützt, aber nicht Ende-zu-Ende; für besonders vertrauliche Inhalte andere Wege nutzen	zu bewerten

4. Ergebnis

[Von der Einrichtung auszufüllen:] Nach Umsetzung der Maßnahmen ist das Restrisiko [gering / vertretbar]. Eine vorherige Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO ist [nicht] erforderlich.

Ort, Datum _____

_____

Schulleitung bzw. Leitung

_____

Datenschutzbeauftragte/r (Stellungnahme)