TECHNISCHE UND ORGANISATORISCHE BESTANDSAUFNAHME

Kando: Datenschutz- und Sicherheitskonzept

Prüfunterlage für Schulen, Schulträger und Datenschutzbeauftragte

Dokumentversion 1.0 · Prüfstand: 14. Juni 2026 · Kontakt: info@kandoapp.de

Einordnung

Dieses Dokument beschreibt den aktuell implementierten technischen Schutzstand. Es ersetzt keine rechtliche Freigabe durch die Schule, den Schulträger oder die zuständige Datenschutzaufsicht. Ob und unter welchen Bedingungen Kando eingesetzt werden darf, ist anhand des jeweiligen Landes- und Schulrechts zu entscheiden.

1. Zweck und Systemgrenzen

Kando unterstützt Lehrkräfte beim Erstellen, Verteilen, Durchführen, Korrigieren und Dokumentieren schulischer Tests. Schülerinnen und Schüler benötigen kein eigenes Benutzerkonto. Die Lehrkraft verwaltet Aufgaben, Tests, Lerngruppen und Ergebnisse in einem verschlüsselten Lehrkraftkonto.

- Lehrkraftbereich: persönliche Anmeldung, verschlüsselte Synchronisierung und lokale Bearbeitung.
- Schülerbereich: temporärer Zugriff auf einen konkreten Test über QR-Code oder manuellen Zugangscode.
- Testserver: kurzfristige, verschlüsselte Vermittlung von Test und Abgabe; keine serverseitige Notenberechnung.
- Ressourcenpool: getrennte fachliche Inhalte ohne zulässige Schülerpersonenbezüge; Sichtbarkeit privat, schulintern oder öffentlich.

2. Rollen und Verantwortlichkeiten

Rolle	Aufgabe und Verantwortung
Schule / Schulträger	Verantwortliche Stelle für Unterrichts-, Schüler-, Leistungs- und Förderdaten; legt Rechtsgrundlage, Zwecke, Zugriffsberechtigungen und Löschfristen fest.
Kando-Betreiber	Technischer Diensteanbieter. Bei Verarbeitung im Auftrag der Schule ist vor Produktivbetrieb ein Vertrag nach Art. 28 DSGVO erforderlich.
Lehrkraft	Nutzt Kando im Rahmen schulischer Vorgaben, pflegt nur erforderliche Daten, schützt Geräte und Exporte und setzt Löschfristen um.
Schülerinnen und Schüler	Betroffene Personen; benötigen kein Kando-Konto und erhalten einen persönlichen zufälligen Schülercode.

3. Verarbeitete Datenkategorien

Bereich	Daten	Schutz
Lehrkraftkonto	E-Mail-Adresse, Anzeigename, Authentifizierungs- und Sitzungsdaten	E-Mail serverseitig verschlüsselt; Passkey als regulärer Servernachweis; Sitzungstoken werden gehasht gespeichert.
Lerngruppen	Name, Nummer, Lerngruppe, optional LRS/LE	Teil der Ende-zu-Ende verschlüsselten Kontoeinstellungen; für den Betreiber nicht lesbar.
Testergebnisse	Antworten, Punkte, Prozentwert, Note oder Status ohne Benotung, Prüfungsereignisse	Lokal und in der Kontosynchronisierung AES-256-GCM-verschlüsselt; Bewertung erfolgt auf dem Lehrkraftgerät.
Temporäre Testsitzung	Verschlüsselter Test, verschlüsselte Abgabe, pseudonyme Versuchsdaten	Sitzungsschlüssel bleibt auf Endgeräten; automatische Löschung spätestens nach 24 Stunden.
Fachliche Ressourcen	Aufgaben, Tests, Vokabellisten, Tags	Serverseitige Rechteprüfung und PostgreSQL Row Level Security; keine Schülerdaten zulässig.

4. Schutzarchitektur

4.1 Verschlüsselte Kontosynchronisierung

Private Kontodaten werden auf dem Endgerät mit AES-256-GCM verschlüsselt. Der Server erhält ausschließlich Verschlüsselungsumschläge und keinen unverschlüsselten Kontoschlüssel. Der lokale Kontoschlüssel wird durch PIN beziehungsweise Wiederherstellungscode geschützt. Ergebnisse und sensible Einstellungen werden zusätzlich auch lokal in IndexedDB verschlüsselt gespeichert, sobald der Lehrkraftschlüssel verfügbar ist.

Zero-Knowledge-Ziel

Schülernamen, Nummern, Antworten, LRS-/LE-Status, Punkte und Noten sollen aus der privaten Kontosynchronisierung durch den Betreiber nicht rekonstruierbar sein. Der Verlust von PIN und Wiederherstellungscode kann deshalb zum Verlust der Entschlüsselungsmöglichkeit führen.

4.2 Schülercodes und Lerngruppen

Jeder Schüler erhält einen zufälligen persönlichen Code. Bei der Testverteilung wird nicht die offene Klassenliste übertragen. Jeder Identitätsdatensatz wird einzeln mit einem aus dem persönlichen Code abgeleiteten Schlüssel geschützt. Nach erfolgreicher Auflösung wird der Code nicht in der Ergebnisdatei gespeichert.

- PBKDF2-SHA-256 mit 50.000 Iterationen für die geschützte Code-Suche.
- AES-GCM für den einzelnen verschlüsselten Identitätsdatensatz.
- Zufällige interne Klassen- und Schüler-IDs statt sprechender Serverkennungen.
- LRS und LE werden auf dem Server nicht im Klartext gespeichert.

4.3 Testverteilung und Warteschleuse

Jede Testsession erhält einen eigenen zufälligen AES-GCM-Schlüssel. Der QR-Code wird lokal erzeugt und enthält einen HTTPS-Link mit Sitzungskennung und einem im Fragment transportierten Schlüssel.

URL-Fragmente werden bei normalen HTTP-Anfragen nicht an den Server übertragen. Es werden keine externen QR-, Kurzlink-, Analyse- oder Trackingdienste verwendet.

- Das Schülergerät wird vorübergehend für 90 Minuten an einen Versuch gebunden.
- Name und Nummer erscheinen in der Warteschleuse nur als verschlüsseltes Anzeigepaket, das die Lehrkraft lokal entschlüsselt.
- Die Lehrkraft kontrolliert den Versuch und gibt ihn einzeln oder gesammelt frei.
- Für LE-Schüler kann die Lehrkraft LE-Aufgaben, Regulär + LRS oder eine individuelle Aufgabenmenge wählen; die Abgabe bleibt technisch als ohne Benotung gekennzeichnet.
- Der Server speichert lediglich gehashte Gerätekennungen, pseudonyme Schülerreferenzen und verschlüsselte Inhalte.

4.4 Bewertung und sensible Fördermerkmale

Die automatische Korrektur sowie die Berechnung von Punkten, Prozenten und Noten erfolgen im Lehrkraftclient. Auf dem Testserver werden keine Noten berechnet. LE-Ergebnisse werden unabhängig von der gewählten Testvariante ohne Note gespeichert und angezeigt. Manuelle Punkteentscheidungen der Lehrkraft überschreiben die automatische Bewertung.

Besonderer Schutzbedarf

LRS- und LE-Zuordnungen können je nach Ausgestaltung Daten mit besonderem Schutzbedarf oder besondere Kategorien personenbezogener Daten berühren. Die Schule muss die einschlägige Rechtsgrundlage nach Landes- und Schulrecht sowie gegebenenfalls Art. 9 DSGVO prüfen.

5. Zugriffsschutz und Berechtigungen

- Verifizierte Lehrkraftkonten; reguläre Anmeldung mit Passkey, PIN nur für die lokale Entschlüsselung beziehungsweise den abgesicherten Ersteinrichtungsweg.
- Lehrkraft-Sitzungen sind widerrufbar; andere angemeldete Geräte können aus der Kontoverwaltung entfernt werden.
- WebApp-Sperre nach 15 Minuten Inaktivität; erneute Authentifizierung beim Zugriff auf den Lehrkraftbereich.
- Serverseitige Rollen Lehrkraft, Schuladmin und Systemadmin.
- Ressourcenzugriffe werden in Services und zusätzlich per PostgreSQL Row Level Security geprüft.
- Private, schulinterne und öffentliche Ressourcen werden auf Datenbankebene getrennt.
- Sicherheitsheader, Größenbegrenzungen, Eingabevalidierung und rate-limitierte sensible Abläufe.

6. Löschung und Aufbewahrung

Datenbereich	Aktueller Mechanismus
Temporäre Testsession	Löschung durch Lehrkraft beim Schließen; automatische Löschung spätestens nach 24 Stunden.
Ergebnisse im Konto	Schulisch festzulegende Frist; Erinnerung, berechnetes Löschdatum und optional automatische Löschung verschlüsselter Ergebnisse.
Gelöschte Datensätze	Minimaler Löschmarker mit zufälliger Datensatz-ID und Zeitstempel kann verbleiben, damit Offline-Geräte gelöschte Inhalte nicht wiederherstellen.
Exporte	PDF-, CSV- und AirDrop-Dateien liegen außerhalb der automatischen Löschkontrolle und müssen schulisch verwaltet und gelöscht werden.
Konto	Löschfunktion für Kontodaten; Backup- und Supportfristen müssen im betrieblichen Löschkonzept festgelegt werden.

7. Technische und organisatorische Maßnahmen (TOM)

Schutzziel	Maßnahmen im System	Schulische Ergänzung
Vertraulichkeit	AES-GCM, Passkey, verschlüsselte Schülerverzeichnisse, pseudonyme Serverreferenzen, RLS	Gerätecode, MDM, Rollenvergabe, keine privaten Cloud-Exporte
Integrität	Authentifizierte Verschlüsselung, Transaktionen, Constraints, Audit-Logs für Ressourcen	Plausibilitätskontrolle, dokumentierte Korrektur- und Freigabeprozesse
Verfügbarkeit	Serverüberwachung, temporärer AirDrop-Fallback, lokale Offline-Daten	Backupkonzept, Wiederanlaufplan, geregelte Verantwortlichkeiten
Belastbarkeit	Größenlimits, Sitzungsablauf, Gerätesperre, Test- und Szenariosimulationen	Pilotbetrieb, Störungsprozess, regelmäßige Überprüfung
Löschbarkeit	Fristenmodell, automatische Löschung, Löschmarker	Verbindliche Fristen und Kontrolle externer Exporte

8. Datenflüsse

1. Die Lehrkraft meldet sich an und entschlüsselt den privaten Kontoschlüssel lokal.
2. Aufgaben, Tests, Einstellungen und Ergebnisse werden lokal bearbeitet und verschlüsselt synchronisiert.
3. Für einen Test wird ein eigener Sitzungsschlüssel erzeugt; der Server erhält nur den verschlüsselten Test.
4. Der Schüler öffnet den Test über QR-Code oder manuellen Zugangscode und identifiziert sich mit seinem persönlichen Schülercode.
5. Die Lehrkraft prüft den wartenden Versuch und legt bei Bedarf die Testvariante fest.
6. Die Abgabe wird auf dem Schülergerät verschlüsselt und temporär auf dem Server abgelegt.
7. Die Lehrkraft lädt die verschlüsselte Abgabe, entschlüsselt und bewertet sie lokal und synchronisiert das Ergebnis erneut verschlüsselt.

9. Restrisiken und Grenzen

- Ende-zu-Ende-Verschlüsselung schützt Inhalte, verhindert aber nicht alle Metadaten wie Zeitpunkt, IP-Adresse oder technische Geräteinformationen in Webserverprotokollen.
- Ein entsperrtes oder kompromittiertes Lehrkraftgerät kann Klartextdaten anzeigen; Geräteschutz bleibt daher wesentlich.
- PDF-, CSV- und AirDrop-Exporte können personenbezogene Daten enthalten und liegen außerhalb der automatischen Kontolöschung.
- Die korrekte Zuordnung der schulrechtlichen Rechtsgrundlage und der besondere Umgang mit LRS-/LE-Daten sind organisatorische Aufgaben der Schule.
- Das System ersetzt keine Aufsicht während einer Prüfung und kann missbräuchliches Verhalten nur begrenzt technisch erkennen.
- Vor Produktivbetrieb sind Hosting, Unterauftragsverarbeiter, Backupfristen, Incident-Prozess und AV-Vertrag verbindlich zu dokumentieren.

10. Prüfliste vor schulischem Produktivbetrieb

Prüfpunkt	Verantwortlich	Status
Rechtsgrundlage nach Landes- und Schulrecht festgelegt	Schule / DSB	☐
Umgang mit LRS-/LE-Daten nach Art. 9 DSGVO geprüft	Schule / DSB	☐
Vertrag zur Auftragsverarbeitung und Unterauftragsverarbeiter geprüft	Schulträger	☐
Verzeichnis der Verarbeitungstätigkeiten ergänzt	Schule	☐
Lösch- und Aufbewahrungsfristen festgelegt und in Kando eingestellt	Schule	☐
Erforderlichkeit einer Datenschutz-Folgenabschätzung dokumentiert	DSB	☐
Eltern- und Schülerinformation freigegeben	Schule	☐
Berechtigungs-, Geräte-, Export- und Incident-Prozess festgelegt	Schule / IT	☐
Pilotbetrieb mit Testdaten durchgeführt	Projektleitung	☐

11. Rechts- und Referenzgrundlagen

- Datenschutz-Grundverordnung, insbesondere Art. 5, 6, 9, 12-14, 25, 28, 30, 32, 33-35: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679
- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Muss-Liste zur Datenschutz-Folgenabschätzung, Version 1.1.
- Jeweils einschlägiges Landesdatenschutz-, Schul- und Prüfungsrecht sowie Vorgaben des zuständigen Schulträgers.
- Kando-Datenschutzerklärung und Nutzungsbedingungen in der jeweils veröffentlichten Fassung unter https://kandoapp.de.

Empfohlene nächste Unterlagen

Für eine schulische Freigabe sollten zusätzlich ein AV-Vertrag einschließlich TOM-Anlage, eine Liste der Unterauftragsverarbeiter, ein betriebliches Lösch- und Backupkonzept, ein Verfahren für Datenschutzverletzungen sowie eine ausgefüllte DSFA-Vorprüfung bereitgestellt werden.