



Datenschutz und technische Datenflüsse

Technisches Whitepaper für öffentliche Schulen in Baden-
Württemberg

Version 1.6.0 · 13. September 2026

Herausgeber und Urheber: mct Datensysteme GmbH, Karlsruhe

ENTSCHEIDUNGSVORLAGE

Die Kernaussage

Notentia ist für lokale, verschlüsselte Schuldokumentation konzipiert – ohne zentrale Fachcloud und ohne laufende Datenübermittlung.

Kurzfassung für Entscheidungsträger

Personenbezogene Schuldaten bleiben auf dem Datenträger der Lehrkraft. Im normalen Arbeitsbetrieb gibt es keinen externen Datenfluss. Lizenzierung und Update werden nur bewusst ausgelöst. Zur Lizenz- und Updateberechtigung werden pseudonyme Instanzdaten, öffentlicher Schlüssel und Programmversion übertragen, jedoch kein Schul- oder Lehrkraftname im Klartext und kein Inhalt aus Schülerakten.

LOKAL

Rust-Server ausschließlich auf 127.0.0.1; keine Erreichbarkeit aus Schulnetz oder Internet.

VERSCHLÜSSELT

SQLCipher-Datenbank; Gesprächsanhänge als verschlüsselte BLOBs innerhalb der Datenbank.

DATENARM

Keine Telemetrie, Werbung, Analyse, Cloud-Synchronisierung, CDNs oder externen Schriftarten.

Was dieses Dokument leistet

Es beschreibt nachvollziehbar Datenkategorien, technische Grenzen, externe Kontakte und organisatorische Voraussetzungen. Es ist als Grundlage für Datenschutzprüfung, Verzeichnis von Verarbeitungstätigkeiten und Freigabeprozesse geeignet.

Was dieses Dokument nicht leistet

Es ist keine Rechtsberatung, Zertifizierung oder Freigabe durch das Ministerium für Kultus, Jugend und Sport Baden-Württemberg. Rechtsgrundlage, Erforderlichkeit, Aufbewahrung und Gerätefreigabe bleiben von der verantwortlichen Schule beziehungsweise ihrem Träger zu prüfen.

Bewertung in einem Satz

Notentia minimiert externe Risiken durch eine lokale Architektur; sicherer Betrieb setzt trotzdem starkes Passwort, getrennten Recovery-Code, freigegebene Geräte und eine zweite verschlüsselte Sicherung voraus.

DATENFLUSS 1

Die Datenschutzgrenze ist sichtbar

Lehrkraft Bedient Notentia bewusst am eigenen Rechner.	→ Lokale Oberfläche Mitgeliefertes Chromium ohne Sync und Erweiterungen.	→ Lokaler Server Nur 127.0.0.1; keine Freigabe im Netzwerk.	→ Verschlüsselte DB Datensatz und Anhänge auf Stick oder Arbeitskopie.
--	--	---	--

Diese Inhalte bleiben innerhalb der Grenze

Datenart	Speicherort	Externer Versand
Schüler- und Klassendaten	SQLCipher-Datenbank	Nein
Noten und Leistungen	SQLCipher-Datenbank	Nein
Beobachtungen und Aufgaben	SQLCipher-Datenbank	Nein
Gesprächsnotizen und Anhänge	verschlüsselte DB/BLOB	Nein
Masterpasswort und Schlüssel	lokale Ableitung/Arbeitsspeicher	Nein
Schulname und Lehrkraft	Manifest zur Zuordnung	Nein; vor Entsperren sichtbar

Bewusst erzeugte Excel- und PDF-Exporte liegen außerhalb dieser Schutzgrenze. Sie sind Klartextdateien und müssen durch geeigneten Speicherort, Berechtigungen und Löschregeln separat geschützt werden.

DATENFLUSS 2

Wenn ein USB-Stick verloren geht

Vertraulichkeit und Verfügbarkeit sind zwei verschiedene Schutzziele.

1 · FUND

Eine fremde Person besitzt den Datenträger physisch.

2 · SPERRE

Ohne Masterpasswort oder Recovery-Code bleibt die SQLCipher-Datenbank unlesbar.

3 · WIEDERANLAUF

Eine getrennte verschlüsselte Sicherung ermöglicht die Wiederherstellung auf einem neuen Datenträger.

Was geschützt ist

- Schülerdaten, Noten, Beobachtungen, Gespräche, Aufgaben und Anhänge innerhalb der Datenbank.
- Der private Instanzschlüssel für die Lizenzbindung; er liegt ebenfalls in der verschlüsselten Datenbank.
- Widerrufene pseudonyme Zuordnungsprüfwerte; sie verhindern die Reaktivierung einer früheren Lizenzzuordnung.
- Notentia-Sicherungsdateien; sie enthalten den bereits verschlüsselten Datensatz.

Was bewusst sichtbar oder außerhalb liegt

- Schulname und Lehrkraft im Manifest, damit ein gesperrter Datensatz zugeordnet werden kann.
- Programmdateien, Versionsnummer und Diagnoseprotokolle ohne Schülerdaten, Passwörter oder Schlüssel.
- Vom Benutzer erstellte Excel- und PDF-Exporte; deren Schutz liegt beim gewählten Zielsystem.

Wichtig

Verschlüsselung verhindert nicht den Verlust der einzigen Kopie. Notentia erinnert deshalb an regelmäßige, geprüfte Sicherungen auf einem zweiten physischen Datenträger.

EXTERNE KONTAKTE

Zwei bewusste Wege nach außen

A · Lizenzierung

Einstellungen Lehrkraft klickt auf Lizenzportal öffnen.	→ Technischer Nachweis Instanz-ID, Version, öffentlicher Schlüssel, HMAC-Prüfwert, Signatur.	→ Lizenzportal Pseudonyme Anfrage; keine Klartextnamen, E-Mail-Adressen oder Schülerdaten.	→ Statusprüfung Nur nach Klick: Notentia lädt das signierte Bundle und prüft es lokal.
---	--	--	--

Bindung ohne Klartextnamen

Notentia bildet lokal HMAC-SHA-256 über Schulname und Lehrkraft. Schlüssel ist der private Instanzschlüssel in der verschlüsselten Datenbank. Das Portal erhält nur den Base64url-codierten Prüfwert und kann die Namen ohne diesen geheimen Schlüssel weder zurückrechnen noch selbst durch eine Wörterbuchprüfung testen. Der Prüfwert wird in Aktivierungsnachweis und Lizenzbundle signiert. Er ist trotzdem als pseudonymisiertes Datum zu behandeln. Bei jeder Änderung speichert Notentia den bisherigen Prüfwert in einer Widerrufsliste innerhalb der SQLCipher-Datenbank. Auch Zurückändern reaktiviert die frühere Lizenz nicht; der Anbieter muss sie neu ausstellen beziehungsweise übertragen.

Grenze der Bindung: Eine vollständige Sicherungs- oder Arbeitskopie übernimmt Datenbank, privaten Instanzschlüssel und Zuordnung. Sie besitzt damit absichtlich dieselbe Lizenzidentität. Das Verfahren verhindert das bloße Umbenennen oder isolierte Übertragen der Lizenz, nicht jedoch das identische Klonen des gesamten verschlüsselten Datensatzes.

B · Programmaktualisierung

Einstellungen Lehrkraft klickt auf Nach Updates suchen.	→ Signierter Nachweis Instanz-ID, installierte Version, öffentlicher Schlüssel und pseudonyme Bindung.	→ Lizenzportal Prüft die gültige Lizenz und gibt einen kurzlebigen Updatezugriff frei.	→ Update-Gateway Manifest und passende Programmpaket e per HTTPS; direkter Zugriff ist gesperrt.	→ Lokale Prüfung Größe, SHA-256, zulässige Dateien und Plattform.	→ Neustart Nur Programm und Weboberfläche werden ersetzt.
---	--	--	--	---	---

Lizenzgebundener Abruf

Bei jeder bewusst gestarteten Updateprüfung aktualisiert das Portal die bei der pseudonymen Instanz hinterlegte Programmversion. Ohne passende Instanzsignatur und aktuell gültige Lizenz werden weder Manifest noch Updatepakete ausgeliefert. Das Zugriffstoken ist auf zehn Minuten begrenzt; Schülerdaten, Klartextnamen, Masterpasswort und Datenbankschlüssel sind nicht Bestandteil des Abrufs.

Transparenzhinweis zu IP-Adressen

Bei jedem Webabruf wird die Quell-IP technisch an den Zielserver übertragen. Caddy-Sicherheitsprotokolle werden begrenzt rotiert und zur Erkennung wiederholter 401/403/404-Angriffe mit Fail2ban ausgewertet. Fachliche Schuldaten sind nicht Bestandteil dieser Requests.

TECHNISCHES SCHUTZKONZEPT

Schutz in mehreren Schichten

Schicht	Maßnahme	Schutzziel
Speicherung	SQLCipher-verschlüsselte SQLite-Datenbank	Vertraulichkeit bei Medienverlust
Anhänge	BLOB in der DB; zusätzliche authentifizierte Verschlüsselung	Keine losen Gesprächsdateien
Schlüssel	Passwortbasierte Ableitung; privater Lizenzschlüssel lokal	Schlüssel verlassen den Datensatz nicht
Netzwerk	Bindung ausschließlich an 127.0.0.1	Keine Erreichbarkeit aus LAN/Internet
Browser	Mitgeliefertes Chromium ohne Sync/Erweiterungen	Reduzierte externe Angriffsfläche
Sitzung	Sperre bei Inaktivität; Ende bei Browserabbruch	Begrenzter Zugriff am Gerät
Integrität	Transaktionen, Rücksetzjournal, Integritätsprüfung	Widerstand gegen abgebrochene Schreibvorgänge
Update	HTTPS, feste Herkunft, SHA-256, Pfad-Whitelist	Erkennung fehlerhafter Pakete
Lizenz	Ed25519-Signatur; HMAC-Bindung und verschlüsselte Widerrufshistorie	Offline prüfbare Berechtigung ohne Klartextnamen im Portal

Die Schutzwirkung hängt vom Endgerät ab. Schadsoftware mit Zugriff nach dem Entsperren, Bildschirmaufnahmen, gemeinsam genutzte Konten oder ein offengelegtes Passwort können nicht allein durch Notentia verhindert werden.

Anknüpfung an geltende Datenschutzprinzipien

Die DSGVO verlangt unter anderem Zweckbindung und Datenminimierung (Art. 5), Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25) sowie angemessene technische und organisatorische Maßnahmen einschließlich Verschlüsselung (Art. 32). Notentias Architektur unterstützt diese Prinzipien, ersetzt aber nicht die schulische Prüfung des konkreten Verfahrens.

Anforderung / Orientierung	Beitrag von Notentia
Datenminimierung	Kein zentrales Schülerkonto; keine Telemetrie; pseudonyme technische Lizenzkennungen ohne Klartextnamen.
Privacy by Design / Default	Lokale Bindung, verschlüsselte Standardspeicherung, bewusst ausgelöste externe Kontakte.
Sicherheit der Verarbeitung	Verschlüsselung, Sitzungsgrenzen, geprüfte Backups, sichere Updateprüfung.
VwV Datenschutz an öffentlichen Schulen	Technische Grundlage für ein lokal betriebenes Verfahren; Verantwortung und Dokumentation verbleiben bei der Schule.
Private Datenverarbeitungsgeräte	Verschlüsselte Speicherung unterstützt die geforderte Absicherung; Gerätefreigabe und organisatorische Vorgaben bleiben zwingend.
Verzeichnis von Verarbeitungstätigkeiten	Dieses Whitepaper liefert technische Angaben, ersetzt aber nicht das schulische VVT.
Keine behauptete Behördenfreigabe Aus der technischen Einordnung folgt weder eine automatische Zulässigkeit noch eine Empfehlung oder Zulassung durch das Kultusministerium Baden-Württemberg.	

BETRIEBSKONZEPT

Technik und Organisation greifen ineinander

Vor Einsatz

Zweck, Rechtsgrundlage, erforderliche Felder, Löschfristen, VVT, Geräte- und USB-Nutzung mit Schulträger/Datenschutz abstimmen.

Passwort

Persönlichen, langen Merksatz verwenden; nicht mit Namen, Schulbezug oder bekannten Zitaten bilden.

Recovery

Recovery-Code getrennt vom Stick ausdrucken und verschlossen verwahren; Zugriff organisatorisch regeln.

Sicherung

Mindestens wöchentlich beziehungsweise nach wesentlichen Änderungen auf einen zweiten physischen Datenträger sichern und Wiederherstellung erproben.

Exporte

Excel/PDF nur bei Bedarf erzeugen, am freigegebenen Ziel speichern und nach Zweckfortfall löschen.

Arbeitsplatz

Bildschirm sperren, Notentia schließen, Stick sicher auswerfen; keine parallele Nutzung mehrerer Kopien.

Verlust/Vorfall

Schulischen Meldeweg unverzüglich nutzen; beurteilen, welche sichtbaren oder exportierten Daten betroffen sein könnten.

Schuljahresende

Aufbewahrung und Löschung nach schulischen Vorgaben durchführen; Archivierung nicht mit unbegrenzter Speicherung verwechseln.

Empfohlene Freigabeunterlagen

Verfahrensbeschreibung/VVT, Rollen- und Berechtigungskonzept, Lösch- und Sicherungskonzept, dokumentierte Gerätefreigabe, Unterweisung der Lehrkräfte sowie dieses technische Whitepaper.

Quellen, Kontakt und Versionsstand

Primärquellen

- [Datenschutz-Grundverordnung, insbesondere Art. 5, 25 und 32](#)
- [EDPB Guidelines 01/2025 on Pseudonymisation](#)
- [VwV Datenschutz an öffentlichen Schulen Baden-Württemberg](#)
- [Pflichten der verantwortlichen öffentlichen Schule](#)
- [Verzeichnis der Verarbeitungstätigkeiten](#)
- [Private Datenverarbeitungsgeräte](#)
- [Cloudbasierte Dienste](#)

Herausgeber, Urheber und Kontakt

mct Datensysteme GmbH
Auf der Breit 19
76227 Karlsruhe
Telefon +49 721 46 47 12-0
E-Mail vertrieb@mct-datensysteme.de
<https://mct-datensysteme.de>

Dokumentstatus

Produktstand: Notentia 1.6.0
Dokumentstand: 13. September 2026
Lizenz- und Update-Infrastruktur: lizenz.notentia.de und notentia.de
© 2026 mct Datensysteme GmbH. Alle Rechte vorbehalten.

Pflegehinweis

Das Dokument ist bei wesentlichen Änderungen an Datenmodell, Verschlüsselung, externen Datenflüssen, Update- oder Lizenzverfahren zu aktualisieren.