



TECHNISCHE UND ORGANISATORISCHE BESTANDSAUFNAHME

Kando: Datenschutz- und Sicherheitskonzept

Prüfunterlage für Schulen, Schulträger und Datenschutzbeauftragte

Dokumentversion 1.6 · Prüfstand: 8. Oktober 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, Üben und Dokumentieren schulischer Tests und Lernchecks. Schülerinnen und Schüler benötigen kein eigenes Benutzerkonto. Die Lehrkraft verwaltet Aufgaben, Tests, Lerngruppen, Übungsfreigaben 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.
- Übungsbereich: verschlüsselte Freigabe ausgewählter Tests als Karteikarten-, Schreib- oder Auswahlübung über persönliche Schülercodes.
- Live-Runde: gemeinsames Vokabelquiz im Unterricht am Beamer; Schülergeräte treten per QR-Code mit einem Spielnamen bei, ohne Namen, Schülercode oder Konto. Nichts wird dauerhaft gespeichert.
- Ressourcenpool: getrennte fachliche Inhalte ohne zulässige Schülerpersonenbezüge; Sichtbarkeit privat, schulintern oder öffentlich.
- Betreiberbereich: Verwaltung von Lehrkraftkonten, Schulen, Testkonto und Audit-Export ausschließlich für Systemadministration.
- Teamarbeit an Tests: Lehrkräfte derselben Schule können namentlich zur Mitarbeit an einem Test eingetragen werden. Geteilt werden ausschließlich fachliche Testinhalte; Lerngruppen, Schülerdaten und Ergebnisse bleiben im verschlüsselten Konto der jeweiligen Lehrkraft.

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. Verwaltet Betrieb, Lehrkraftkonten, Schulstammdaten, Backup-/Restore-Prozess und sicherheitsrelevante Auditdaten. 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, Anzeigenname, Authentifizierungs- und Sitzungsdaten	E-Mail serverseitig verschlüsselt; Passkey als regulärer Servernachweis; Sitzungstoken werden gehasht gespeichert.
Lerngruppen	Name, Nummer, Lerngruppe, optional individuelle Ausgleichs- und Förderoptionen	Teil der Ende-zu-Ende verschlüsselten Kontoeinstellungen; für Dritte nicht lesbar. Der Betreiber kann sie allein über den Wiederherstellungsumschlag öffnen, siehe 4.1.
Testergebnisse	Antworten, Punkte, Prozentwert, Note oder Status ohne Benotung, Prüfungsergebnisse	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.
Übungsfreigaben	Verschlüsseltes Übungspaket, Schülercode-Zuordnung, lokale Fehlerhistorie	Zugriff nur mit persönlichem Schülercode; Fehlerhistorie wird auf dem Schülergerät pro Schülercode getrennt gespeichert.
Live-Runde	Verschlüsseltes Fragenpaket, Spielname (vorgegeben oder frei gewählt), verschlüsselte Antworten mit Eingangszeit	Nur im Arbeitsspeicher des Servers, Schlüssel nur im QR-Link; Wertung auf dem Lehrkraftgerät; Löschung beim Schließen, spätestens nach drei Stunden.
Fachliche Ressourcen	Aufgaben, Tests, Vokabellisten, Tags, Kontextsätze und Tatoeba-Quellenangaben	Serverseitige Rechteprüfung und PostgreSQL Row Level Security; keine Schülerdaten zulässig. Tatoeba-Suche läuft gegen lokal gespeicherten Korpus.
Betrieb und Administration	Kontostatus, Schulmitgliedschaften, Auditereignisse, Backup-Manifest	Zugriff nur für berechtigte Schuladmins beziehungsweise Systemadmins; Audit-Export für Rechenschaft und Missbrauchsprüfung.
Rückmeldungen aus der App	Anzeigenname, Konto-E-Mail und freier Text eines Verbesserungsvorschlags	Wird auf dem Kando-Server abgelegt und zusätzlich an das Betreiberpostfach gesendet. Keine Schülerdaten; die Lehrkraft entscheidet selbst, was sie schreibt.
Anonyme Nutzungsstatistiken	Genutzte Funktionen, aufgerufene Seiten, Fehlertypen, Plattform und App-Version	Ohne Namen, E-Mail-Adressen, Schüler- oder Inhaltsdaten und ohne IP-Adressen oder Gerätekennungen. Nur nach Zustimmung der Lehrkraft (§ 25 TDDDG), in den App-Einstellungen jederzeit widerrufbar.

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. Einer dieser Umschläge dient der Kontowiederherstellung und ist mit einem serverseitigen Hauptschlüssel gesichert; er wird bei der Anmeldung automatisch angelegt. Der lokale Kontoschlüssel wird durch das Kontopasswort beziehungsweise den Notfallschlüssel geschützt. Das Passwort umfasst mindestens zehn Zeichen; bei Konten aus der früheren PIN-Fassung gilt der bisherige sechsstelligen PIN einmalig als aktuelles Passwort. Ergebnisse und sensible Einstellungen werden zusätzlich auch lokal in IndexedDB verschlüsselt gespeichert, sobald der Lehrkraftschlüssel verfügbar ist.

Grenze der Verschlüsselung

Schülernamen, Nummern, Antworten, individuelle Ausgleichsoptionen, Punkte und Noten liegen auf dem Server ausschließlich verschlüsselt. Rekonstruierbar sind sie jedoch über den Wiederherstellungsumschlag: Wer Zugriff auf den Server und dessen Hauptschlüssel hat, kann den Kontoschlüssel gewinnen. Ein Abzug der Datenbank allein genügt dafür nicht, da Kontoprofile und Hauptschlüssel getrennt davon auf dem Server liegen. Der Betreiber ist damit technisch in der Lage, private Kontodaten zu entschlüsseln; organisatorisch ist dieser Weg auf die Wiederherstellung eines Kontos beschränkt.

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.
- Individuelle Ausgleichs- und Förderoptionen 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 Schülerinnen und Schüler mit zieldifferenter Aufgabenstellung kann die Lehrkraft eine individuelle Aufgabenvariante 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, Prozentsätzen und Noten erfolgen im Lehrkraftclient. Auf dem Testserver werden keine Noten berechnet. Ergebnisse mit zieldifferenter Aufgabenstellung werden unabhängig von der gewählten Testvariante ohne Note gespeichert und angezeigt. Manuelle Punkteentscheidungen der Lehrkraft überschreiben die automatische Bewertung.

Besonderer Schutzbedarf

Kando speichert keine Diagnosebezeichnung als Pflichtangabe, sondern technische Ausgleichsoptionen wie Zeitverlängerung, erweiterte Rechtschreibtoleranz, größere Eingabefelder, Vorlesen oder zieldifferente Aufgabenvarianten. Diese Angaben können je nach schulischem Einsatz dennoch Rückschlüsse auf Gesundheit, Behinderung oder Förderbedarf erlauben. Die Schule muss daher die einschlägige Rechtsgrundlage nach Landes- und Schulrecht sowie gegebenenfalls Art. 9 DSGVO prüfen.

4.5 Übungsfreigaben und lokale Fehlerhistorie

Lehrkräfte können Tests zusätzlich als Übungspakete freigeben. Die Freigabe enthält den verschlüsselten Testinhalt und verschlüsselte Schülercode-Zuordnungen. Schülerinnen und Schüler öffnen die Übung mit ihrem persönlichen Code; ein eigenes Konto ist nicht erforderlich.

- Übungen können als Schreiben, Karteikarten oder Auswahlaufgaben ausgeführt werden; Multiple Choice und True/False werden ohne Notenbildung geübt.
- Die individuelle Fehlerhistorie wird lokal im Browser oder in der App pro Schülercode getrennt gespeichert, damit auf demselben Gerät nicht die Fehler eines anderen Kindes angezeigt werden.
- Die Übungsfunktion ist nicht als Leistungsbewertung konzipiert. Sie erzeugt keine serverseitige Note und ersetzt keine schulische Korrekturentscheidung.

4.6 Beispielsätze und Tatoeba-Korpus

Kando kann Lehrkräften beim Erstellen von Vokabelaufgaben passende Beispielsätze aus einem lokal auf dem Kando-Server gespeicherten Tatoeba-Korpus vorschlagen. Dabei werden keine Suchanfragen an Tatoeba oder andere externe Dienste weitergeleitet.

- Gespeichert werden Satztext, Sprachkennung, Satz-ID, Erstellernamen und Lizenzhinweis gemäß CC BY 2.0 FR.
- Bei Veröffentlichung oder Nutzung eines Tatoeba-Satzes wird der Lizenzhinweis in der App angezeigt.
- Der Korpus darf keine Schülerdaten enthalten und ist fachlicher Inhalt, nicht Teil der privaten Schülerdatensynchronisierung.

4.7 Live-Runde im Unterricht

Die Lehrkraft kann aus einem Test eine Live-Runde starten: Die Klasse beantwortet gemeinsam Vokabelfragen, die am Beamer erscheinen, auf ihren Geräten. Die Runde ist ein Spiel zur Wiederholung und keine Leistungsfeststellung; Ergebnisse gelangen nicht in die Ergebnisverwaltung.

- Schülergeräte öffnen die Runde direkt über einen QR-Code. Sie geben weder Namen noch Schülercode ein und brauchen kein Konto.
- Jedes Gerät erhält einen Spielnamen. Voreingestellt wählt das Kind einen von drei vorgeschlagenen Namen in der Fremdsprache mit deutscher Übersetzung (zum Beispiel „Brave Fox – Mutiger Fuchs“). Die Lehrkraft kann freie Spielnamen zulassen; diese werden auf Länge, Zeichen und anstößige Wörter geprüft, und die Lehrkraft kann Teilnehmende aus der Runde entfernen.
- Fragen, Auflösungen und Antworten werden auf den Geräten mit einem zufälligen Rundenschlüssel (AES-256-GCM) verschlüsselt. Der Schlüssel steht nur im Fragment des QR-Links und erreicht den Server nicht. Der Server vermittelt ausschließlich verschlüsselte Inhalte und misst die Eingangszeit einer Antwort.
- Gewertet wird auf dem Gerät der Lehrkraft. Am Beamer erscheinen höchstens die fünf Besten mit Spielnamen; jedes Kind sieht nur das eigene Ergebnis, den eigenen Platz nur unter den besten fünf. Rangliste und Zeitwertung sind abschaltbar.
- Die Runde liegt nur im Arbeitsspeicher des Servers und wird beim Schließen, spätestens drei Stunden nach dem Start, gelöscht; ein Serverneustart beendet sie. Die Auswertung je Vokabel enthält keine Spielnamen und bleibt auf dem Lehrkraftgerät.
- Auf Schülergeräten findet keine Nutzungsstatistik statt.

5. Zugriffsschutz und Berechtigungen

- Verifizierte Lehrkraftkonten; reguläre Anmeldung mit Passkey oder Passwort, das Passwort zusätzlich für die lokale Entschlüsselung.
- 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.
- Schulmitgliedschaften können angefragt und durch Schuladmins angenommen oder abgelehnt werden; neue Schulen werden durch das Betreiberteam angelegt.
- Mehrere Lehrkräfte derselben Schule können an einem Test zusammenarbeiten. Die Eigentümerin trägt sie einzeln ein; sie dürfen Aufgaben und Einstellungen ändern, den Test aber weder löschen noch weitergeben und seine Sichtbarkeit nicht ändern. Schuladmins erhalten über ihre Rolle keinen inhaltlichen Zugriff auf fremde Tests.
- Das Verteilen bleibt Sache der einzelnen Lehrkraft: Mitarbeitende sehen weder die Testsitzungen noch die Abgaben oder Ergebnisse der anderen. Jede Sitzung ist an die verteilende Lehrkraft gebunden und nur mit deren Sitzungsnachweis abrufbar.
- Systemadmins können Lehrkraftkonten sperren, anonymisieren/löschen, Schulen verwalten, Testkonten erneuern und Auditdaten exportieren.
- 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-, JSON- und AirDrop-Dateien liegen außerhalb der automatischen Löschkontrolle und müssen durch die Schule auf schulisch freigegebenen Speicherorten geschützt, verwaltet und nach den festgelegten Löschfristen eigenständig gelöscht werden.
Konto	Löschfunktion für Kontodaten; Backup- und Supportfristen müssen im betrieblichen Löschkonzept festgelegt werden.
Übungsfreigaben	Zeitlich befristete Freigaben; lokale Fehlerdaten bleiben auf dem Schülergerät und können durch Browser-/App-Datenlöschung entfernt werden.
Live-Runde	Nur im Arbeitsspeicher; Löschung beim Schließen durch die Lehrkraft, nach Spielende spätestens nach zehn Minuten, insgesamt spätestens drei Stunden nach dem Start.
Rückmeldungen aus der App	Aufbewahrung bis zur Bearbeitung des Vorschlags, längstens 24 Monate; Löschung auf Wunsch jederzeit.
Anonyme Nutzungsstatistiken	Ohne Personenbezug; nur nach Zustimmung, jederzeit in den App-Einstellungen widerrufbar. Bereits übertragene Werte sind keiner Person zuzuordnen und daher nicht einzeln löschar.

6.1 Backup, Restore und Betriebsmonitoring

Für den Produktivbetrieb ist ein wöchentliches verschlüsseltes Backup vorgesehen. Der aktuelle technische Stand enthält Skripte für PostgreSQL-Dump, Dateidaten, verschlüsselte Archivierung, Aufbewahrungsfrist und einen Restore-Test gegen eine getrennte Testdatenbank.

- Backup-Archiv: AES-256-CBC mit PBKDF2 und mindestens 32 Zeichen langer Passphrase; Ablage standardmäßig unter /var/backups/kando.
- Zeitplan: systemd-Timer kando-backup.timer, wöchentlich sonntags; Betriebsmonitor kando-monitor.timer prüft Webserver, Kando-Server, PostgreSQL und Healthcheck.
- Optionales externes Ziel: BACKUP_REMOTE, zum Beispiel ein Strato-Speicher in einem deutschen Rechenzentrum.
- Restore-Test: regelmäßige Wiederherstellung in kando_restore_test; keine Wiederherstellung direkt in die Produktivdatenbank ohne vorherigen Test.
- Backups enthalten verschlüsselte private Daten, technische Kontodaten, fachliche Ressourcen und Auditdaten. Sie sind trotz Inhaltsverschlüsselung als personenbezogenes Sicherheitsbackup zu behandeln.

7. Technische und organisatorische Maßnahmen (TOM)

Schutzziel	Maßnahmen im System	Schulische Ergänzung
Vertraulichkeit	AES-GCM, Passkey, verschlüsselte Schülerverzeichnisse, pseudonyme Serverreferenzen, RLS, vollständige Räumung kontobezogener Daten beim Lehrkraftwechsel auf demselben Gerät	Gerätecode, MDM, Rollenvergabe, keine privaten Cloud-Exporte, keine unverschlüsselten USB-Sticks
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, regelmäßige Kontrolle externer Exporte und schulische Löschverantwortung

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.
8. Für Übungsfreigaben öffnet der Schüler das freigegebene Paket mit seinem Schülercode; die Fehlerwiederholung bleibt lokal pro Schülercode getrennt.

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-, JSON- und AirDrop-Exporte können personenbezogene Daten enthalten und liegen außerhalb der automatischen Kontolöschung. Kando kann solche externen Kopien technisch nicht automatisch löschen.
- Die korrekte Zuordnung der schulrechtlichen Rechtsgrundlage und der besondere Umgang mit Ausgleichs- und Förderoptionen 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, AV-Vertrag sowie schulische Export- und Löschprozesse verbindlich zu dokumentieren.
- Übungsdaten auf Schülergeräten können außerhalb des Lehrkraftkontos lokal verbleiben, bis Browser- oder App-Daten gelöscht werden.

10. Prüfliste vor schulischem Produktivbetrieb

Prüfpunkt	Verantwortlich	Status
Rechtsgrundlage nach Landes- und Schulrecht festgelegt	Schule / DSB	☐
Umgang mit Ausgleichs- und Förderoptionen nach Schulrecht und gegebenenfalls 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	☐
Backupziel, Backup-Passphrase, Restore-Test und Aufbewahrungsfrist dokumentiert	Betreiber / Schule	☐
Umgang mit Übungsfreigaben und lokalen Übungsdaten auf Schülergeräten kommuniziert	Schule	☐
Speicherorte für Exporte auf schulische Systeme beschränkt und Löschung externer PDF-/CSV-Dateien geregelt	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, Vorgaben für externe Exporte sowie eine ausgefüllte DSFA-Vorprüfung bereitgestellt werden.