Apenschi SOFTWARE

Datenschutzerklärung und Informationen zum Datenschutz

Informationen zum Datenschutz in den Produkten *TAPUCATE* *TAPUCATE* EP1 & EP2

Stand: 01.09.2022

Educate with TAPUCATE!

Inhaltsverzeichnis

1) Vorwort
2) Grundlegende Fragen zum Datenschutz in ***TAP**UCATE*
3) Eingaben in ***TAP**UCATE*
4) Ausgaben aus ***TAP**UCATE*
5) Schutz des Gerätes, auf dem ***TAP**UCATE* verwendet wird
6) Sichere Passwörter

1) Vorwort

Mit ***TAP**UCATE* werden sensible, personenbezogene und amtliche Daten verarbeitet. Dementsprechend hoch sind die Anforderungen an den Schutz dieser Daten. Die Sicherheitsmechanismen von ***TAP**UCATE* müssen daher über das für Apps übliche Maß hinausgehen.

Dieses Dokument informiert den Benutzer detailliert über datenschutzbezogene Vorgehensweisen und Funktionen von ***TAP**UCATE*, sowie potentielle Risiken und Möglichkeiten, wie diese minimiert werden können.

Es gibt in ***TAP**UCATE* ein ganze Reihe von Maßnahmen, um die Daten zu schützen. Die deutlichste davon ist der Verzicht auf jegliche Verbindungen zu Datennetzen (Internet, eMail, usw.) und Apps (Kontakte, Kalender, usw.). D.h. ***TAP**UCATE* ist technisch gar nicht in der Lage, Daten ins Internet oder über andere Wege zu übertragen. Umgekehrt kann ***TAP**UCATE* dadurch auch über diese Netze nicht erreicht, also auch nicht selbst angegriffen werden. Der Verzicht auf diese Funktionen ist das wichtigste Sicherheitsfeature von ***TAP**UCATE* und ein Alleinstellungsmerkmal gegenüber nahezu allen anderen Lehrer-Apps!

Aber auch eine perfekt abgesicherte App ist machtlos, wenn der Benutzer leichtsinnig agiert und die Absicherung des Gesamtsystems vernachlässigt. Auch in dieser Hinsicht soll dieses Dokument den Benutzer unterstützen und nützliche/wichtige Hinweise liefern.

Die nachfolgenden Aussagen gelten für die beiden ***TAP****UCATE*-Apps ab Update 1.7, sowie für die Erweiterungs-Apps EP1 und EP2.
Es ist möglich, dass zukünftig weitere Erweiterungen und Zusatz-Apps für ***TAP****UCATE* erscheinen, für die wir gegebenenfalls eigene Datenschutzerklärungen veröffentlichen.

2) Grundlegende Fragen zum Datenschutz in *TAPUCATE*

Welche Berechtigungen werden verwendet?
Bei der Installation von Apps werden dem Benutzer die Berechtigungen angezeigt, welche die jeweilige App verwendet. Der Benutzer muss diese Berechtigungen bestätigen, um die App installieren zu können. Ohne die entsprechenden Berechtigungen kann eine App bestimmte Funktionen nicht ausführen.

TAP*UCATE* verwendet die folgenden Berechtigungen:

WRITE_EXTERNAL_STORAGE
Erlaubt einer App den Schreib- und Lesezugriff im primären (=eingebauten) und den Lesezugriff im sekundären Speicher (SD-Karte). Das Schreiben auf die SD-Karte ist im Allgemeinen nicht erlaubt (lediglich in einem App-Spezifischen verzeichnis), wird aber von einigen Geräterherstellern in Android-Versionen unterhalb von 4.4.2 zugelassen.

TAP*UCATE* benötigt diese Berechtigung, um Datensicherungen, CSV- und PDF-Exporte sowie Log-Dateien in einem Speicher ablegen zu können, der dem Benutzer zugänglich ist.

CHECK_LICENSE
Erlaubt einer App die Prüfung der Lizenz, um sicherstellen zu können, dass die App legal erworben wurde. Die Prüfung selbst wird von einem Dienst des Gerätes durchgeführt, der das Ergebnis dann er App mitteilt. D.h. die App muss dafür selbst keine Internet-Verbindung aufbauen.

VIBRATE
Erlaubt einer App die Aktivierung des Vibrationsalarms des Gerätes.

***TAP**UCATE* verwendet dies, um den Benutzer bei bestimmten Aktionen ein haptisches Feedback geben zu können. Im Sitzplan z.B. wird dem Benutzer nach langem Drücken durch eine Vibration signalisiert, dass die Schülerkachel in den Verschiebe-Modus gewechselt ist.

Außer den hier genannten drei Berechtigungen verwendet ***TAP**UCATE* keine weiteren!

Welche der in ***TAP**UCATE* erfassten Daten werden von ***Apenschi Software*** verarbeitet und gespeichert?

Keine!

***TAP**UCATE* speichert und verarbeitet alle Daten ausschließlich lokal auf dem Gerät des Lehrers. Es findet keine Datenübertragung nach Apenschi Software (oder Dritten) statt und es ist Apenschi Software technisch auch nicht möglich, auf die Daten auf den Geräten zuzugreifen.

Welche Daten werden von ***TAP**UCATE* automatisch erhoben?

***TAP**UCATE* erhebt selbst keinerlei Daten automatisch! Alle von ***TAP**UCATE* gespeicherten Daten werden vom Benutzer eingegeben oder durch Benutzeraktionen unmittelbar erzeugt.
Grundsätzlich (also auch auf Benutzerinteraktion hin) speichert ***TAP**UCATE* keine Standortdaten, ruft keine Kontakt- oder Kalenderdaten oder andere personenbezogene Daten externer Apps ab.

Welche Daten müssen für die Verwendung von ***TAP**UCATE* eingegeben werden?

***TAP**UCATE* macht keinerlei Vorgaben für die zu erfassenden Daten. Der Nutzer kann frei entscheiden, wieviele und welche Daten er in ***TAP**UCATE* erfasst. Auch die anonyme Erfassung der Daten ist möglich.

Wo werden die Daten von ***TAP**UCATE* gespeichert?

Die Daten werden von ***TAP**UCATE* in einem geschützten Bereich auf dem Gerät gespeichert, auf den nur ***TAP**UCATE* zugreifen kann (Ausnahme ist das „Rooten“ des Gerätes, von dem abzuraten ist). Benutzer und andere Apps haben auf den Speicherbereich keinen Zugriff!
Vom Benutzer erzeugte Exporte speichert ***TAP**UCATE* im öffentlich zugänglichen ***TAP**UCATE*-Verzeichnis, damit diese dem Benutzer zugänglich sind (siehe Kapitel 3 → Exporte).

Wie lange werden die Daten von ***TAP**UCATE* gespeichert?

Die Dauer der Speicherung wird vom Benutzer festgelegt. Die Speicherung beginnt mit der Erfassung der Daten durch den Benutzer und endet, sobald dieser die Daten wieder löscht.

Wie können die in ***TAP**UCATE* erfassten Daten restlos wieder gelöscht werden (z.B. bei Deinstallation der App)?

***TAP**UCATE* verfügt über eine Funktion mit deren Hilfe die erfassten Daten zuverlässig und vollständig gelöscht werden können (MENÜ → DATEN LÖSCHEN → ALLE DATEN LÖSCHEN)

Welche Daten werden von ***TAP**UCATE* oder Apenschi Software an Dritte weitergegeben?

Apenschi®Software und damit auch ***TAP**UCATE* geben grundsätzlich keinerlei Daten an Dritte weiter.

Welche Daten werden von ***TAP**UCATE* an andere Geräte/Server gesendet?

***TAP**UCATE* sendet grundsätzlich keine Daten (siehe auch → „Welche Berechtigungen werden verwendet?“) , an andere Geräte oder Server.
Der Benutzer kann in ***TAP**UCATE* eMails erzeugen, die aber ebenfalls nicht von ***TAP**UCATE* selbst versendet werden (siehe Kapitel 3 → eMails).

Wie werden die Daten von ***TAP**UCATE* verschlüsselt?

***TAP**UCATE* verwendet AES-256 für die Verschlüsselung der Daten. Es wurde bei der Umsetzung der Verschlüsselung besonders darauf geachtet, typische Fehler, die zu einer Schwächung des Verfahrens führen können, zu vermeiden und innerhalb der AES-Varianten die sicherste Konfiguration zu wählen (siehe unten).
AES ist bereits seit langer Zeit im Einsatz, ohne das bisher nennenswerte Schwachstellen gefunden wurden und gilt als sehr sicher.

Datensicherungen werden von ***TAP**UCATE* vollverschlüsselt. Zusätzlich werden bestimmte Felder, die zur Identifizierung von Schülern verwendet werden könnten, auch innerhalb der Datenbank verschlüsselt (z.B. Name, Vorname, Geburtsdatum, Adresse, Kontakte, Geschlecht, Religion, usw.).

Zur Nachvollziehbarkeit für Experten hier die Eigenschaften des verwendeten AES Algorithmus:

- 256-Bit Schlüssellänge
- PKCS5 Block Padding
- Salt
- Cipher Block Chaning (CBC)
- Key Derivation (PBKDF2WithHmacSHA1)

Wie wird der Zugang zu ***TAP**UCATE* gesichert?

Für ***TAP**UCATE* kann ein eigenes Zugangspasswort festgelegt werden, welches nach einer einstellbaren Zeit (minimal 5 sek.) nach dem Verlassen von ***TAP**UCATE* wieder eingegeben werden muss, um auf die Daten zugreifen zu können. Solange kein korrektes Passwort eingegeben wurde, ist nur ein Sperrbildschirm sichtbar.

Dies dient der Absicherung gegen kurzfristige Zugriffe, z.B. weil das Gerät eingeschaltet für kurze Zeit unbeaufsichtigt bleibt (z.B. weil der Benutzer kurzzeitig den Raum verlässt), kann aber die Schutzmechanismen des Gerätes selbst nicht ersetzen, sondern nur ergänzen! Nutzen Sie daher immer alle Schutzmechanismen Ihres Gerätes!

Wie verarbeitet und schützt ***TAP**UCATE* die Schülerfotos?

Schülerfotos können in TAPUCATE auf drei verschiedene Arten hinzugefügt werden.

1) Im Rahmen des CSV-Imports
2) Durch direktes Fotografieren
3) Durch Auswahl eines bereits vorhandenen Fotos

Bei allen drei Methoden legt ***TAP**UCATE* verkleinerte Kopien der Fotos in seinem geschützten Speicherbereich ab und verschlüsselt diese mit dem oben genannten Verfahren. Die ursprünglichen Namen der Fotos tauscht ***TAP**UCATE* gegen eine Nummer aus. Der Benutzer und andere Apps haben keinen direkten Zugriff auf die Fotos. Es gibt für die Fotos eine eigene Datensicherungsfunktion, welche alle vorhandenen Schülerfotos in einer zusätzlich verschlüsselten Datei ablegt.

Die in den Schülerdatensätzen hinterlegten Verweise auf die zugehörigen Fotos werden verschlüsselt in der Datenbank abgelegt.

In den Einstellungen kann die Auflösung der von TAPUCATE erzeugten und verwendeten Schülerfotos eingestellt werden. Aus Datenschutzgründen ist es sinnvoll, die Auflösung so gering wie möglich zu wählen. Idealerweise ist die Auflösung so gering, dass die Schüler nur noch schwer erkennbar sind.

Beachten Sie bzgl. der Schülerfotos bitte die folgenden Punkte:

- Je nach Land und Anwendungszweck gibt es unterschiedliche datenschutzrechtliche Anforderungen an die Verwendung von Schülerfotos. Praktisch immer ist die explizite Einwilligung der Betroffenen notwendig! Bitte beachten Sie die für Sie geltenden Datenschutzregelungen!
- Unmittelbar nach dem Import sollten die Originalfotos gelöscht werden. TAPUCATE übernimmt das, wenn Sie den nach dem Import erscheinenden Dialog entsprechend bestätigen.
- Auch nach dem direkten Fotografieren/der Auswahl aus der Galerie sollten die Originale vom Mobilgerät entfernt werden. Hierauf hat TAPUCATE keinen Einfluss, d.h. das liegt in der Verantwortung des Benutzers.
- Verwenden Sie möglichst eine sehr geringe Auflösung für die Fotos

Was passiert, wenn ich das Passwort für meine Datensicherungen vergesse?

Datensicherungen werden von ***TAP**UCATE* mit einem sehr sicheren Verfahren verschlüsselt. Es gibt definitiv keine Möglichkeit, die Daten ohne das korrekte Passwort zurückzugewinnen! Sie sollten Ihre Passwörter deshalb immer sorgfältig und an einem sicheren Ort notieren und bei deren Eingabe sorgfältig vorgehen!

***TAP**UCATE* verfügt über eine Archiv-Funktion, mit der Datensicherungen vorübergehend und ohne Gefahr für den aktuellen Datenbestand geöffnet werden können. Nutzen Sie diese Funktion regelmäßig, um Ihre Datensicherungen auf Funktionsfähigkeit und korrektes Passwort zu überprüfen!!

3) Eingaben in *TAP*UCATE

Eingaben sind in ***TAP**UCATE* über die Bedienoberfläche der App oder per CSV Import möglich.
Zusätzlich kann durch die Wiederherstellung von Datensicherungen die Datenbank auch direkt gefüllt werden. Dies ist mit Datensicherungen möglich, die entweder mit ***TAP**UCATE* erstellt oder mit Hilfe der ***TAP**UCATE*-Tools auf dem PC erzeugt wurden.

***TAP**UCATE* bietet eine Vielzahl von Eingabefeldern, die aber nur in Ausnahmefällen alle verwendet werden. ***TAP**UCATE* macht keinerlei Vorgaben dafür, welche Felder genutzt werden müssen und welche Daten eingegeben werden müssen. Die Entscheidung über Art und Umfang der eingegebenen Daten liegt also allein beim Anwender.
Beachten Sie die für Sie geltenden Datenschutzbestimmungen!

4) Ausgaben aus *TAP*UCATE

Exporte
Daten können über Exportfunktionen von ***TAP**UCATE* ausgegeben werden. Alle Exporte werden vom Benutzer selbst veranlasst, finden also nie automatisch statt. Es gibt drei Arten von Exporten: CSV, PDF und Datenbankexporte.

CSV Exporte speichern die jeweiligen Daten in Textform, damit diese von anderen

Programmen weiterverarbeitet werden können. CSV-Dateien können naturgemäß nicht verschlüsselt werden und sollten vom Benutzer sobald wie möglich vom Gerät gelöscht werden.

PDF Exporte speichern die vom Benutzer gewählten Daten in PDF-Dokumenten. PDF Exporte können optional mit dem PDF-internen Verschlüsselungsverfahren verschlüsselt werden (in den Einstellungen kann zu diesem Zweck ein Passwort hinterlegt werden).

eMails

In ***TAP****UCATE* können eMails aus vorgefertigten Textblöcken mit den erfassten eMail-Adressen erzeugt werden. ***TAP****UCATE* verschickt diese eMails grundsätzlich nicht selbst. Stattdessen kann der Benutzer eine externe eMail-App auswählen, an welche der Text der eMail und evtl. Anhänge übergeben werden. Der Benutzer versendet die eMails dann mit der gewählten App selbst und hat zuvor die Möglichkeit den Inhalt der eMail vollständig zu prüfen.
Aufgrund dieser Vorgehensweise ist es leider nicht möglich, individuelle Serien-eMails zu versenden. Lediglich Serien-eMails mit dem gleichen Inhalt können (durch automatisches Befüllen des BCC-Feldes der externen eMail App) erzeugt werden.

Datensicherungen

Datensicherungen sind vollständige Kopien des Datenbestandes mit dem primären Ziel, die Daten in ***TAP****UCATE* wieder herstellen zu können.
Ein weiterer Anwendungsfall ist die Archivierung von Daten. Mit Hilfe der Archiv-Funktion können ältere Datensicherungen temporär eingesehen werden. Datensicherungen sind immer vollständig verschlüsselt und können daher nur in ***TAP****UCATE* selbst bzw. ***TAP****UCATE*-Tools auf dem PC verwendet werden. Für die Verwendung ist die Eingabe des korrekten Passwortes notwendig. **Ohne das korrekte Passwort sind die Daten definitiv nicht mehr verwendbar!!**

(!) Achten Sie darauf, das nach Im- und Exporten keine Dateien auf dem Gerät gespeichert bleiben. Löschen Sie exportierte Dateien, sobald Sie deren Weiterverarbeitung (Drucken, Kopieren auf sichere Datenträger,…) abgeschlossen haben.

5) Schutz des Gerätes, auf dem *TAPUCATE* verwendet wird

Trotz der Schutzmechanismen in ***TAP**UCATE* ist es für eine vollständige Absicherung notwendig, auch die Schutzfunktionen des Gerätes immer konsequent zu nutzen!
Bei der Verwendung von ***TAP**UCATE* sollten unbedingt die nachfolgenden Punkte befolgt werden:

- Schalten Sie Ihr Gerät nicht für die Installation von Apps aus „Unbekannten Quellen“ frei
- Seien Sie mit der Installation von Apps möglichst sparsam und installieren Sie nur Apps, die bereits von vielen anderen verwendet werden und positiv bewertet wurden
- Rooten Sie Ihr Gerät nicht und verwenden Sie keine Custom-ROMS (wenn Sie nicht wissen was das ist, haben Sie es wohl auch nicht getan)
- Nutzen Sie eines der sicheren Sperr-Verfahren für Ihr Gerät
- Lassen Sie das Gerät immer nach kurzer Zeit schon sperren
- Verwenden Sie die Verschlüsselung des Gerätes
- Verwenden Sie die Verschlüsselung der SD-Karte
- Nutzen Sie die Angebote der Hersteller zur Lokalisierung und Fernlöschung von verlorenen Geräten

6) Sichere Passwörter

Schlechte Passwörter sind die häufigste und die am meisten unterschätzte Sicherheitslücke!

Bei der Wahl eines sicheren Passwortes müssen Sie berücksichtigen, dass Hacker wesentlich geschickter beim Erraten von Passwörtern vorgehen, als sich das die allermeisten Computernutzer vorstellen können. Hacker verwenden regelmäßig gestohlene Passwortdatenbanken, um typische menschliche Verhaltensweisen der Nutzer zu analysieren und auszunutzen.

Versuchen Sie deshalb nicht, die Sicherheit Ihrer Passwörter selbst zu beurteilen, sondern halten Sie Sich strikt an die nachfolgenden Regeln!

Als grobe Regel kann man sagen, dass ein Passwort immer dann unsicher wird, wenn es bequem einzugeben und zu merken ist.

1) Ein Passwort muss heutzutage mindestens 8 Zeichen lang sein. Für kritische Passwörter ist ein Länge von mindestens 12 Zeichen zu empfehlen.

2) Ein Passwort sollte Zahlen beinhalten, die sich **nicht** ausschließlich am Ende des Passwortes befinden!

3) Ein Passwort sollte keine für die Deutsche Sprache typischen „sprechbaren“ Buchstabenkombinationen beinhalten! Am besten man verzichtet komplett auf Vokale.

4) Ein Passwort sollte mehrere Sonderzeichen wie „!&$%/()=[]{\'#*+~ beinhalten.

5) Ein Passwort sollte Groß- und Kleinbuchstaben beinhalten.

Erläuterungen:

<u>Zu Regel 1:</u>
Hacker verfügen heute teilw. über eine unvorstellbare Rechenpower, die früher Supercomputern vorbehalten war. Sie können in Sekunden zig Millionen von Passwörtern durchprobieren. Dabei probieren sie keinesfalls nur systematisch Buchstabenkombinationen ab, sondern verwenden „Wörterbücher“, welche Passwörter in der Reihenfolge ihrer Wahrscheinlichkeit beinhalten!

<u>Zu Regel 2:</u>
Hacker wissen, dass die meisten Nutzer Zahlen (wenn überhaupt) oft nur am Ende eines Passwortes verwenden und dass es sich dabei dann oft um Jahreszahlen oder um Kombinationen handelt, die für die jeweilige Nutzergruppe als Geburtsdatum in Frage kommt (sie werden als Erstes Zahlenpaare bis 31 bzw. bis 12 sowie die Zahlen 14 bis 50, bzw. 1950 bis 2014 durchprobieren).

<u>Zu Regel 3:</u>
Hacker nutzen es aus, dass Nutzer Passwörter verwenden, die leicht zu merken sind.

Zu Regel 4 und 5:

Wenn man nicht ein möglichst breites Spektrum an zur Verfügung stehenden Zeichen verwendet, schwächt man effektiv das Verschlüsselungsverfahren. Weil die Anzahl möglicher Kombinationen zurückgeht, wird aus einem Verfahren mit einem 256-Bit Schlüssel schnell eines mit nur 80-Bit.

IMPRESSUM

Herausgeber und für den Inhalt verantwortlich:

Apenschi® SOFTWARE

Andreas Schilling
Finkenweg 12
33178 Borchen
Fax 032223943730
info@tapucate.de

Der Herausgeber ist bemüht, die Informationen in dieser Publikation korrekt und aktuell zu halten, kann aber weder für Aktualität, noch Richtigkeit oder Vollständigkeit eine Gewähr übernehmen. Er behält sich vor, den Inhalt dieser Publikation jederzeit zu ändern oder ganz zu entfernen. Der Herausgeber übernimmt, abgesehen von nachgewiesenem vorsätzlichem oder grob fahrlässigem Handeln, grundsätzlich keinerlei Haftung für Schäden, die durch die Verwendung, nicht-Verwendung oder Fehlerhaftigkeit der hier bereitgestellten Informationen und Medien entstehen.

Alle Texte, Bilder und sonstige Medien in dieser Publikation: (C) 2022 Apenschi Software Vervielfältigung und Weiterverarbeitung jeglicher Art bedarf der schriftlichen Genehmigung. Alle Rechte vorbehalten.

Apenschi® ist eine eingetragene Marke.
Android™, Google™, und GoogleDrive™ sind Marken von Google LLC.

Auch bei anderen Begriffen und Bildern in diesem Handbuch kann es sich um Marken oder eingetragene Marken handeln. In diesem Fall liegen die Rechte an diesen Marken bei den jeweiligen Rechteinhabern.

Vielen Dank, dass Sie ***TAP****UCATE* verwenden!!

Educate with ***TAP****UCATE!*