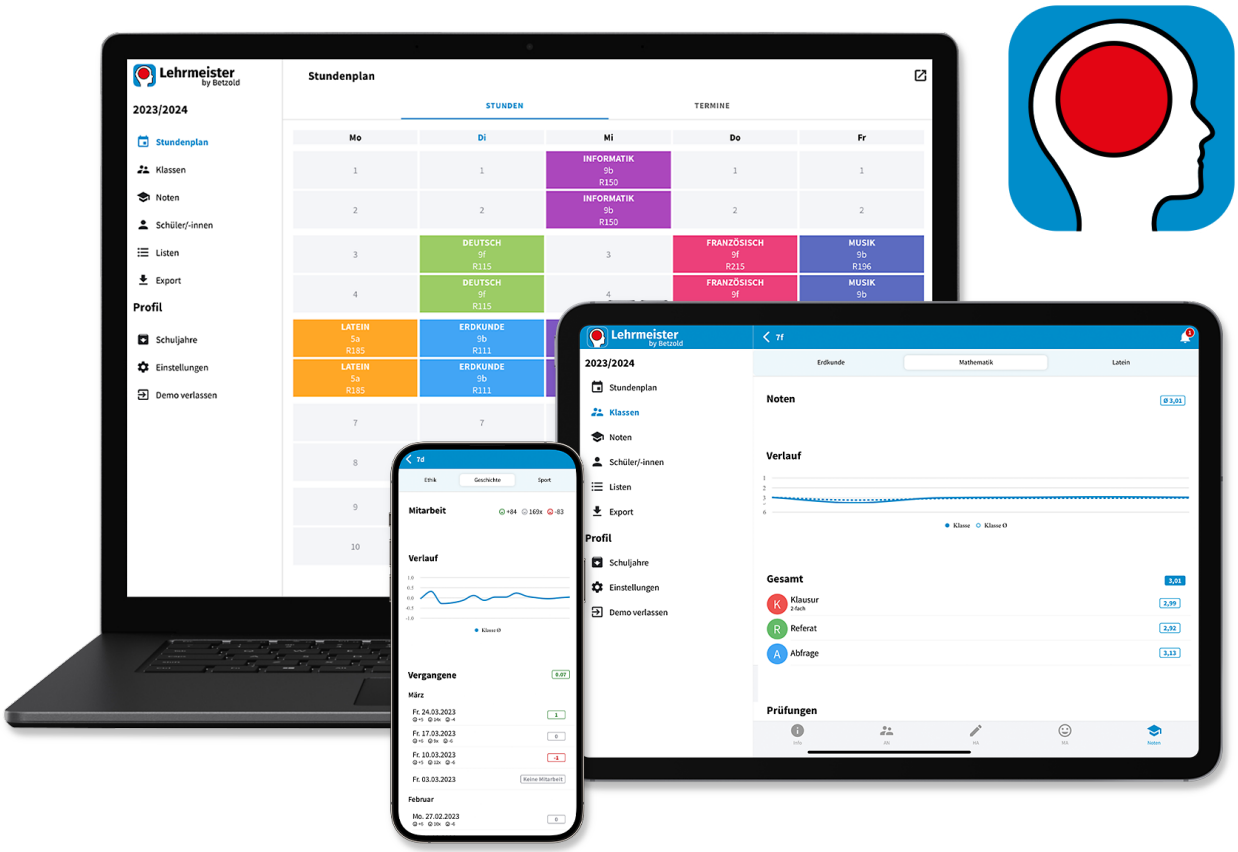
Lehrmeister by Betzold

Die sichere Lehrer-App



www.lehrmeister.eu

Lehrmeister by Betzold - Datenschutz und IT-Sicherheit

Stand: März 2023

Das Grundprinzip von Lehrmeister ist es, **Datenschutz und Benutzerfreundlichkeit** zu verbinden. Oft ist Software entweder gut bedienbar und vernachlässigt dabei leider die Sicherheit oder sie ist sicher, aber schlecht zu bedienen. Gerade bei der Verarbeitung von personenbezogenen Daten sollten jedoch höchste Sicherheitskriterien erfüllt werden.

Im Folgenden wird ausführlich erläutert, wie Lehrmeister das Thema Datenschutz und Datensicherheit behandelt. Die verschiedenen Fragen werden so beantwortet, dass keine besonderen IT-Kenntnisse erforderlich sind, beinhalten aber auch Fachbegriffe für Experten. Dieses Dokument eignet sich also auch, um beispielsweise die Verwendung von Lehrmeister **mit der datenschutzbeauftragten Person deiner Schule** zu besprechen.

Wieso muss ich mich bei Lehrmeister registrieren?

Ohne eine Registrierung kann die **Gefahr eines Datenverlusts** nicht ausgeschlossen werden. Nur durch einen Lehrmeister-Account können wir eine **Kopie deiner verschlüsselten Daten** auf unseren Servern sichern und diese vor dem Verlust bewahren. Ohne Konto sind deine Daten nur lokal auf deinem Gerät gespeichert. Wenn du dein Gerät verlierst, es dir gestohlen wird oder du einfach nur versehentlich den App- bzw. Browser-Cache löschst, sind alle Daten unwiderruflich verloren.

Für dein Konto werden auch nur die **nötigsten Informationen** gespeichert: lediglich **eine E-Mail-Adresse** von dir, die nicht zwingend deinen Namen enthalten muss. Wenn du deinen Account löschst, werden direkt alle Daten vollständig entfernt.

Wenn du deine Daten nicht auf unseren Servern sichern möchtest, kannst du in den Einstellungen der App die **Synchronisation auch deaktivieren**. Allerdings besteht dann die Gefahr, dass die Daten z. B. durch Leeren des Caches gelöscht werden. Die App erinnert dich deshalb regelmäßig daran, ein aktuelles Back-up deiner Daten zu erstellen.

Wie funktioniert die Datenverschlüsselung bei Lehrmeister?

Alle deine Daten werden bei Lehrmeister **Ende zu Ende verschlüsselt**. Das bedeutet, dass sie direkt auf deinem Gerät verschlüsselt und erst danach zum Server übertragen werden. Die Datenübertragung zum Server ist zusätzlich durch den **sichersten Standard (TLS 1.3)** verschlüsselt und durch die Zertifizierungsstelle **„Let's Encrypt"** verifiziert.

Wenn Daten verschlüsselt werden, entsteht beispielsweise aus dem Text „Klasse 10b" eine lange Kombination aus Zeichen, die weder für Menschen noch Maschinen Sinn ergeben. Es gibt verschiedene mathematische Verschlüsselungsverfahren. Lehrmeister verwendet hierfür den weltweit etablierten Standard, die **symmetrische AES-Verschlüsselung** (mit einer Schlüssellänge von 256 bit, die z. B. das „Bundesamt für Sicherheit in der Informationstechnik" (kurz BSI) empfiehlt). Nur mit dem passenden Schlüssel entsteht aus den mit AES verschlüsselten Daten wieder der Text „Klasse 10b". Um

deine Daten zu verschlüsseln, wird also ein sicherer Schlüssel benötigt, der auch durch millionenfaches Ausprobieren nicht erraten werden kann. Wenn du dich bei Lehrmeister registrierst, werden deshalb aus dem von dir gewählten Passwort zwei Varianten erstellt:

Zunächst wird aus deinem Passwort durch eine sogenannte **kryptografische Hash-Funktion** eine lange Kombination aus Zeichen erstellt, sozusagen dein Passwort-Hash. Aus dem Passwort entsteht durch die Hash-Funktion immer wieder der gleiche Passwort-Hash. Allerdings kann umgekehrt vom Passwort-Hash nicht auf das ursprüngliche Passwort geschlossen werden. Nur dieser Hash, niemals dein Passwort, wird bei der Registrierung zu unserem Server gesendet und dort zusammen mit deiner E-Mail-Adresse gespeichert. Wenn du dich anschließend mit deiner E-Mail-Adresse und deinem Passwort anmeldest, wird dein eingegebenes Passwort durch die gleiche Hash-Funktion verarbeitet, der Passwort-Hash zum Server gesendet und dort mit der Datenbank verglichen. Nur bei identischem Passwort sind auch die Hashes identisch und du kannst dich anmelden.

Neben dem Hash zur Authentifizierung wird aus deinem Passwort auch ein **Schlüssel für die Datenverschlüsselung** generiert. Dieser Schlüssel wird **nur auf deinem Gerät gespeichert** und nicht an den Server übertragen. Hierfür verwendet Lehrmeister ebenfalls einen **weltweiten Standard (PBKDF2)**, der u. a. vom „National Institute of Standards and Technology“ (NIST) empfohlen wird. Anschließend werden mit diesem Schlüssel alle Daten, die du eingibst, vor dem Speichern verschlüsselt und beim Auslesen entschlüsselt. Dadurch ist sichergestellt, dass deine Daten niemals im Klartext gespeichert werden, sondern ausschließlich verschlüsselt.

Was passiert, wenn ich mein Passwort vergesse?

Wenn du dein Passwort vergisst, kann **niemand deine Daten entschlüsseln**. Dein Passwort und dein Schlüssel sind nie zu unserem Server übertragen worden. Alles, was gespeichert wurde, ist der Hash-Wert deines Passworts. Selbst wenn wir deinen Account durch die erneute Verifizierung deiner E-Mail-Adresse zurücksetzen, sind alle Daten, die du in die App eingetragen hast, unlesbar. Aber keine Angst, im Internet findest du viele Tipps, wie du dir ein Passwort merken oder zusätzlich sichern kannst. Wir empfehlen hierfür **Passwortmanager-Anwendungen**.

Wenn du dein Passwort trotzdem sichern möchtest, bieten wir dir dafür eine Option bei der Registrierung. Dann wird der aus deinem Passwort erstellte Schlüssel auf unserem Server gespeichert. Zudem kannst du unter Einstellungen in der App jederzeit deinen Schlüssel sichern oder das Back-up wieder löschen lassen. Wenn dein Konto über ein **Schlüssel-Back-up** verfügt, kannst du auch dein Passwort zurücksetzen lassen.

Wer sagt mir, dass das alles so stimmt?

Vertrauen ist gut – Kontrolle ist besser. IT-Sicherheit darf nicht auf Vertrauen basieren, sondern muss immer nachvollziehbar sein und durch ein sicheres Verfahren gewährleistet werden. Lehrmeister wendet das sogenannte **Zero-Knowledge-Prinzip** an. Deine Daten sind sicher, da wir diese, selbst wenn wir wollten, niemals entschlüsseln könnten. Aufgrund des beschriebenen Verschlüsselungsverfahrens kann nur mit dem richtigen Passwort der Datensalat zu sinnvollen und lesbaren Informationen werden.

Mit etwas IT-Wissen kann das sogar überprüft werden. Beispielsweise kannst du die Browserversion von Lehrmeister in Google Chrome starten und über die „Chrome Dev Tools“ nachsehen, welche Daten übertragen werden und was in der lokalen Datenbank auf deinem Gerät gespeichert ist. Alle, die sich mit Web-/Softwareentwicklung und IT-Security auskennen, können also problemlos überprüfen, dass alles so, wie in diesem Dokument beschrieben, abläuft.

Ist Lehrmeister DSGVO-konform?

Ja. Wir erfüllen alle Anforderungen der Datenschutz-Grundverordnung (**EU-DSGVO**). Wir nehmen das Prinzip **Datensparsamkeit** sehr ernst und speichern nur die nötigsten Informationen, die Lehrmeister zum Betrieb benötigt (z. B. deine E-Mail-Adresse). Dies beinhaltet auch, dass wir **keine Third-Party-Webseiten** (z. B. Google Analytics, Google Fonts) einbinden. Wenn du deinen Account löschst, werden sofort alle deine Daten auf unserem Server gelöscht.

Was ist ein Auftragsdatenverarbeitungsvertrag (AVV)?

Ein Auftragsdatenverarbeitungsvertrag (AVV) ist ein Vertrag, der regelt, wie personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden. Wenn du zum Beispiel eine App nutzt, um deine Schüler oder Studenten zu verwalten, musst du sicherstellen, dass die personenbezogenen Daten gemäß den Datenschutzbestimmungen verarbeitet werden. Der AVV definiert die Rechte und Pflichten des Auftragnehmers und des Auftraggebers im Hinblick auf den Datenschutz und stellt sicher, dass die Daten geschützt und gespeichert werden.

Brauche ich für eine rechtssichere Nutzung einen AVV?

Ob du einen AVV benötigst, hängt davon ab, wie du die App nutzt und in welchem Verhältnis du zu deinen Schülerinnen und Schülern oder Studentinnen und Studenten stehst. Wenn du die App privat nutzt, brauchst du keinen AVV. Wenn du sie aber beruflich einsetzt, müsstest du, wenn du personenbezogene Daten deiner Schülerinnen und Schülern oder Studentinnen und Studenten einpflegst, einen AVV abschließen.

Allerdings gibt es rechtlich unterschiedliche Auslegungen, ob es sich bei den durch Nutzerinnen und Nutzer eingepflegten Ende-zu-Ende verschlüsselten Daten tatsächlich um personenbezogene Daten handelt. Im Zweifel solltest du dich am besten mit der Datenschutzbeauftragten Person deiner Institution absprechen. So stellst du sicher, dass du alle gesetzlichen Anforderungen erfüllst und die App rechtssicher nutzen kannst.

Wer schließt einen AVV ab und wo kann man das tun?

Das kann je nach Anstellungsverhältnis variieren. Im Schulkontext: hier schließt nicht die Lehrkraft einen AVV ab, sondern die Institutionsleitung, sprich die Schulleitung.

Eine Institutionsleitung/Schulleitung kann unter folgendem Link einen AVV abschließen:

https://lehrmeister.eu/avv

Nachdem wir den AVV überprüft und freigegeben haben, erhält die Institutsleitung einen Verknüpfungscode. Mit diesem Code lässt sich der abgeschlossene AVV in der App ganz einfach mit einem Nutzerkonto verknüpfen.

Wie ist Lehrmeister vor Sicherheitslücken geschützt?

Es gibt keine Möglichkeit zu beweisen, dass eine Software sicher ist. Auch wenn die aktuellsten Sicherheitsstandards eingehalten werden, gibt es keine Garantie, dass nicht in Zukunft eine Sicherheitslücke gefunden wird. Es gibt aber Möglichkeiten, dieses Risiko zu minimieren. Neben dem Einsatz von empfohlenen Standards und Verfahren verwendet Lehrmeister für sicherheitskritische Bestandteile deshalb **Open-Source-Software-Bibliotheken**. Diese werden von Millionen anderen Softwareprojekten genutzt und unterliegen der ständigen Kontrolle einer Vielzahl an Entwicklungsteams und IT-Security-Fachleuten. Konkret verwendet Lehrmeister beispielsweise **„Let's Encrypt"** für die **TLS-Zertifizierung** und das populärste Open-Source-Paket **node-forge** für **AES** und **PBKDF2**.

Wo sind meine Daten online gespeichert?

Alle Server von Lehrmeister stehen **in Deutschland** und unterliegen somit dem **deutschen bzw. europäischen Datenschutzrecht**. Zudem werden die Server von dem deutschen Unternehmen netcup GmbH betrieben und nicht von amerikanischen Unternehmen wie beispielsweise Amazon AWS, Google Cloud Platform oder Microsoft Azure. Die Server von netcup stehen in Nürnberg und sind zudem nach dem **internationalen Sicherheitsstandard ISO/IEC 27001** zertifiziert.

Was ist das Geschäftsmodell von Lehrmeister?

Entwicklung, Support und Server kosten Geld. Wieso ist Lehrmeister dann kostenlos? Lehrmeister ist von **fünf Studierenden an der Hochschule der Medien in Stuttgart** gestartet und über den Abschluss hinaus weiterentwickelt worden. Wir haben selbst viele Menschen im Freundeskreis und in der Verwandtschaft, die die App im Schulalltag einsetzen. Das positive Feedback unserer Nutzenden motiviert uns zusätzlich, Lehrmeister fortzuführen. Die Tatsache, tausende Lehrkräfte bei der Arbeit zu unterstützen, freut uns und erscheint uns im Vergleich zu vielen Projekten in der IT-Branche als äußerst sinnvoll.

Herzblut allein reicht allerdings auf Dauer nicht aus, um den finanziellen Aufwand durch Serverkosten oder das zeitliche Engagement durch Support und Weiterentwicklung komplett zu decken. Bisher hatten wir mehrere Ansätze im Kopf, das Projekt in der Zukunft zu finanzieren, beispielsweise über Spenden oder exklusive Features für zahlende Nutzende. Mit Betzold als Kooperationspartner haben wir jetzt noch eine weitere Option gefunden. Die Kooperation ermöglicht es uns, unsere App im Moment **weiterhin kostenfrei** anbieten zu können. Zugleich haben wir mit Betzold einen starken Partner im Boot, der unsere Leidenschaft für Bildung teilt und mehr als 50 Jahre Erfahrung im Bildungsbereich aufweist. So können wir nun noch mehr Lehrkräfte mit unserer App erreichen.

Noch Fragen?

Du hast noch Fragen oder es gibt Unklarheiten?
Dann schreib uns einfach eine E-Mail an **lehrmeister@betzold.de**.