



SCHWELLENWERTANALYSE UND RISIKOABSCHÄTZUNG

Kando: Datenschutz-Folgenabschätzung (DSFA)

Musterunterlage nach Art. 35 DSGVO für Lernstands-, Ergebnis- und Förderdaten

Dokumentversion 1.4 · Prüfstand: 1. Oktober 2026 · Kontakt: info@kandoapp.de

Wichtiger Hinweis für Schulen

Dieses Dokument ist eine Muster- und Arbeitsunterlage. Die Schule beziehungsweise der Schulträger bleibt für die konkrete DSFA, die Rechtsgrundlage und die Freigabe im eigenen Schulbetrieb verantwortlich. Lokale Vorgaben, Schulrecht, Aufbewahrungsfristen, Geräteverwaltung und Zuständigkeiten müssen ergänzt werden.

1. Gegenstand und Zweck der Verarbeitung

Kando ist eine Web- und Mobilanwendung für Lehrkräfte zur Erstellung, Durchführung, automatischen Vorkorrektur, Übungsfreigabe und Rückmeldung von Lernstandsüberprüfungen. Schülerinnen und Schüler benötigen kein eigenes Konto. Sie verwenden persönliche Schülercodes, damit Tests und Übungspakete ohne Klarnamenübertragung zugeordnet werden können.

- Tests und Lernstände: Aufgaben, Antworten, Punkte, Prozentwerte, Noten oder Status ohne Benotung.
- Ausgleichs- und Differenzierungsdaten: Zeitverlängerung, erweiterte Rechtschreibtoleranz, größere Eingabefelder, Vorlesen, zielfferente Aufgabenvarianten, Niveaubezeichnungen und weitere schulisch festgelegte Nachteilsausgleichslogik.
- Übungsbereich: verschlüsselte Freigaben, Karteikarten, Schreiben, Multiple Choice, True/False und lokale Fehlerwiederholung pro Schülercode.
- Live-Runde: gemeinsames Vokabelquiz am Beamer mit Spielnamen statt Namen; verschlüsselte Fragen und Antworten nur im Arbeitsspeicher des Servers, Wertung auf dem Lehrkraftgerät, keine Leistungsfeststellung.
- Fachliche Ressourcen: Aufgabenpool, Tests, Tags, Tatoeba-Kontextsätze und Quellenangaben ohne zulässige Schülerpersonenbezüge.
- Zusammenarbeit: Mehrere Lehrkräfte derselben Schule können an einem Test arbeiten. Das Verteilen und die Ergebnisse bleiben je Lehrkraft getrennt; Schuladmins erhalten über ihre Rolle keinen inhaltlichen Zugriff auf fremde Tests.
- Lehrkraftbezogene Nebendaten: Rückmeldungen aus dem Feedback-Formular mit Anzeigenname und Konto-E-Mail sowie anonyme Nutzungsstatistiken ohne Personenbezug. Beide betreffen die Lehrkraft, nicht Schülerinnen und Schüler.

2. Erforderlichkeit einer DSFA

Eine DSFA ist im schulischen Einsatz regelmäßig zu prüfen, weil minderjährige Personen betroffen sind und mit Lernstands-, Leistungs- und gegebenenfalls Ausgleichs- oder Förderdaten gearbeitet wird. Kando speichert keine Diagnose als Pflichtfeld, die eingesetzten Ausgleichsoptionen können je nach Ausgestaltung aber besondere Kategorien personenbezogener Daten oder jedenfalls Daten mit hohem Schutzbedarf betreffen.

Prüfentscheidung

Kando reduziert das Risiko technisch erheblich durch Ende-zu-Ende-Verschlüsselung und Datenminimierung. Gleichwohl sollte die Schule die DSFA vor Produktivbetrieb dokumentieren, weil Zweck, Rechtsgrundlage, Fristen, Geräteverwaltung und pädagogische Bewertung schulisch festgelegt werden.

3. Systematische Beschreibung der Verarbeitung

1. Die Lehrkraft registriert ein verifiziertes Konto, legt Passwort, Notfallschlüssel und nach der Ersteinrichtung einen Passkey fest.
2. Lerngruppen, Schülernummern, individuelle Ausgleichs- und Förderoptionen, Ergebnisse und private Einstellungen werden lokal verschlüsselt und nur als verschlüsselte Pakete synchronisiert.
3. Bei Tests erzeugt die Lehrkraft eine temporäre Sitzung mit eigenem Sitzungsschlüssel. Der QR-Code enthält keine Schülerdaten und wird ohne externe QR-Dienste erzeugt.
4. Der Schüler gibt seinen persönlichen Schülercode ein. Nur der zugehörige verschlüsselte Identitätsdatensatz kann geöffnet werden.
5. Die Lehrkraft gibt den Versuch frei. Das Schülergerät wird vorübergehend an den Versuch gebunden, damit Mehrfachstarts kontrollierbar werden.
6. Abgaben werden auf dem Schülergerät verschlüsselt, temporär über den Server übermittelt und anschließend auf dem Lehrkraftgerät entschlüsselt, korrigiert und wieder verschlüsselt synchronisiert.
7. Übungsfreigaben verwenden ebenfalls persönliche Schülercodes; die Fehlerhistorie wird lokal pro Schülercode getrennt geführt und ist nicht als Note vorgesehen.
8. In einer Live-Runde treten Schülergeräte über einen QR-Code ohne Schülercode bei und erhalten einen Spielnamen. Fragen und Antworten laufen verschlüsselt über den Server; das Lehrkraftgerät wertet und zeigt höchstens die fünf Besten. Nach dem Schließen ist auf dem Server nichts mehr gespeichert.
9. Betreiberfunktionen ermöglichen Kontosperrung, Kontoanonymisierung/-löschung, Schulverwaltung, Testkonto-Erneuerung und Audit-Export für Rechenschaft und Sicherheit.
10. Zur Kontosicherheit kann die Systemadministration je Lehrkraftkonto Anmeldeverfahren, Zeitpunkt der letzten Anmeldung sowie hinterlegte Passkeys und offene Sitzungen einsehen (Bezeichnung des Geräts, Anmeldeverfahren, Zeitstempel). Zweck ist ausschließlich Kontosicherheit und Support, nicht die Kontrolle der Arbeitszeit oder Tätigkeit. Der Abruf erfolgt einzelfallbezogen und wird selbst im Audit-Protokoll vermerkt.

4. Datenschutz durch Technikgestaltung

Schutzprinzip	Umsetzung in Kando
Datenminimierung	Schüler benötigen kein Konto. Im Testserver werden keine offenen Klassenlisten gespeichert; temporäre Testdaten werden spätestens nach 24 Stunden gelöscht.
Pseudonymisierung	Schülercodes, zufällige IDs, gehashte Gerätekennungen und pseudonyme Versuchsdaten vermeiden sprechende Serverreferenzen.
Ende-zu-Ende-Verschlüsselung	Private Lerngruppen, Ergebnisse, sensible Einstellungen und Synchronisierungsinhalte werden mit AES-256-GCM verschlüsselt. Der Betreiber besitzt keinen privaten Kontoschlüssel im Klartext, kann ihn aber über den für die Kontowiederherstellung hinterlegten Umschlag gewinnen; dieser Weg ist organisatorisch auf die Wiederherstellung beschränkt.
Lokale Bewertung	Punkte, Prozentwerte und Noten werden auf dem Lehrkraftgerät berechnet. Der Testserver berechnet keine Noten.
Zweckbindung der	Sicherheitsdetails eines Lehrkraftkontos werden nur auf ausdrücklichen Einzelabruf

Schutzprinzip	Umsetzung in Kando
Betreibersicht	angezeigt, enthalten keine Anmeldedaten, Schlüssel oder IP-Adressen und werden protokolliert.
Trennung von Inhalt und Personenbezug	Bei gemeinsamer Testbearbeitung werden nur Aufgaben und Testeinstellungen freigegeben. Ergebnisse, Lerngruppen und Schülerdaten sind mit dem persönlichen Kontoschlüssel verschlüsselt und für mitarbeitende Kolleginnen und Kollegen technisch nicht zugänglich.
Berechtigung	Lehrkraft, Schuladmin und Systemadmin; private, schulinterne und öffentliche Ressourcen sind serverseitig getrennt und durch RLS/Services geschützt.
Transparenz	Bewertungskriterien, Exam-Mode-Hinweise, Audit-Logs, Export-Hinweise und Ressourcen für Schulen sind dokumentiert.
Verfügbarkeit	Wöchentliches verschlüsseltes Backup, Betriebsmonitoring, Restore-Test und AirDrop-/Dateifallback für Störfälle.

5. Risikoanalyse

Risiko	Auswirkung	Gegenmaßnahmen	Restrisiko
Server-Datenleck	Angreifer erhalten Datenbank, Backups oder Dateidaten.	AES-GCM für private Inhalte; keine offenen Schülerlisten im Testserver; Backup verschlüsselt; RLS, Rechteprüfung, Sicherheitsheader und Größenlimits.	Gering, sofern Schlüssel und Backup-Passphrase getrennt geschützt werden.
Kompromittiertes Lehrkraftgerät	Klartextdaten sind sichtbar, wenn das Gerät entsperrt ist.	Passkey oder Kontopasswort, 15-Minuten-Sperre in der WebApp, widerrufbare Sitzungen, Geräteverwaltung, lokale Verschlüsselung.	Mittel; MDM, Gerätecode und organisatorische Regeln der Schule bleiben nötig.
Falsche Testzuordnung	Ein Ergebnis könnte einem falschen Schüler oder Niveau zugeordnet werden.	Persönliche Schülercodes, verschlüsselte Identitätsdatensätze, Warteschleuse mit Lehrkraftfreigabe, clientAttemptId und Gerätebindung.	Gering bis mittel; Lehrkraft muss Freigabe kontrollieren.
Offenlegung von Ausgleichs- oder Fördermerkmalen	Sensible Angaben können unberechtigt sichtbar werden oder Rückschlüsse auf Unterstützungsbedarf erlauben.	Ausgleichsoptionen in verschlüsselten Kontoeinstellungen; keine offene Speicherung im Testserver; zieldifferente Abgaben ohne Note; minimale Anzeige in der Schüleransicht.	Gering, sofern Klassenlisten, Codekarten und Ausdrucke geschützt werden.
Exporte auf privaten Geräten	PDF-/CSV-Dateien bleiben außerhalb von Kando liegen.	Warnhinweise, Ressourcen für Schulen, Exportverantwortung und Löschfristen dokumentiert.	Mittel; externe Dateien kann Kando technisch nicht löschen.
Übungsgerät wird gemeinsam genutzt	Fehlerhistorie eines Schülers könnte einem anderen angezeigt werden.	Lokale Fehlerhistorie ist pro Schülercode getrennt; Schülercodewechsel setzt die angezeigten Fehler um.	Gering; Browserdaten können durch Schule gelöscht werden.
Bloßstellung oder Kränkung in der Live-Runde	Schwächere Kinder werden über Ranglisten sichtbar; ein frei gewählter Spielname	Spielnamen voreingestellt aus geprüften Listen; freie Namen nur nach Wahl der Lehrkraft und mit Wortfilter; Lehrkraft kann Teilnehmende entfernen; am Beamer nur die	Gering; die Lehrkraft entscheidet über Einsatz und

Risiko	Auswirkung	Gegenmaßnahmen	Restrisiko
	kann beleidigend sein oder den echten Namen enthalten.	fünf Besten, Rangliste abschaltbar; kein Ergebnis in der Notenverwaltung.	Einstellungen.
Tatoeba-/ Kontextsätze	Lizenz- oder Drittanbieterproblem.	Lokaler Serverkorporus, keine externen Suchanfragen; Anzeige von Satz-ID, Ersteller und CC BY 2.0 FR-Lizenz.	Gering; Lehrkraft prüft fachliche Eignung.
Betriebsausfall oder Datenverlust	Tests oder Kontodaten sind zeitweise nicht verfügbar.	Wöchentliches verschlüsseltes Backup, Restore-Test, Monitor, AirDrop-/Dateifallback bei Abgabe.	Gering bis mittel; Wiederanlaufzeit muss betrieblich festgelegt werden.
Missbrauch von Adminrechten	Konten, Schulen oder Auditdaten werden unbefugt verwaltet.	Systemadmin-Rolle, Audit-Protokoll, Schutz der Betreiberzugänge, keine normale Schuladministration für Betreiberfunktionen. Die Rolle Schuladministration verwaltet Mitgliedschaften und hat kein Schreibrecht auf fremdes Unterrichtsmaterial.	Mittel; Vier-Augen-Prinzip ist organisatorisch sinnvoll.
Unbefugter Zugriff über Testfreigaben	Mitarbeitende sehen Material, das nicht für sie bestimmt ist.	Mitarbeit nur für namentlich eingetragene Lehrkräfte derselben Schule; Eintragen ausschließlich durch die Eigentümernde Lehrkraft; jede Änderung der Beteiligten wird protokolliert; Ergebnisse und Schülerdaten bleiben Ende-zu-Ende verschlüsselt.	Gering.

6. Interessenabwägung und Verhältnismäßigkeit

Die Verarbeitung dient der Durchführung schulischer Lernstandsüberprüfungen, differenzierter Förderung und zeitnaher Rückmeldung. Die gewählte Architektur beschränkt die serverseitige Lesbarkeit besonders sensibler Daten, vermeidet Schülerkonten und reduziert Drittanbieterabhängigkeiten. Kando ist nur verhältnismäßig, wenn die Schule die Nutzung auf erforderliche Daten beschränkt, Ausgleichs- und Förderoptionen nur bei tragfähiger Rechtsgrundlage erfasst, Exporte schützt und Löschfristen tatsächlich umsetzt.

7. Ergänzende schulische Maßnahmen

- Rechtsgrundlage nach Schul- und Landesdatenschutzrecht festlegen; bei Ausgleichs- und Förderoptionen mit Rückschluss auf Gesundheit, Behinderung oder Förderbedarf Art. 9 DSGVO beziehungsweise landesrechtliche Spezialnorm prüfen.
- AV-Vertrag, TOM-Anlage, Unterauftragsverarbeiter, Hosting- und Backupziel dokumentieren.
- Dienstliche Geräte, MDM, Bildschirmsperre, Passwort-/Passkey-Regeln und Umgang mit privaten Geräten regeln.
- Löschfristen für Ergebnisse, Exporte, Ausdrucke und Backups festlegen; regelmäßige Restore-Tests dokumentieren.
- Eltern und Schüler altersangemessen informieren; bei Bedarf alternative Durchführung ohne Kando vorsehen.
- Lehrkräfte zum Umgang mit Aufgabenpool, urheberrechtlich geschützten Inhalten, Tatoeba-Lizenzen und personenbezogenen Daten in öffentlichen Ressourcen schulen.

8. Ergebnis der Musterbewertung

Bei korrekter Einrichtung, Abschluss eines AV-Vertrags, Umsetzung schulischer Geräte- und Löschregeln sowie Beachtung der Förderdatenschutzanforderungen erscheint der Einsatz von Kando aufgrund der

durchgehenden Verschlüsselung auf dem Endgerät und der lokalen Bewertung technisch gut absicherbar. Die verbleibenden Risiken liegen vor allem beim betreiberseitigen Wiederherstellungsweg, bei entsperren Lehrkraftgeräten, Exportdateien, organisatorischer Rollenvergabe und der rechtlichen Einordnung von Förderdaten.

9. Freigabe und lokale Ergänzungen

Schule / Schulträger: _____

Datenschutzbeauftragte Person: _____

Rechtsgrundlage: _____

Aufbewahrungsfrist Ergebnisse: _____

Backup-Aufbewahrungsfrist: _____

Datum / Unterschrift: _____