

Concetto di protezione dei dati

Versione scolastica locale Trattamento, protezione e diritti

Nessuna registrazione audio memorizzata. Nessun profilo vocale.

I nomi della classe, le affermazioni private e le osservazioni estranee alla materia vengono filtrati prima dell'archiviazione delle note di apprendimento. La revisione da parte dei docenti è facoltativa.

Tutti i file e i dati dell'installazione scolastica locale sono cifrati durante la memorizzazione e la trasmissione. La scuola stabilisce la durata di conservazione dei contenuti di apprendimento; lo standard è un anno scolastico.

Questo documento descrive la **versione scolastica locale di ContextFriend**: trattamento, misure di protezione e diritti. Durante la configurazione presso una scuola, ogni installazione viene verificata e documentata sulla base di questo concetto.

La scuola titolare integra i propri dati di contatto, basi giuridiche, funzioni e date di cancellazione. Questo concetto generale di prodotto non sostituisce né la sua informativa sulla protezione dei dati né una valutazione d'impatto sulla protezione dei dati necessaria o un contratto di trattamento per conto del titolare (art. 28 GDPR).

In questa versione completa

Responsabilità e basi giuridiche · Pagina 2

Trattamento e filtraggio · Pagina 4

Accesso e ulteriori misure di protezione · Pagina 6

Destinatari e manutenzione · Pagina 8

Versione, evidenze e fonti · Pagina 10

Categorie di dati e finalità · Pagina 3

Cifratura · Pagina 5

Termini di conservazione e cancellazione · Pagina 7

Diritti e violazioni dei dati · Pagina 9

Versione breve: separata, sulla pagina della privacy

Fornitore ed editore

TamerinTECH GmbH

Seestr. 19

83727 Schliersee

Germany

Telefono: +49 8026 387 25 98

hello@context-friend.com

www.tamerin.tech

Amministratore: Ron Tamerin

Responsabile dei contenuti: Ron Tamerin

Indirizzo come indicato

Tribunale del registro: Amtsgericht München

Registro delle imprese: HRB 263667

Partita IVA (DE): DE340834936

Contatto privacy: hello@context-friend.com

[Impressum completo sul sito](#)

Responsabilità e liceità

1. Ambito di applicazione

La versione scolastica locale serve alla rielaborazione di determinate unità didattiche. Crea note di apprendimento relative alla materia, rende fruibili materiali messi a disposizione legittimamente e consente, nei limiti permessi dalla scuola, di porre domande a un'IA locale. Riconoscimento vocale, filtraggio, IA, ricerca, gestione degli account e memorizzazione avvengono sul server della scuola.

Le disposizioni valgono per tutte le persone i cui dati sono coinvolti: studenti, docenti, assistenti scolastici, supplenti e altri presenti, nonché i genitori ed esercenti la responsabilità genitoriale autorizzati. La semplice visita del sito web e i moduli di contatto sono descritti separatamente nell'[informativa sulla privacy del sito web pubblico](#).

2. Titolare del trattamento e contatti per la protezione dei dati

Scuola: titolare del trattamento ai sensi del GDPR è la scuola o l'ente indicato nella sua informativa specifica per la scuola. Essa decide finalità, base giuridica, portata, cerchia di utenti, termini di conservazione ed esercizio. La dirigenza scolastica organizza l'approvazione; il responsabile della protezione dei dati (RPD) della scuola fornisce consulenza e vigila in modo indipendente. L'ente gestore delle spese scolastiche (Schulaufwandsträger) e l'IT della scuola svolgono i rispettivi compiti operativi stabiliti.

Fornitore: TamerinTECH GmbH fornisce il prodotto. Questo ruolo di fornitore non comporta di per sé alcun accesso ai dati delle lezioni. In caso di trattamento di dati personali su incarico, ad esempio nel supporto, TamerinTECH agisce solo su istruzione e sulla base di un contratto necessario ai sensi dell'art. 28 GDPR.

Contatto: la scuola pubblica il proprio indirizzo e il contatto di servizio del suo responsabile della protezione dei dati (RPD) prima dell'uso. Le richieste in materia di protezione dei dati a TamerinTECH raggiungono il punto di contatto all'indirizzo hello@context-friend.com o all'indirizzo del fornitore a pagina 1. Un punto di contatto non è automaticamente un responsabile della protezione dei dati formalmente designato. Una designazione necessaria e la comunicazione dei suoi dati di contatto avvengono separatamente ai sensi dell'art. 37 GDPR e del § 38 BDSG (legge federale tedesca sulla protezione dei dati).

3. Basi giuridiche e informazioni necessarie

Per le scuole statali bavaresi vanno esaminati in particolare l'art. 6, par. 1, lett. e) e par. 3 GDPR, l'[art. 85 BayEUG](#) (legge bavarese sull'istruzione) nonché il [§ 46 BaySchO con l'allegato 1](#) (regolamento scolastico bavarese). Da ciò non deriva alcuna autorizzazione generale a una rilevazione permanente delle lezioni. L'elaborazione vocale, la memoria di apprendimento, gli accessi e i registri di sicurezza vanno esaminati ciascuno sotto il profilo della necessità e di alternative idonee.

Per le funzioni facoltative, un consenso necessario va raccolto in modo specifico, informato, libero e revocabile per il futuro. La scuola chiarisce la rappresentanza dei minori, un'alternativa equivalente senza svantaggi e i diritti di partecipazione dei dipendenti. L'iscrizione e la lettura di questo documento non sostituiscono un consenso.

Le categorie particolari di dati personali, ad esempio i dati sanitari, non vengono raccolte in modo mirato. Se il loro trattamento è inevitabile, deve essere rispettato anche l'art. 9 GDPR; in assenza di una base solida, la rilevazione va sospesa. Resta inoltre da rispettare il diritto sulla parola pronunciata (Recht am gesprochenen Wort).

Categorie di dati e finalità

4. Quali dati vengono trattati

Categoria di dati	Contenuto, finalità e limite
Parlato	Parlato durante le parti di lezione espressamente attivate, per la conversione locale in testo. Le voci non vengono mai salvate, archiviate o copiate in backup come file audio. Nessuna riproduzione, nessun profilo vocale.
Testo non elaborato	Testo riconosciuto esclusivamente per il filtraggio locale dei contenuti. Scartato dopo il filtraggio, al più tardi cinque minuti dopo la rilevazione. Nessuna archiviazione permanente, nessuna fonte di ricerca e nessuna copia di sicurezza.
Note di apprendimento e materiali	Spiegazioni relative alla materia, esempi, esercizi, riferimenti alle fonti e documenti messi a disposizione legittimamente dalla scuola. Finalità: rielaborazione e ripasso nel corso autorizzato.
Dati di ricerca e derivati	Porzioni di testo, indici di ricerca locali, embedding e collegamenti tematici. Ricevono le stesse autorizzazioni e date di cancellazione delle loro fonti.
Domande e risposte	Propri inserimenti, risposte e contesto della conversazione relativi alla singola domanda di apprendimento. Una cronologia permanente viene tenuta solo con l'approvazione della scuola e viene spiegata in anticipo. Nessuna visione generale da parte di altri studenti.
Accessi e autorizzazioni	Identificativi necessari, credenziali di accesso protette, ruoli, assegnazioni ai corsi e approvazioni necessarie. Nessun elenco pubblico di persone; nessuna raccolta preventiva di dati di profilo privati.
Dati di sicurezza	Eventi necessari di accesso, consultazione e amministrazione, eventualmente indirizzi IP e orari. Finalità: protezione degli accessi e chiarimento degli errori. Nessun testo delle lezioni, contenuto di chat o valore di accesso segreto nei registri.
Copie di sicurezza	Copie cifrate dei dati memorizzati espressamente ammessi, a fini di ripristino. Nessuna copia audio o di testo grezzo; diritti di accesso e durata limitati.

4.1 Origine e riferibilità alle persone

I dati nascono nelle parti di lezione attivate, dai propri inserimenti, dalle assegnazioni ai corsi da parte della scuola e dai materiali messi a disposizione. In caso di fonti di dati esterne, la scuola fornisce le informazioni necessarie ai sensi dell'art. 14 GDPR. La semplice possibilità di trattare dati non è un'autorizzazione a raccogliere tutte le categorie di dati.

La voce, il contenuto di una domanda, un identificativo o il contesto possono rendere riconoscibile una persona. I filtri dei nomi e gli pseudonimi non costituiscono una prova completa di anonimato. L'affermazione sui nomi rimossi si riferisce alle note di apprendimento, non ai dati dell'account necessari o alle evidenze di legge della scuola.

4.2 Analisi escluse

Nessuna pubblicità, nessun commercio di dati, nessun addestramento o fine-tuning di modelli di IA con contenuti delle lezioni. Nessuna impronta vocale, nessun profilo individuale di personalità o di rendimento, nessuna analisi del tempo di parola, delle emozioni, del comportamento o delle presenze. Una statistica tecnica di esercizio non deve consentire alcuna valutazione di singoli studenti o docenti e non viene trasmessa al fornitore.

Trattamento durante le lezioni

5. Flusso dei dati e filtro dei contenuti

1. **Attivazione:** il docente attiva l'elaborazione vocale solo per le parti di lezione concordate. Lo stato attivo è riconoscibile; un arresto termina la rilevazione.
2. **Riconoscimento locale:** il parlato viene convertito in testo sul server della scuola. In nessun momento viene creato un file audio memorizzato, nemmeno per la manutenzione o la diagnosi degli errori.
3. **Filtro prima dell'archiviazione:** i nomi della classe, le informazioni private e le affermazioni estranee alla materia vengono rimossi. Rientrano tra questi, ad esempio, i nomi chiamati, le richieste di andare in bagno, i conflitti privati, le informazioni sanitarie e le interruzioni organizzative senza riferimento all'apprendimento.
4. **Nota di apprendimento relativa alla materia:** viene memorizzato il contenuto tematico ripulito. I nomi storici o letterari necessari dal punto di vista del contenuto, ad esempio in un argomento di storia, restano possibili. L'affermazione personale originaria non viene conservata accanto a essa.
5. **Ricerca e risposta:** solo i contenuti ammessi del corso autorizzato entrano nella ricerca e nell'IA locale. Le chat personali, i registri di sicurezza e i contenuti ritirati non sono fonti di apprendimento condivise.
6. **Cancellazione:** il testo non elaborato viene scartato dopo il filtraggio, al più tardi cinque minuti dopo la rilevazione. Le fonti e i dati di ricerca da esse generati vengono cancellati allo stesso termine stabilito dalla scuola.

Se il filtro si guasta, ciò non deve determinare alcuna archiviazione o pubblicazione non filtrata. Le parti non elaborabili in modo sicuro vengono scartate. I contenuti privati non vengono copiati nemmeno in registri diagnostici, raccolte di dati di test o copie di sicurezza.

6. Revisione facoltativa e limiti di contenuto

I docenti possono verificare, correggere o cancellare le note. La revisione è facoltativa; non esiste alcun passaggio di approvazione obbligatorio per ogni nota. Le note di apprendimento possono quindi essere visibili già prima di una revisione umana. I filtri automatici possono non rilevare alcune informazioni e i contenuti dell'IA possono essere errati o incompleti.

La scuola istituisce un canale di segnalazione raggiungibile. I contenuti personali o errati segnalati vengono verificati e, se necessario, bloccati, corretti o cancellati, inclusi i loro derivati. Un avviso su possibili errori dell'IA non sostituisce né un filtraggio tecnico efficace né la gestione delle segnalazioni.

L'IA supporta l'apprendimento e il ripasso. Non prende decisioni su valutazione, promozione o ammissione e non elabora valutazioni automatizzate del rendimento riferite a persone. I contenuti delle lezioni basati sulle fonti e le spiegazioni generali integrative devono restare distinguibili.

6.1 Protezione di tutti i presenti

Prima dell'impiego, studenti, docenti e altre persone interessate vengono informati. Le conversazioni private vengono escluse dalla rilevazione. Chi non può essere rilevato ha bisogno di una soluzione effettivamente efficace nell'aula; non creare un account o cambiare semplicemente posto non è sufficiente. Se necessario, l'elaborazione vocale resta disattivata.

Cifratura

7. Tutti i file protetti durante la memorizzazione e la trasmissione

Tutti i file e i dati dell'installazione scolastica locale sono cifrati a riposo (at rest) e durante la trasmissione (in transit). Questa disposizione comprende tutti i luoghi di archiviazione e i percorsi di rete dell'applicazione, incluse le copie di sicurezza, i file temporanei e gli accessi amministrativi.

7.1 Dispositivi di archiviazione e volumi di dati cifrati

I supporti fisici di dati o i volumi di dati vengono cifrati prima dell'archiviazione di dati scolastici. Ne fanno parte le banche dati con i loro registri delle modifiche, i materiali caricati, le note di apprendimento, gli indici di ricerca, i dati degli account, i registri di sicurezza nonché i file temporanei, nella misura in cui possono essere creati. L'audio e il testo grezzo non devono per questo diventare dati memorizzati ammessi.

Procedure idonee sono ad esempio **LUKS2 con dm-crypt su Linux** o **FileVault su macOS**. Le unità esterne, i volumi aggiuntivi, le copie di sicurezza, gli snapshot nonché i file di swap e di ibernazione vengono considerati separatamente. Un'unità di sistema cifrata da sola non dimostra che tutti gli altri luoghi di archiviazione siano cifrati.

Le copie di sicurezza si trovano esclusivamente su supporti locali cifrati e protetti separatamente. Non esistono copie non cifrate su supporti rimovibili né alcuna sincronizzazione automatica con il cloud. La piattaforma concreta, i volumi coperti e la procedura scelta vengono documentati per l'installazione.

7.2 Trasmissione cifrata

Gli accessi tramite browser avvengono tramite **HTTPS/TLS**. Tutti gli altri percorsi di rete, inclusi il punto terminale del microfono verso il server della scuola, i servizi interni attraverso la rete, la trasmissione delle copie di sicurezza e la manutenzione remota autorizzata, devono essere autenticati e cifrati. I certificati e le controparti vengono verificati; un errore non deve determinare alcun ritorno a una connessione non cifrata.

Un accesso remoto ammesso utilizza inoltre l'accesso sicuro controllato dalla scuola. La semplice appartenenza alla rete scolastica o una password Wi-Fi non sostituiscono la verifica dei singoli percorsi di trasmissione. Un dispositivo collegato solo fisicamente viene valutato come collegamento locale a sé stante e protetto contro l'accesso non autorizzato.

7.3 Chiavi, ripristino e limiti

La scuola stabilisce le persone competenti per le chiavi e il ripristino. Le chiavi di ripristino vengono conservate separatamente dal supporto di dati protetto e in modo accessibile solo alle persone autorizzate; nessuna archiviazione nell'area documenti generale e nessun deposito incontrollato in un account cloud privato.

Durante la configurazione vengono verificati i supporti di dati bloccati, il riavvio, lo sblocco, la revoca dei diritti e il ripristino di una copia di sicurezza cifrata. In caso di sostituzione o dismissione, i dati e le chiavi vanno cancellati in modo controllato.

La cifratura dei supporti di dati protegge in particolare un supporto di memoria bloccato, perso o rimosso. Le applicazioni autorizzate in esecuzione devono poter elaborare i contenuti. Per questo restano inoltre necessari la protezione degli accessi, dispositivi finali sicuri, il filtraggio dei contenuti e la cancellazione. Il PDF pubblico stesso non richiede alcuna password.

Accessi e ulteriori misure di protezione

8. Ruoli e autorizzazioni

Ruolo	Ambito consentito
Studenti	Contenuti di apprendimento dei propri corsi autorizzati; proprie domande all'IA, se approvate. Nessun accesso a chat di altri, funzioni amministrative o testi integrali delle lezioni.
Docenti	Visualizzare i contenuti di apprendimento dei corsi loro assegnati e, facoltativamente, verificarli, correggerli o rimuoverli. La visione delle cronologie individuali degli esercizi richiede una finalità scolastica propria, spiegata in anticipo, e l'autorizzazione corrispondente.
Genitori ed esercenti la responsabilità genitoriale	Nessun accesso automatico. Un accesso in sola lettura consentito separatamente è limitato ai contenuti assegnati e non consente alcuna osservazione generale della classe o di conversazioni di altri.
Dirigenza scolastica / amministrazione	Competenze designate per approvazioni, diritti sui corsi, blocchi e verifiche singole motivate. Un ruolo amministrativo non giustifica alcuna analisi senza motivo di tutte le interazioni di apprendimento.
IT della scuola	Manutenzione tecnica necessaria, backup e ripristino con diritti privilegiati limitati. Nessuna analisi pedagogica autonoma dei contenuti.
Supporto del fornitore	Solo un accesso concretamente incaricato e limitato nel tempo. Nessuna connessione permanente, nessuna auto-approvazione e nessun uso privato dei contenuti delle lezioni.

8.1 Applicazione tecnica

I diritti sui corsi e sui ruoli vengono controllati sul server a ogni interrogazione, ricerca, visualizzazione e modifica. Un pulsante visibile o un accesso valido da soli non sono sufficienti. La revoca di un'autorizzazione termina anche le sessioni esistenti e gli accessi a contenuti ritirati.

Le credenziali di accesso vengono memorizzate in forma protetta; le password non vengono archiviate in chiaro. Gli accessi privilegiati ricevono un fattore di autenticazione aggiuntivo o procedure protette in modo equivalente. Gli account tecnici ricevono solo i diritti necessari al loro compito. I valori di accesso segreti non compaiono nei contenuti di apprendimento o nei registri.

8.2 Esercizio, dispositivi finali e disponibilità

Il server e i supporti di backup si trovano in un'area protetta contro l'accesso fisico non autorizzato. Le esposizioni di rete sono limitate ai servizi necessari; gli accessi a banca dati, modelli e archiviazione non vengono aperti direttamente agli studenti o alle reti domestiche. Gli aggiornamenti di sicurezza, le competenze e le procedure di ripristino sono documentati.

La lettura e le domande interattive all'IA sono approvazioni separate. L'accesso da casa non consente alcun ascolto e non attiva alcun microfono. L'applicazione non crea copie permanenti dei contenuti in banche dati del browser o cache offline. Le scuole regolano i dispositivi finali sicuri e la disconnessione; gli screenshot o le copie private create autonomamente non possono essere impediti completamente con mezzi tecnici.

In caso di guasti è disponibile un'alternativa di apprendimento idonea. Non esiste alcun passaggio automatico a servizi di IA esterni. Le nuove funzioni e i percorsi di dati modificati vengono valutati sotto il profilo della protezione dei dati prima dell'attivazione.

Termini di conservazione e cancellazione

9. Decide la scuola, lo standard è un anno scolastico

La scuola stabilisce la durata di conservazione dei contenuti di apprendimento. Lo standard è un anno scolastico: cancellazione alla fine del rispettivo anno scolastico. Nel regolare anno scolastico bavarese 2026/27 si tratta del 31 luglio 2027. Un contenuto aggiunto successivamente non riceve automaticamente altri dodici mesi. La base per il limite dell'anno scolastico è l'[art. 5 BayEUG](#).

Può essere stabilito un termine più breve. Una conservazione più lunga richiede una finalità ancora ammissibile e necessaria e viene spiegata in anticipo. Una semplice consultazione successiva non prolunga alcun termine. I limiti seguenti sono disposizioni del prodotto; disposizioni applicabili più severe prevalgono.

Dati	Termine / evento di cancellazione
Audio	Nessun file audio memorizzato, nessun archivio e nessuna copia di sicurezza.
Testo non elaborato	Scartato dopo il filtraggio, al più tardi cinque minuti dopo la rilevazione. Nessuna copia di sicurezza.
Contenuti di apprendimento e derivati	Note, materiali, domande/risposte memorizzate e relativi dati di ricerca: data di cancellazione stabilita dalla scuola, per impostazione standard la fine dell'anno scolastico in questione.
Accessi e account	Blocco al termine dell'autorizzazione; cancellazione dei dati dell'account necessari al più tardi 30 giorni dopo.
Registri di sicurezza	Eventi di accesso al massimo 7 giorni; eventi amministrativi particolari come le modifiche dei diritti al massimo 30 giorni. In entrambi i casi senza contenuti delle lezioni o delle conversazioni.
Copie di sicurezza	Cifrate, a rotazione, al massimo 14 giorni. Nessuna ulteriore copia in un archivio senza scadenza. I dati cancellati non devono tornare accessibili tramite un ripristino.
Statistica di esercizio anonima	Solo indicatori complessivi effettivamente anonimi, nella misura in cui la scuola li consente. Periodo stabilito dalla scuola, per impostazione standard la fine dell'anno scolastico; nessuna cronologia individuale né trasmissione al fornitore.

9.1 Catena di cancellazione completa

In caso di cancellazione, il contenuto viene prima escluso dalla visualizzazione, dalla ricerca e dalla consultazione da parte dell'IA. Successivamente vengono ripuliti la fonte, le versioni, le note derivate, le voci di indice, i file e le memorie intermedie ammesse. Cancellare soltanto una nota visibile non è sufficiente se i suoi derivati restano consultabili.

Una copia di sicurezza esistente può contenere ancora al massimo 14 giorni una copia non più accessibile per l'uso. Prima di autorizzare un ripristino, le cancellazioni e le revoche dei diritti avvenute nel frattempo vengono applicate nuovamente. Le procedure di cancellazione non riuscite vengono recuperate e controllate.

Le evidenze legali necessarie relative a consensi, approvazioni o casi di protezione dei dati vengono tenute dalla scuola separatamente, secondo il termine di volta in volta applicabile. Esse non giustificano alcun archivio generale delle lezioni o dell'audio in ContextFriend.

Destinatari, accesso remoto e manutenzione

10. Nessun trattamento esterno dei contenuti delle lezioni

Per questa versione locale sono esclusi i servizi di IA esterni, gli spazi di archiviazione cloud, il tracciamento dei contenuti e l'uso dei dati delle lezioni da parte dei produttori di microfoni o di modelli. L'applicazione utilizza i contenuti esclusivamente per le finalità stabilite dalla scuola. Il download di un modello o un aggiornamento software non trasmette alcun contenuto delle lezioni al fornitore.

L'accesso è concesso solo alle persone autorizzate per il rispettivo corso e la rispettiva finalità nonché, se del caso, agli organismi tecnici espressamente incaricati. La scuola indica i fornitori di servizi effettivamente impiegati e i loro ruoli nella sua informativa specifica per la scuola. Ulteriori responsabili del trattamento (art. 28 GDPR) vengono impiegati solo sulla base contrattuale necessaria e secondo la procedura di autorizzazione concordata.

10.1 Accesso da casa

Un accesso da casa viene autorizzato esclusivamente dalla scuola. La connessione conduce in forma cifrata a un punto terminale controllato dalla scuola e apre solo l'applicazione consentita, nessun accesso generale alla rete scolastica. La sola lettura non consente ancora domande interattive all'IA.

I testi consentiti vengono visualizzati sul dispositivo finale connesso; questa visualizzazione avviene quindi al di fuori dell'edificio scolastico. Gli operatori di rete possono vedere i metadati di connessione. L'IA e il patrimonio di dati di riferimento restano sul server della scuola. Per questa versione non è previsto alcun trasferimento di contenuti delle lezioni a soggetti in paesi terzi; accessi diversi non devono essere attivati tacitamente.

10.2 Accesso del fornitore solo nel singolo caso

TamerinTECH non ha alcun accesso permanente ai dati delle lezioni. Il supporto tecnico viene svolto per quanto possibile senza accesso ai contenuti. Se nel singolo caso è necessaria la visione dei dati, la scuola stabilisce in anticipo finalità, persona incaricata, autorizzazioni, durata e strumenti ammessi. In caso di trattamento di dati personali per conto del titolare, il necessario contratto di trattamento per conto del titolare (art. 28 GDPR) è efficace in anticipo.

La manutenzione remota avviene in forma cifrata verso un dispositivo di supporto protetto e gestito in Germania. Copie dei contenuti, download, stampe, registrazioni e il trasferimento in sistemi di ticket esterni o strumenti di IA non sono consentiti. La sessione termina con l'esecuzione dell'incarico, la scadenza della finestra concordata o la revoca; i diritti residui vengono revocati. Se le possibilità di protezione non sono sufficienti, la manutenzione avviene in loco.

Un'evidenza di manutenzione documenta motivo, persona autorizzata, periodo e misure eseguite, senza includere contenuti delle lezioni. Il supporto non è un'autorizzazione a registrare audio o a creare una propria raccolta di test e addestramento. Un ruolo scolastico privato di un collaboratore del fornitore non fonda alcun diritto aggiuntivo del fornitore.

10.3 Copie di sicurezza e modifiche

Le copie di sicurezza restano su supporti separati e cifrati nell'area di protezione locale stabilita dalla scuola. Competenza, portata del backup, obiettivi di ripristino e test di ripristino periodici vanno documentati. I rischi di un guasto dell'intera sede vengono valutati separatamente; essi non consentono alcuna copia cloud occulta.

Le modifiche a modelli, funzioni, autorizzazioni, luoghi di archiviazione, termini o destinatari vengono valutate prima del loro impiego e aggiornate in modo tracciabile nell'informativa. Un aggiornamento non deve ampliare

tacitamente il concetto di protezione qui descritto.

Diritti e violazioni dei dati

11. Diritti degli interessati

Nei presupposti di legge sussistono i diritti di accesso, rettifica, cancellazione, limitazione del trattamento e, se del caso, portabilità dei dati. In caso di trattamento per un compito di interesse pubblico è possibile opporsi per motivi connessi alla situazione particolare. I consensi prestati sono revocabili per il futuro. Le regole di riferimento si trovano negli artt. da 12 a 22 GDPR.

La scuola titolare o il suo responsabile della protezione dei dati (RPD) ricevono le richieste. L'identità viene verificata solo nella misura necessaria. La risposta avviene di norma entro un mese; su una proroga ammessa dalla legge e sui suoi motivi si informa entro i termini. Un rifiuto viene motivato e corredato delle informazioni previste sui mezzi di tutela.

TamerinTECH supporta la scuola in caso di trattamento su incarico, ma non prende alcuna decisione autonoma sulla divulgazione di dati delle lezioni di terzi. Gli interessati non devono districarsi tra impostazioni tecniche per presentare la loro richiesta.

11.1 Possibilità di reclamo

Competenza	Contatto
Scuole statali bavaresi	Bayerischer Landesbeauftragter für den Datenschutz (autorità bavarese per la protezione dei dati) Casella postale 22 12 19, 80502 München Indirizzo per visitatori: Wagnmüllerstraße 18, 80538 München Telefono: +49 89 212672-0 poststelle@datenschutz-bayern.de www.datenschutz-bayern.de
Soggetti non pubblici in Baviera	Bayerisches Landesamt für Datenschutzaufsicht (ufficio statale bavarese per la vigilanza sulla protezione dei dati) Casella postale 1349, 91504 Ansbach Indirizzo per visitatori: Promenade 18, 91522 Ansbach Telefono: +49 981 180093-0 poststelle@lda.bayern.de www.la.bayern.de

Per altri enti gestori o competenze particolari la scuola indica l'autorità di controllo competente. Le autorità offrono moduli online sicuri per i reclami. Il punto di contatto presso il fornitore e l'autorità di controllo sono soggetti diversi.

12. Errori e incidenti di sicurezza

La divulgazione involontaria, l'accesso non autorizzato, la perdita o altre violazioni dei dati personali vengono segnalate senza indugio attraverso il canale di segnalazione della scuola. I soggetti competenti limitano l'accesso, mettono in sicurezza le evidenze necessarie povertà di contenuti e verificano conseguenze e rimedi. I contenuti di apprendimento interessati vengono bloccati se necessario.

Il titolare del trattamento valuta una notifica all'autorità di controllo ai sensi dell'art. 33 GDPR, di norma entro 72 ore dalla presa di conoscenza, nella misura in cui sussiste l'obbligo di notifica. In caso di rischio presumibilmente elevato, gli interessati vengono informati ai sensi dell'art. 34 senza ingiustificato ritardo. Un responsabile del trattamento informa il titolare senza indugio dopo la presa di conoscenza.

La ripresa dell'esercizio e il ripristino avvengono solo dopo la verifica delle misure di protezione, dei diritti e delle disposizioni di cancellazione. Un'interruzione non giustifica né una registrazione audio né la trasmissione

incontrollata di dati scolastici.

Vincolatività e fonti

13. Configurazione presso la scuola e gestione dei documenti

Per ogni scuola devono essere definiti lo stato effettivo della fornitura, le funzioni, i dispositivi, i modelli, i percorsi dei dati, i termini e i soggetti competenti. La scuola redige la propria informativa concreta e il necessario registro delle attività di trattamento. Verifica l'obbligo di una valutazione d'impatto sulla protezione dei dati; se una valutazione d'impatto (DPIA) è necessaria, deve essere completata prima del trattamento. Un rischio elevato residuo va trattato ai sensi dell'art. 36 GDPR.

Durante la configurazione, in ogni installazione vengono verificati e documentati in particolare: nessuna archiviazione audio anche in caso di errori, filtraggio prima della memorizzazione, il limite di cinque minuti per il testo grezzo, la cifratura di tutti i percorsi di archiviazione e trasmissione, diritti sui corsi efficaci, correzione e ritiro nonché cancellazione incluse le copie di sicurezza. L'assenza di una revisione obbligatoria da parte dei docenti va espressamente considerata nella valutazione dei rischi.

La dirigenza scolastica decide sull'impiego insieme ai soggetti scolastici competenti. Gli interessati vengono informati prima dell'inizio; i consensi necessari vengono raccolti separatamente. Vanno garantite la competenza specifica e un accompagnamento adeguato all'età nell'uso dell'IA. Questo concetto non contiene alcuna promessa statale di autorizzazione o di finanziamento.

La Versione 1.3 del 16 ottobre 2026 vale insieme alla versione breve recante la stessa data. Le modifiche vengono documentate in modo tracciabile. I PDF pubblici non contengono documenti scolastici, contrattuali o di domanda compilati. La scuola riceve separatamente i documenti contrattuali e operativi di cui ha bisogno.

14. Fonti giuridiche e tecniche

1. [Regolamento generale sulla protezione dei dati \(GDPR\)](#), in particolare artt. 5, 6, 9, da 12 a 22, 25, 28, 30, da 32 a 39.
2. [Art. 85 BayEUG](#) sul trattamento dei dati personali; [art. 5 BayEUG](#) sul limite dell'anno scolastico.
3. [§ 46 BaySchO con l'allegato 1](#) sulle attività di trattamento scolastiche; restano da esaminare le ulteriori disposizioni pertinenti per la singola scuola.
4. [Ministero bavarese dell'istruzione: intelligenza artificiale](#), con la guida operativa per la pratica pedagogica del 19 maggio 2026.
5. [§ 38 BDSG](#) sulla designazione dei responsabili della protezione dei dati di soggetti non pubblici; la verifica va effettuata indipendentemente da questa informazione di contatto.
6. [Documentazione del kernel Linux: dm-crypt e cryptsetup/LUKS](#); [Apple: FileVault](#). Le descrizioni delle procedure non sostituiscono la verifica dell'installazione.
7. Fonti dei contatti: [Note legali di ContextFriend](#), [BayLfD](#) e [BayLDA](#). Data di consultazione: 14 ottobre 2026.

Contatto per la protezione dei dati presso il fornitore

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

Per i dati delle lezioni rivolgetevi alla scuola titolare o al suo responsabile della protezione dei dati (RPD). L'informativa semplificata per le famiglie e questa versione completa sono disponibili all'indirizzo context-friend.com/school-documents.