

Datenschutzkonzept

Lokale Schulversion

Verarbeitung, Schutz und Rechte

Keine gespeicherten Tonaufnahmen. Keine Stimmprofile.

Namen aus der Klasse, private Aussagen und fachfremde Bemerkungen werden vor der Ablage der Lernnotizen gefiltert. Die Durchsicht durch Lehrkräfte ist optional.

Alle Dateien und Daten der lokalen Schulinstallation sind bei Speicherung und Übertragung verschlüsselt. Die Schule bestimmt die Speicherdauer der Lerninhalte; Standard ist ein Schuljahr.

Dieses Dokument beschreibt die **lokale Schulversion von ContextFriend**: Verarbeitung, Schutzmaßnahmen und Rechte. Bei der Einrichtung an einer Schule wird jede Installation anhand dieses Konzepts geprüft und dokumentiert.

Die verantwortliche Schule ergänzt ihre eigenen Kontaktdaten, Rechtsgrundlagen, Funktionen und Löschtermine. Dieses allgemeine Produktkonzept ersetzt weder ihre Datenschutzhinweise noch eine erforderliche Datenschutz-Folgenabschätzung oder einen Vertrag zur Auftragsverarbeitung.

In dieser Vollfassung

Verantwortung und Rechtsgrundlagen · Seite 2

Verarbeitung und Filterung · Seite 4

Zugriff und weitere Schutzmaßnahmen · Seite 6

Empfänger und Wartung · Seite 8

Version, Nachweise und Quellen · Seite 10

Datenarten und Zwecke · Seite 3

Verschlüsselung · Seite 5

Speicherfristen und Löschung · Seite 7

Rechte und Datenschutzvorfälle · Seite 9

Kurzfassung: separat auf der Datenschutzseite

Anbieter und Herausgeber

TamerinTECH GmbH

Seestr. 19

83727 Schliersee

Deutschland

Telefon: +49 8026 387 25 98

hello@context-friend.com

www.tamerin.tech

Geschäftsführer: Ron Tamerin

Inhaltlich verantwortlich: Ron Tamerin

Anschrift wie nebenstehend

Registergericht: Amtsgericht München

Handelsregister: HRB 263667

USt-IdNr.: DE340834936

Datenschutzkontaktstelle: hello@context-friend.com

[Vollständiges Impressum auf der Website](#)

Verantwortung und Zulässigkeit

1. Geltungsbereich

Die lokale Schulversion dient der Nachbereitung bestimmter Unterrichtseinheiten. Sie erstellt fachliche Lernnotizen, erschließt rechtmäßig bereitgestellte Materialien und ermöglicht, soweit schulisch erlaubt, Fragen an eine lokale KI. Spracherkennung, Filterung, KI, Suche, Kontenverwaltung und Speicherung finden auf dem Schulserver statt.

Die Vorgaben gelten für alle Personen, deren Daten dabei betroffen sind: Lernende, Lehrkräfte, Schulbegleitungen, Vertretungen und weitere Anwesende sowie berechtigte Erziehungsberechtigte. Reiner Websitebesuch und Kontaktformulare sind gesondert in der [Datenschutzerklärung der öffentlichen Website](#) beschrieben.

2. Verantwortliche Stelle und Datenschutzkontakte

Schule: Verantwortlich im Sinne der DSGVO ist die Schule oder die in ihren schulbezogenen Hinweisen benannte Stelle. Sie entscheidet über Zweck, Rechtsgrundlage, Umfang, Nutzerkreis, Speicherfristen und Betrieb. Die Schulleitung organisiert die Freigabe; der schulische Datenschutzbeauftragte berät und überwacht unabhängig. Der Schulaufwandsträger und die Schul-IT übernehmen die jeweils festgelegten Betriebsaufgaben.

Anbieter: TamerinTECH GmbH liefert das Produkt. Ein Zugang zu Unterrichtsdaten besteht nicht allein durch diese Lieferantenrolle. Bei beauftragter Verarbeitung personenbezogener Daten, etwa im Support, handelt TamerinTECH nur nach Weisung und auf Grundlage eines erforderlichen Vertrags nach Art. 28 DSGVO.

Kontakt: Die Schule veröffentlicht ihre Anschrift und den dienstlichen Kontakt ihres Datenschutzbeauftragten vor der Nutzung. Datenschutzanfragen an TamerinTECH erreichen die Kontaktstelle unter hello@contextfriend.com oder der Anbieteranschrift auf Seite 1. Eine Kontaktstelle ist nicht automatisch ein förmlich benannter Datenschutzbeauftragter. Eine erforderliche Benennung und Bekanntgabe seiner Kontaktdaten erfolgen gesondert nach Art. 37 DSGVO und § 38 BDSG.

3. Rechtsgrundlagen und erforderliche Informationen

Für staatliche bayerische Schulen sind insbesondere Art. 6 Abs. 1 Buchst. e und Abs. 3 DSGVO, [Art. 85 BayEUG](#) sowie [§ 46 BaySchO mit Anlage 1](#) zu prüfen. Daraus folgt keine pauschale Erlaubnis für eine dauernde Erfassung des Unterrichts. Sprachverarbeitung, Lernspeicher, Zugänge und Sicherheitsprotokolle sind jeweils auf Erforderlichkeit und geeignete Alternativen zu prüfen.

Bei freiwilligen Funktionen ist eine erforderliche Einwilligung bestimmt, informiert, freiwillig und für die Zukunft widerruflich einzuholen. Die Schule klärt die Vertretung Minderjähriger, eine gleichwertige Alternative ohne Nachteil und die Beteiligungsrechte von Beschäftigten. Anmeldung und Lesen dieses Dokuments ersetzen keine Einwilligung.

Besondere Kategorien personenbezogener Daten, etwa Gesundheitsangaben, werden nicht gezielt erhoben. Ist ihre Verarbeitung unvermeidbar, muss zusätzlich Art. 9 DSGVO beachtet werden; fehlt eine tragfähige Grundlage, ist die Erfassung auszusetzen. Auch das Recht am gesprochenen Wort bleibt zu beachten.

Datenarten und Zwecke

4. Welche Daten verarbeitet werden

Datenkategorie	Inhalt, Zweck und Grenze
Gesprochene Sprache	Sprache während ausdrücklich aktivierter Unterrichtsabschnitte zur lokalen Umwandlung in Text. Stimmen werden niemals als Audiodatei gespeichert, archiviert oder gesichert. Keine Wiedergabe, kein Stimmprofil.
Unbearbeiteter Text	Erkannter Wortlaut ausschließlich zur lokalen Inhaltsfilterung. Verwerfen nach der Filterung, spätestens fünf Minuten nach Erfassung. Keine dauerhafte Ablage, keine Suchquelle und keine Sicherung.
Lernnotizen und Materialien	Fachliche Erklärungen, Beispiele, Aufgaben, Quellenbezüge und von der Schule zulässig bereitgestellte Dokumente. Zweck: Nachbereitung und Wiederholung im berechtigten Kurs.
Suchdaten und Ableitungen	Textabschnitte, lokale Suchindizes, Embeddings und fachliche Verknüpfungen. Sie erhalten dieselben Berechtigungen und Löschtermine wie ihre Quellen.
Fragen und Antworten	Eigene Eingaben, Antworten und Gesprächskontext zur jeweiligen Lernfrage. Ein dauerhafter Verlauf wird nur bei schulischer Freigabe geführt und vorher erklärt. Keine allgemeine Einsicht anderer Lernender.
Zugänge und Berechtigungen	Notwendige Kennungen, geschützte Anmeldedaten, Rollen, Kurszuordnungen und erforderliche Freigaben. Kein öffentliches Personenverzeichnis; keine vorsorgliche Erhebung privater Profilangaben.
Sicherheitsdaten	Erforderliche Anmelde-, Zugriffs- und Verwaltungsereignisse, gegebenenfalls IP-Adressen und Zeitpunkte. Zweck: Zugriffsschutz und Fehlerklärung. Keine Unterrichtstexte, Chatinhalte oder geheimen Zugangswerte in Protokollen.
Sicherungskopien	Verschlüsselte Kopien der ausdrücklich zugelassenen gespeicherten Bestände für Wiederherstellung. Keine Audio- oder Rohtextkopien; begrenzte Zugriffsrechte und Laufzeit.

4.1 Herkunft und Personenbezug

Daten entstehen in den aktivierten Unterrichtsabschnitten, durch eigene Eingaben, schulische Kurszuordnungen und bereitgestellte Materialien. Die Schule benennt bei fremden Datenquellen die erforderlichen Informationen nach Art. 14 DSGVO. Die bloße Möglichkeit, Daten zu verarbeiten, ist keine Erlaubnis, alle Datenkategorien zu erheben.

Stimme, Frageinhalt, Kennung oder Kontext können eine Person erkennbar machen. Namensfilter und Pseudonyme sind kein vollständiger Anonymitätsnachweis. Die Aussage zu entfernten Namen bezieht sich auf die Lernnotizen, nicht auf notwendige Kontodaten oder gesetzliche Nachweise der Schule.

4.2 Ausgeschlossene Auswertungen

Keine Werbung, kein Datenhandel, kein Training oder Fine-Tuning von KI-Modellen mit Unterrichtsinhalten. Keine Stimmabdrücke, individuellen Persönlichkeits- oder Leistungsprofile, Sprechzeit-, Emotions-, Verhaltens- oder Anwesenheitsanalyse. Eine technische Betriebsstatistik darf keine Bewertung einzelner Lernender oder Lehrkräfte ermöglichen und wird nicht an den Anbieter übermittelt.

Verarbeitung im Unterricht

5. Datenfluss und Inhaltsfilter

1. **Aktivierung:** Die Lehrkraft aktiviert die Sprachverarbeitung nur für vereinbarte Unterrichtsabschnitte. Der aktive Zustand ist erkennbar; ein Stopp beendet die Erfassung.
2. **Lokale Erkennung:** Sprache wird auf dem Schulserver in Text umgewandelt. Es entsteht zu keinem Zeitpunkt eine gespeicherte Audiodatei, auch nicht zur Wartung oder Fehlerdiagnose.
3. **Filter vor Ablage:** Namen aus der Klasse, private Angaben und fachfremde Aussagen werden entfernt. Dazu gehören etwa Namensrufe, Toilettenfragen, private Konflikte, Gesundheitsangaben und organisatorische Zwischenrufe ohne Lernbezug.
4. **Fachliche Lernnotiz:** Gespeichert wird der bereinigte fachliche Inhalt. Sachlich benötigte historische oder literarische Namen, etwa in einem Geschichtsthema, bleiben möglich. Die ursprüngliche persönliche Aussage wird nicht daneben aufbewahrt.
5. **Suche und Antwort:** Nur zugelassene Inhalte des berechtigten Kurses gelangen in die Suche und die lokale KI. Persönliche Chats, Sicherheitsprotokolle und zurückgezogene Inhalte sind keine gemeinsamen Lernquellen.
6. **Löschung:** Unbearbeiteter Text wird nach der Filterung verworfen, spätestens fünf Minuten nach Erfassung. Quellen und daraus erzeugte Suchdaten werden nach derselben schulischen Frist gelöscht.

Fällt der Filter aus, darf dies keine ungefilterte Ablage oder Veröffentlichung auslösen. Nicht sicher verarbeitbare Abschnitte werden verworfen. Private Inhalte werden auch nicht in Diagnoseprotokolle, Testdatensammlungen oder Sicherungen kopiert.

6. Optionale Durchsicht und fachliche Grenzen

Lehrkräfte können Notizen prüfen, korrigieren oder löschen. Die Durchsicht ist optional; es gibt keinen verpflichtenden Freigabeschritt für jede Notiz. Lernnotizen können daher bereits vor einer menschlichen Durchsicht sichtbar sein. Automatische Filter können Angaben übersehen, und KI-Inhalte können falsch oder unvollständig sein.

Die Schule richtet einen erreichbaren Meldeweg ein. Gemeldete personenbezogene oder falsche Inhalte werden geprüft und erforderlichenfalls gesperrt, korrigiert oder gelöscht, einschließlich ihrer Ableitungen. Ein Hinweis auf mögliche KI-Fehler ersetzt keine wirksame technische Filterung und keine Bearbeitung von Meldungen.

Die KI unterstützt Lernen und Wiederholung. Sie trifft keine Entscheidungen über Benotung, Versetzung oder Aufnahme und erstellt keine automatisierten personenbezogenen Leistungsbewertungen. Quellenbezogene Unterrichtsinhalte und ergänzende allgemeine Erläuterungen müssen unterscheidbar bleiben.

6.1 Schutz aller Anwesenden

Vor dem Einsatz werden Lernende, Lehrkräfte und weitere betroffene Personen informiert. Private Gespräche werden von der Erfassung ausgenommen. Wer nicht erfasst werden darf, benötigt eine tatsächlich wirksame Lösung im Raum; kein Konto anzulegen oder lediglich den Sitzplatz zu wechseln genügt nicht. Erforderlichenfalls bleibt die Sprachverarbeitung ausgeschaltet.

Verschlüsselung

7. Alle Dateien bei Speicherung und Übertragung geschützt

Alle Dateien und Daten der lokalen Schulinstallation sind im Ruhezustand (at rest) und bei der Übertragung (in transit) verschlüsselt. Diese Vorgabe umfasst sämtliche Speicherorte und Netzwerkwege der Anwendung, einschließlich Sicherungen, temporärer Dateien und administrativer Zugriffe.

7.1 Verschlüsselte Speichergeräte und Datenvolumes

Die physischen Datenträger beziehungsweise Datenvolumes werden vor der Ablage von Schuldaten verschlüsselt. Dazu gehören Datenbanken mit ihren Änderungsprotokollen, hochgeladene Materialien, Lernnotizen, Suchindizes, Kontodaten, Sicherheitsprotokolle sowie temporäre Dateien, soweit sie überhaupt angelegt werden dürfen. Audio und Rohtext dürfen dadurch nicht zu erlaubten Speicherbeständen werden.

Geeignete Verfahren sind beispielsweise **LUKS2 mit dm-crypt unter Linux** oder **FileVault unter macOS**. Externe Laufwerke, zusätzliche Volumes, Sicherungen, Snapshots sowie Auslagerungs- und Ruhezustandsdateien werden gesondert berücksichtigt. Ein verschlüsseltes Systemlaufwerk allein belegt nicht, dass alle weiteren Speicherorte verschlüsselt sind.

Sicherungskopien liegen ausschließlich auf verschlüsselten, getrennt geschützten lokalen Medien. Es gibt keine unverschlüsselten Kopien auf Wechselmedien und keine automatische Cloud-Synchronisierung. Die konkrete Plattform, die abgedeckten Volumes und das gewählte Verfahren werden für die Installation dokumentiert.

7.2 Verschlüsselte Übertragung

Browserzugriffe erfolgen über **HTTPS/TLS**. Alle weiteren Netzwerkstrecken, einschließlich Mikrofonendpunkt zum Schulserver, interner Dienste über das Netzwerk, Sicherungsübertragung und freigegebener Fernwartung, müssen authentisiert und verschlüsselt sein. Zertifikate und Gegenstellen werden geprüft; ein Fehler darf keinen Rückfall auf eine unverschlüsselte Verbindung auslösen.

Ein zugelassener Fernzugang nutzt zusätzlich den von der Schule kontrollierten sicheren Zugang. Die bloße Zugehörigkeit zum Schulnetz oder ein WLAN-Passwort ersetzen nicht die Prüfung der einzelnen Übertragungswege. Ein rein physisch angeschlossenes Gerät wird als eigener lokaler Anschluss bewertet und gegen unbefugten Zugriff geschützt.

7.3 Schlüssel, Wiederherstellung und Grenzen

Die Schule bestimmt die zuständigen Personen für Schlüssel und Wiederherstellung. Wiederherstellungsschlüssel werden getrennt vom geschützten Datenträger und nur für Berechtigte zugänglich verwahrt; keine Ablage im allgemeinen Dokumentenbereich und keine unkontrollierte Hinterlegung in einem privaten Cloudkonto.

Bei der Einrichtung werden gesperrte Datenträger, Neustart, Entsperren, Rechteentzug und die Wiederherstellung einer verschlüsselten Sicherung geprüft. Beim Austausch oder der Aussonderung sind Daten und Schlüssel kontrolliert zu löschen.

Datenträgerverschlüsselung schützt insbesondere ein gesperrtes, verlorenes oder ausgebautes Speichermedium. Berechtigte laufende Anwendungen müssen Inhalte verarbeiten können. Deshalb bleiben Zugriffsschutz, sichere Endgeräte, Inhaltsfilterung und Löschung zusätzlich erforderlich. Die öffentliche PDF selbst benötigt kein Passwort.

Zugriffe und weitere Schutzmaßnahmen

8. Rollen und Berechtigungen

Rolle	Erlaubter Umfang
Lernende	Lerninhalte der eigenen berechtigten Kurse; eigene KI-Fragen, sofern freigegeben. Kein Zugriff auf fremde Chats, Verwaltungsfunktionen oder vollständige Unterrichtswortlaute.
Lehrkräfte	Lerninhalte ihrer zugeordneten Kurse ansehen und optional prüfen, korrigieren oder entfernen. Eine Einsicht in individuelle Aufgabenverläufe erfordert einen eigenen, vorher erklärten schulischen Zweck und die passende Berechtigung.
Erziehungsberechtigte	Kein automatischer Zugang. Ein gesondert erlaubter Lesezugang ist auf die zugeordneten Inhalte beschränkt und erlaubt keine allgemeine Beobachtung der Klasse oder fremder Gespräche.
Schulleitung / Verwaltung	Benannte Zuständigkeiten für Freigaben, Kursrechte, Sperrungen und begründete Einzelprüfungen. Eine Verwaltungsrolle rechtfertigt keine anlasslose Auswertung sämtlicher Lerninteraktionen.
Schul-IT	Erforderliche technische Pflege, Sicherung und Wiederherstellung mit begrenzten privilegierten Rechten. Keine eigenständige pädagogische Inhaltsauswertung.
Anbieter-Support	Nur ein konkret beauftragter, zeitlich begrenzter Zugriff. Keine ständige Verbindung, keine Selbstfreigabe und keine private Nutzung von Unterrichtsinhalten.

8.1 Technische Durchsetzung

Kurs- und Rollenrechte werden auf dem Server bei jeder Abfrage, Suche, Anzeige und Änderung kontrolliert. Eine sichtbare Schaltfläche oder ein gültiger Zugang allein genügt nicht. Berechtigungsentzug beendet auch bestehende Sitzungen und Zugriffe auf zurückgezogene Inhalte.

Anmeldedaten werden geschützt gespeichert; Passwörter werden nicht im Klartext abgelegt. Privilegierte Zugänge erhalten einen zusätzlichen Anmeldefaktor oder gleichwertig abgesicherte Verfahren. Technische Konten erhalten nur die für ihre Aufgabe notwendigen Rechte. Geheime Zugangswerte erscheinen nicht in Lerninhalten oder Protokollen.

8.2 Betrieb, Endgeräte und Verfügbarkeit

Server und Sicherungsmedien befinden sich in einem gegen unbefugten Zutritt geschützten Bereich. Netzfrequenzen sind auf notwendige Dienste beschränkt; Datenbank-, Modell- und Speicherzugriffe werden nicht direkt für Lernende oder Heimnetze geöffnet. Sicherheitsupdates, Zuständigkeiten und Wiederherstellungsverfahren sind dokumentiert.

Lesen und interaktive KI-Fragen sind getrennte Freigaben. Heimzugang ermöglicht kein Mithören und schaltet keine Mikrofone ein. Die Anwendung legt keine dauerhaften Inhaltskopien in Browserdatenbanken oder Offline-Caches an. Schulen regeln sichere Endgeräte und Abmeldung; Screenshots oder selbst angelegte private Kopien lassen sich nicht vollständig technisch verhindern.

Bei Ausfällen steht eine geeignete Lernalternative zur Verfügung. Es gibt keinen automatischen Wechsel auf externe KI-Dienste. Neue Funktionen und geänderte Datenwege werden vor Aktivierung datenschutzrechtlich bewertet.

Speicherfristen und Löschung

9. Die Schule entscheidet, Standard ist ein Schuljahr

Die Schule bestimmt die Speicherdauer der Lerninhalte. Standard ist ein Schuljahr: Löschung am Ende des jeweiligen Schuljahres. Im regulären bayerischen Schuljahr 2026/27 ist dies der 31. Juli 2027. Ein später hinzugefügter Inhalt erhält nicht automatisch weitere zwölf Monate. Grundlage für die Schuljahresgrenze ist [Art. 5 BayEUG](#).

Eine kürzere Frist kann festgelegt werden. Eine längere Speicherung braucht einen weiterhin zulässigen und erforderlichen Zweck und wird vorab erklärt. Ein bloßer späterer Abruf verlängert keine Frist. Die nachstehenden Grenzen sind Produktvorgaben; strengere anwendbare Vorgaben gehen vor.

Bestand	Frist / Löschereignis
Audio	Keine gespeicherten Audiodateien, kein Archiv und keine Sicherungskopien.
Unbearbeiteter Text	Verwerfen nach der Filterung, spätestens fünf Minuten nach Erfassung. Keine Sicherung.
Lerninhalte und Ableitungen	Notizen, Materialien, gespeicherte Fragen/Antworten sowie zugehörige Suchdaten: schulischer Löschtermin, standardmäßig Ende des betreffenden Schuljahres.
Zugänge und Konten	Sperrung mit Ende der Berechtigung; Löschung der erforderlichen Kontodaten spätestens 30 Tage danach.
Sicherheitsprotokolle	Zugriffseignisse höchstens 7 Tage; besondere Verwaltungsereignisse wie Rechteänderungen höchstens 30 Tage. Jeweils ohne Unterrichts- oder Gesprächsinhalte.
Sicherungen	Verschlüsselt, rollierend höchstens 14 Tage. Keine Weiterkopie in ein unbefristetes Archiv. Gelöschte Daten dürfen durch einen Restore nicht wieder zugänglich werden.
Anonyme Betriebsstatistik	Nur tatsächlich anonyme Gesamtkennzahlen, soweit die Schule diese erlaubt. Schulisch bestimmter Zeitraum, standardmäßig Ende des Schuljahres; keine individuelle Historie oder Anbieterübermittlung.

9.1 Vollständige Löschkette

Bei Löschung wird der Inhalt zunächst von Anzeige, Suche und KI-Abruf ausgeschlossen. Danach werden Quelle, Versionen, abgeleitete Notizen, Indexeinträge, Dateien und zulässige Zwischenspeicher bereinigt. Das Löschen nur einer sichtbaren Notiz genügt nicht, wenn ihre Ableitungen weiter abrufbar bleiben.

Eine vorhandene Sicherung kann eine nicht mehr zur Nutzung zugängliche Kopie noch höchstens 14 Tage enthalten. Vor Freigabe einer Wiederherstellung werden zwischenzeitliche Löschungen und Rechteentzüge erneut angewendet. Ausgefallene Löschläufe werden nachgeholt und kontrolliert.

Erforderliche rechtliche Nachweise zu Einwilligungen, Freigaben oder Datenschutzfällen führt die Schule getrennt nach der jeweils geltenden Frist. Sie rechtfertigen kein pauschales Unterrichts- oder Audioarchiv in ContextFriend.

Empfänger, Fernzugang und Wartung

10. Keine externe Verarbeitung von Unterrichtsinhalten

Für diese lokale Version sind externe KI-Dienste, Cloudspeicher, Inhalts-Tracking und die Nutzung von Unterrichtsdaten durch Mikrofon- oder Modellhersteller ausgeschlossen. Die Anwendung nutzt die Inhalte ausschließlich für die von der Schule festgelegten Zwecke. Ein Modellbezug oder Softwareupdate überträgt keine Unterrichtsinhalte an den Lieferanten.

Zugriff erhalten nur die für den jeweiligen Kurs und Zweck berechtigten Personen sowie gegebenenfalls ausdrücklich beauftragte technische Stellen. Die Schule nennt tatsächlich eingesetzte Dienstleister und ihre Rollen in den schulbezogenen Hinweisen. Weitere Auftragsverarbeiter werden nur auf der erforderlichen vertraglichen Grundlage und nach dem vereinbarten Genehmigungsverfahren eingesetzt.

10.1 Zugang von zu Hause

Ein Heimzugang wird ausschließlich durch die Schule freigegeben. Die Verbindung führt verschlüsselt zu einem schulisch kontrollierten Endpunkt und eröffnet nur die erlaubte Anwendung, keinen allgemeinen Zugang zum Schulnetz. Lesen allein erlaubt noch keine interaktiven KI-Fragen.

Erlaubte Texte werden am angemeldeten Endgerät angezeigt; diese Anzeige findet dann außerhalb des Schulgebäudes statt. Netzbetreiber können Verbindungsmetadaten sehen. Die KI und der maßgebliche Datenbestand bleiben auf dem Schulserver. Eine Übertragung von Unterrichtsinhalten an Stellen in Drittstaaten ist für diese Version nicht vorgesehen; abweichende Zugriffe dürfen nicht stillschweigend freigeschaltet werden.

10.2 Anbieterzugriff nur im Einzelfall

TamerinTECH hat keinen ständigen Zugang zu Unterrichtsdaten. Technischer Support wird möglichst ohne Inhaltszugriff durchgeführt. Ist Dateneinsicht im Einzelfall erforderlich, legt die Schule zuvor Zweck, beauftragte Person, Berechtigungen, Dauer und zulässige Werkzeuge fest. Bei personenbezogener Verarbeitung im Auftrag ist zuvor der erforderliche AVV wirksam.

Fernwartung erfolgt verschlüsselt zu einem abgesicherten, verwalteten Supportgerät in Deutschland. Inhaltskopien, Downloads, Druck, Aufzeichnungen und die Übernahme in externe Ticketsysteme oder KI-Werkzeuge sind nicht erlaubt. Die Sitzung endet mit Auftragserfüllung, Ablauf des vereinbarten Fensters oder Widerruf; verbleibende Rechte werden entzogen. Reichen die Schutzmöglichkeiten nicht aus, erfolgt die Wartung vor Ort.

Ein Wartungsnachweis dokumentiert Anlass, berechtigte Person, Zeitraum und ausgeführte Maßnahmen, ohne Unterrichtsinhalte aufzunehmen. Support ist keine Erlaubnis, Audio aufzuzeichnen oder eine eigene Test- und Trainingssammlung anzulegen. Eine private Schulrolle eines Anbietermitarbeiters begründet keine zusätzlichen Anbieterrechte.

10.3 Sicherung und Änderungen

Sicherungen bleiben auf getrennten, verschlüsselten Medien im schulisch festgelegten lokalen Schutzbereich. Zuständigkeit, Sicherungsumfang, Wiederherstellungsziele und regelmäßige Wiederherstellungstests sind zu dokumentieren. Risiken eines Ausfalls des gesamten Standorts werden gesondert bewertet; sie erlauben keine verdeckte Cloudkopie.

Änderungen an Modellen, Funktionen, Berechtigungen, Speicherorten, Fristen oder Empfängern werden vor ihrem Einsatz bewertet und in den Hinweisen nachvollziehbar aktualisiert. Ein Update darf das hier beschriebene Schutzkonzept nicht stillschweigend erweitern.

Rechte und Datenschutzvorfälle

11. Rechte der betroffenen Personen

Nach den gesetzlichen Voraussetzungen bestehen Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und gegebenenfalls Datenübertragbarkeit. Bei Verarbeitung für eine öffentliche Aufgabe kann aus Gründen der besonderen Situation widersprochen werden. Erteilte Einwilligungen sind für die Zukunft widerruflich. Die maßgeblichen Regeln stehen in Art. 12 bis 22 DSGVO.

Die verantwortliche Schule beziehungsweise ihr Datenschutzbeauftragter nehmen Anliegen entgegen. Die Identität wird nur im erforderlichen Umfang geprüft. Die Antwort erfolgt grundsätzlich innerhalb eines Monats; über eine gesetzlich zulässige Verlängerung und deren Gründe wird fristgerecht informiert. Eine Ablehnung wird begründet und mit den vorgesehenen Rechtsschutzinformationen versehen.

TamerinTECH unterstützt die Schule bei beauftragter Verarbeitung, trifft aber keine eigenständige Entscheidung über die Freigabe fremder Unterrichtsdaten. Betroffene müssen sich nicht durch technische Einstellungen arbeiten, um ihr Anliegen vorzubringen.

11.1 Beschwerdemöglichkeiten

Zuständigkeit	Kontakt
Staatliche bayerische Schulen	Bayerischer Landesbeauftragter für den Datenschutz Postfach 22 12 19, 80502 München Besucheranschrift: Wagnmüllerstraße 18, 80538 München Telefon: +49 89 212672-0 poststelle@datenschutz-bayern.de www.datenschutz-bayern.de
Nichtöffentliche Stellen in Bayern	Bayerisches Landesamt für Datenschutzaufsicht Postfach 1349, 91504 Ansbach Besucheranschrift: Promenade 18, 91522 Ansbach Telefon: +49 981 180093-0 poststelle@lda.bayern.de www.lda.bayern.de

Bei anderen Trägern oder besonderen Zuständigkeiten benennt die Schule die zuständige Aufsicht. Die Behörden bieten sichere Onlineformulare für Beschwerden an. Die Kontaktstelle beim Anbieter und die Aufsichtsbehörde sind verschiedene Stellen.

12. Fehler und Sicherheitsvorfälle

Unbeabsichtigte Offenlegung, unberechtigter Zugriff, Verlust oder andere Datenschutzverletzungen werden über den schulischen Meldeweg unverzüglich gemeldet. Die zuständigen Stellen begrenzen den Zugriff, sichern erforderliche inhaltsarme Nachweise und prüfen Folgen und Abhilfe. Betroffene Lerninhalte werden erforderlichenfalls gesperrt.

Die verantwortliche Stelle prüft eine Meldung an die Aufsicht nach Art. 33 DSGVO, grundsätzlich innerhalb von 72 Stunden nach Bekanntwerden, soweit die Meldepflicht besteht. Bei voraussichtlich hohem Risiko werden Betroffene nach Art. 34 ohne unangemessene Verzögerung informiert. Ein Auftragsverarbeiter informiert die verantwortliche Stelle unverzüglich nach Bekanntwerden.

Wiederanlauf und Wiederherstellung erfolgen erst nach Prüfung der Schutzmaßnahmen, Rechte und Löschvorgaben. Eine Störung rechtfertigt weder eine Tonaufzeichnung noch die unkontrollierte Weitergabe von Schuldaten.

Verbindlichkeit und Quellen

13. Einrichtung an der Schule und Pflege der Dokumente

Für jede Schule müssen der tatsächliche Lieferstand, Funktionen, Geräte, Modelle, Datenwege, Fristen und zuständigen Stellen feststehen. Die Schule erstellt ihre konkreten Hinweise und das erforderliche Verzeichnis der Verarbeitungstätigkeiten. Sie prüft die Pflicht zur Datenschutz-Folgenabschätzung; ist eine DSFA erforderlich, muss diese vor der Verarbeitung abgeschlossen sein. Ein verbleibendes hohes Risiko ist nach Art. 36 DSGVO zu behandeln.

Bei der Einrichtung werden an jeder Installation insbesondere geprüft und dokumentiert: keine Audioablage auch bei Fehlern, Filterung vor Speicherung, die Fünf-Minuten-Grenze für Rohtext, Verschlüsselung sämtlicher Speicher- und Übertragungswege, wirksame Kursrechte, Korrektur und Rücknahme sowie Löschung einschließlich Sicherungen. Das Fehlen einer verpflichtenden Durchsicht durch Lehrkräfte ist bei der Risikobewertung ausdrücklich zu berücksichtigen.

Die Schulleitung entscheidet über den Einsatz mit den zuständigen schulischen Stellen. Betroffene werden vor Beginn informiert; erforderliche Einwilligungen werden gesondert eingeholt. Die fachliche Kompetenz und altersgerechte Begleitung bei KI-Nutzung sind sicherzustellen. Dieses Konzept enthält keine staatliche Zulassungs- oder Förderzusage.

Version 1.3 vom 16. Oktober 2026 gilt gemeinsam mit der gleich datierten Kurzfassung. Änderungen werden nachvollziehbar dokumentiert. Die öffentlichen PDFs enthalten keine ausgefüllten Schul-, Vertrags- oder Antragsunterlagen. Die Schule erhält ihre benötigten Vertrags- und Betriebsunterlagen gesondert.

14. Rechts- und Fachquellen

1. [Datenschutz-Grundverordnung](#), insbesondere Art. 5, 6, 9, 12 bis 22, 25, 28, 30, 32 bis 39.
2. [Art. 85 BayEUG](#) zur Verarbeitung personenbezogener Daten; [Art. 5 BayEUG](#) zur Schuljahresgrenze.
3. [§ 46 BaySchO mit Anlage 1](#) zu schulischen Verarbeitungstätigkeiten; weitere für die jeweilige Schule einschlägige Vorschriften bleiben zu prüfen.
4. [Bayerisches Kultusministerium: Künstliche Intelligenz](#), mit dem Handlungsleitfaden zur pädagogischen Praxis vom 19. Mai 2026.
5. [§ 38 BDSG](#) zur Benennung von Datenschutzbeauftragten nichtöffentlicher Stellen; die Prüfung ist unabhängig von dieser Kontaktinformation vorzunehmen.
6. [Linux-Kernel-Dokumentation: dm-crypt](#) und [cryptsetup/LUKS](#); [Apple: FileVault](#). Verfahrensbeschreibungen ersetzen keine Prüfung der Installation.
7. Kontaktquellen: [ContextFriend Impressum](#), [BayLfD](#) und [BayLDA](#). Abrufstand: 14. Oktober 2026.

Datenschutzkontakt beim Anbieter

TamerinTECH GmbH · Seestr. 19 · 83727 Schliersee · Deutschland
hello@context-friend.com · +49 8026 387 25 98

Für Unterrichtsdaten wenden Sie sich an die verantwortliche Schule oder deren Datenschutzbeauftragte. Die vereinfachte Familieninformation und diese Volfassung stehen unter context-friend.com/school-documents.