Die App Classroom und die DSGVO

Vorbemerkung

Die nachfolgenden Informationen richten sich in erster Linie an den Datenschutzbeauftragten Ihrer Schule, damit dieser bzw. Ihr Schulleiter Ihnen die Verwendung der App Classroom genehmigen kann. Aber auch Sie als Nutzer der App finden hier Informationen wie die personenbezogenen Daten Ihrer SchülerInnen verarbeitet und gespeichert werden.

Grundsätzlich werden die Daten ausschließlich lokal auf Ihrem Gerät verarbeitet. Eine Übermittlung von Daten – mit Ausnahme der im Weiteren erläuterten Exportfunktion – findet weder an den Herausgeber der App noch an Dritte statt. Damit ist Ihre Schule die verantwortliche datenverarbeitende Stelle im Sinne der DSGVO. Alle Rechte und Pflichten, die sich aus der Verwendung der App Classroom ergeben, gelten zwischen Ihrer Schule (vertreten durch Sie) und Ihren SchülerInnen bzw. deren Erziehungsberechtigen.

Welche personenbezogenen Daten werden verarbeitet bzw. gespeichert?

- Name des Schülers
- Foto des Schülers im Sitzplan (optional)
- Zugehörigkeit des Schülers zu einer oder mehreren Klassen bzw. Kursen
- E-Mail-Adresse (optional, nicht im- oder exportierbar)
- Erinnerungen (freier Text)
- Noten (mit frei wählbarem Datum und frei konfigurierbarem Notensystem)
- Einzelpunkte in Schulaufgaben/Tests und der sich ergebenden Note
- Klassenbucheinträge aus frei konfigurierbaren Kategorien (z.B. vergessenen Hausaufgaben, Verspätung, …) mit frei wählbarem Datum
- Checklisteneinträge (Sie können freie Checklisten z.B. „Elternbrief abgegeben“ erstellen und jeden Schüler darin abhaken)
- Stundenplan, also welche Klasse an welchem Wochentag zu welcher Zeit unterrichtet wird

Wie werden die Daten gespeichert?

Die Daten werden in einer Datenbank komplett in einer einzelnen Datei lokal auf Ihrem Gerät gespeichert. Eine Verschlüsselung der Datenbankdatei ist möglich, aber nicht vorgeschrieben. Der verwendete Verschlüsselungsalgorithmus AES-256 gilt nach derzeitigem Wissensstand als sicher und nicht brechbar, falls ein ausreichend gutes Passwort verwendet wird.

Wird eine verschlüsselte Datenbank verwendet, dann wird die Datenbankdatei für jeden Datenzugriff lokal auf dem Gerät komplett entschlüsselt und anschließend wieder komplett verschlüsselt. Temporär unverschlüsselte Daten werden sofort nach dem Zugriff wieder gelöscht. Das Passwort kann vorübergehend (bis zum Verlassen der App) oder dauerhaft (verschlüsselt in der iOS Keychain) gespeichert werden, so dass die Ver- und Entschlüsselung vollständig im Hintergrund abläuft.

Welche Daten können exportiert werden?

Jeder Export von Daten erfolgt ausschließlich durch eine Aktion des Nutzers. Eine automatische Übermittlung von Nutzungsdaten oder anderer Daten an den Herausgeber der App oder Dritte erfolgt grundsätzlich nicht.

a) Die Datenbankdatei kann durch Einstellung des Nutzers nicht nur lokal auf dem Gerät gespeichert werden, sondern zusätzlich in der iCloud des Nutzers oder in einem verknüpften Dropboxkonto des Nutzers. Die Verschlüsselung erfolgt dann mit demselben Passwort, das der Nutzer für die lokale Speicherung verwendet. Die Speicherung kann manuell, automatisch in regelmäßigen Intervallen oder automatisch bei jeder Datenänderung erfolgen.

b) Backups: Backups können in einstellbaren Intervallen (z.B. täglich oder wöchentlich) erstellt werden, während die App verwendet wird. Die Backups werden auf Wunsch des Nutzers lokal oder in der iCloud des Nutzers oder in einem verknüpften Dropboxkonto des Nutzers gespeichert. Die Verschlüsselung der Backups erfolgt dann mit demselben Passwort, das der Nutzer für die Datenbankdatei verwendet.

c) Screenshots: Der Sitzplan und die Notenübersicht einer Klasse können als Bilddatei exportiert werden und z.B. gedruckt oder als E-Mail verschickt werden.

d) Bild-Export: Die Fotos der SchülerInnen können in der Foto-Mediathek Ihres Geräts gespeichert werden.

e) CSV-Export: Die Datenbank kann in Textform per E-Mail verschickt werden oder in ein verknüpftes Dropboxkonto des Nutzers gespeichert werden. Diese Textdatei enthält dann die Namen, die Klasse, die Noten (mit Datum) und die Klassenbucheinträge (mit Datum) aller Schüler der gesamten Datenbankdatei. Der Export erfolgt unverschlüsselt.

f) Synchronisation über iCloud oder Dropbox: Wenn die Datenbankdatei in der iCloud oder Dropbox gespeichert ist (siehe a), dann kann der Nutzer die Datenbankdatei auf mehreren Geräten mit dem gleichen iTunes-Account oder dem gleichen Dropboxkonto verwenden. Die App prüft dann regelmäßig, ob in der iCloud oder in dem Dropboxkonto eine Änderung vorliegt und lädt die Datei auf des Gerät herunter. Ebenso wird jede Änderung der Daten auf dem Gerät automatisch in die iCloud oder die Dropbox gespeichert. Zur Verschlüsselung siehe a)

Wer hat Zugriff auf die Daten?

- Geschützter Speicherort: Alle lokalen Dateien liegen in einem Verzeichnis auf dem Gerät, auf das nur die App Classroom Zugriff hat. Keine anderen Apps können auf die Dateien zugreifen.
- Passwortschutz des Geräts: Es wird empfohlen, den Zugriff auf iOS durch Passwort, FaceId oder TouchId zu schützen.
- Zusätzlich bietet die App die Möglichkeit der Zugangskontrolle durch ein Passwort oder TouchId. Dadurch können unbefugte Personen keine Daten in der App Classroom sehen, selbst wenn Sie das Gerät kurz unbeaufsichtigt im Klassenzimmer oder Schülerhand lassen.

Wie kann man die App Classroom DSGVO-konform verwenden?

- Verschlüsseln Sie die Datenbankdatei mit einem sicheren Passwort. Dieses Passwort sollten Sie in der App nicht dauerhaft, sondern nur bis zum Verlassen der App hinterlegen.
- Stellen Sie ein, dass Sie die App nur mittels TouchId oder Passworteingabe öffnen können, um unbefugten Datenzugriff durch Schüler oder KollegInnen zu verhindern.
- Erstellen Sie regelmäßig Backups, die lokal auf dem Gerät gespeichert werden, um unbeabsichtigte Änderungen von Daten rückgängig machen zu können.
- Erstellen Sie regelmäßig Systembackups von Ihrem Gerät über iTunes, die lokal auf diesem zweiten Computer gespeichert werden, um unbeabsichtigten Datenverlust verhindern zu können.
- Stellen Sie Ihr Gerät so ein, dass die Systembackups nicht in der iCloud gespeichert werden.
- Speichern Sie keine Dateien in der Dropbox oder iCloud, auch nicht verschlüsselt. Der verwendete Verschlüsselungsalgorithmus gilt zwar derzeit als sicher, aber es kann nicht mit Sicherheit ausgeschlossen werden, dass die Dateien in der Zukunft unbefugt entschlüsselt werden könnten.
- Verschicken Sie keine personenbezogenen Daten per E-Mail. Benutzen Sie nicht die Funktion des CSV-Export.
- Erfassen Sie nur Daten (wie Noten und Klassenbucheinträge), die zur Berechnung der Zeugnisnote erforderlich sind.
- In manchen Bundesländern ist das Speichern von Bildern Ihrer Schüler auf privaten Geräten grundsätzlich nicht erlaubt. In allen anderen Fällen benötigen Sie das Einverständnis der SchülerInnen bzw. deren Erziehungsberechtigten zur Speicherung der Bilder. Exportieren Sie keine Bilder in die iCloud.
- Löschen Sie alte Datenbankdateien und auch deren Backups, wenn das Schuljahr beendet ist und die Daten nicht mehr benötigt werden.

Hinweise

Es gibt viele Wege, um mit personenbezogenen Daten von Schülern schlecht oder rechtswidrig umzugehen. Natürlich ist dies auch mit der App Classroom möglich. Aber bei einem verantwortungsvollen Umgang mit den Daten Ihrer Schüler sollte die DSGVO der Verwendung von Classroom nicht im Wege stehen. Bitte beachten Sie, dass dieses Dokument keine Rechtsberatung darstellt, sondern Sie und den Datenschutzbeauftragten Ihrer Schule bei der Entscheidung unterstützen soll, ob und wie Sie die App Classroom DSGVO-konform verwenden können.

Sollten Sie weitere Fragen haben, schreiben Sie bitte eine E-Mail an support@reissl.com.

Stefan Reißl, Herausgeber der App Classroom für iOS

Stand 13.08.2019