Informationen zum Datenschutz in SchILD*app*

Stand: 01.12.2017

ribeka

Die SchILD-Entwickler

Inhalt

1. Welche Zugriffsberechtigungen werden von SchILD*app* verwendet?

- **INTERNET**

Diese Berechtigung erlaubt einer App eine vorhandene Internetverbindung (WLAN oder Mobilfunk) zu nutzen, um Daten zu übertragen.

SchILD*app* benötigt diese Berechtigung um mit dem SchILD-Webserver Ihrer Schule zu kommunizieren. Um über SchILD*app* Daten mit Ihrer lokalen SchILD-Datenbank (SchILD-NRW oder SchILD*zentral*) austauschen zu können, wird ein auf einem schuleigenen Webserver installierter Kommunikationsserver verwendet. Dieser prüft die Zugriffsberechtigungen von SchILD*app* respektive der angemeldeten Lehrkraft und verwaltet die Datensynchronisation. SchILD*app* benötigt nur Zugriff auf das Internet um sich mit diesem Kommunikationsserver (Webserver) zum Datenaustausch verbinden zu können.

- **READ_PHONE_STATE (Telefonstatus und Identität abrufen)**

Diese Berechtigung ermöglicht einer App die IMEI, SIM-Kartennummer, eigene Telefonnummer, Telefonnummer des Anrufenden sowie den Namen des Telefonproviders auszulesen und festzustellen, ob Anrufe eingehen und Gespräche geführt werden.

SchILD*app* nutzt diese Berechtigung ausschließlich zum Auslesen der IMEI (International Mobile Equipment Identity). Die IMEI ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät weltweit eindeutig identifiziert werden kann. Damit SchILD*app* mit der SchILD-Datenbank Ihrer Schule kommunizieren kann, muss das betreffende Mobilgerät vorher durch Hinterlegen der IMEI in SchILD freigeschaltet werden. Vor jedem Datentransfer zwischen SchILD*app* und SchILD wird die Zugriffsberechtigung des Mobilgeräts anhand der IMEI geprüft.

- **CAMERA**
  Diese Berechtigung erlaubt einer App den Zugriff auf die integrierte Kamera.

Mit SchILD*app* können Fotos von SchülerInnen aufgenommen werden, welche in den Schülerinformationen und in den Sitzplänen der Anwendung angezeigt werden können. Die aufgenommenen Fotos werden verkleinert und verschlüsselt in der SchILD*app*-Datenbank gespeichert. Bitte denken Sie daran die Originalbilder aus der Galerie Ihres Mobilgeräts zu löschen. Die Möglichkeit über SchILD*app* Schülerfotos aufzunehmen kann zentral oder für einzelne SchülerInnen in den SchILD-Einstellungen (bspw. von der Schulleitung) deaktiviert werden.

- **READ_EXTERNAL_STORAGE (USB-Speicherinhalte lesen)**
- **WRITE_EXTERNAL_STORAGE (USB-Speicherinhalte ändern oder löschen)**

Diese Berechtigungen ermöglichen einer App das Lesen, Ändern und Löschen von Daten im externen Speicher. Der externe Speicher beinhaltet die SD-Karte und einen Teil des fest eingebauten Speichers.

Diese Berechtigungen benötigt SchILD*app* um Fotos auf dem externen Speicher abzulegen.

- **VIBRATE (Vibrationsalarm steuern)**

Diese Berechtigung ermöglicht einer App den Vibrationsalarm des Mobilgerätes auszulösen.
Bei wichtigen Nutzeranfragen (bspw. beim Löschen von Daten oder fehlerhaften Eingaben) nutzt SchILD*app* zusätzlich den Vibrationsalarm um die Aufmerksamkeit des Nutzers zu erregen.

2. Welche Daten werden von SchILDapp gespeichert?

In SchILD*app* werden lediglich Daten gespeichert und verarbeitet (sowie mit SchILD synchronisiert), die essentiell für die Nutzung bzw. die Leistungsdatenverwaltung notwendig sind.

Dies sind im Einzelnen:

- Allgemeine Schuldaten (Name der Schule, Adresse, Schulnummer)
- Lehrerdaten (Name, Vorname, Lehrerkürzel, E-Mail-Adresse, IMEI)
- Fächer-, Kursbezeichnungen
- Klassen-, Kurszugehörigkeit der SchülerInnen
- Schülerdaten (Name, Vorname, optional :Telefonnummer, E-Mail-Adresse , Foto, Notiz)
- Teilleistungsarten (bspw. Kursarbeiten, Tests)
- Teilleistungsnoten
- Zeugnisnoten
- Mahnungen
- Fehlstunden
- Sitzpläne, Raumnummern

3. Wo werden die Daten von SchILDapp gespeichert?

Die Datenbank von SchILD*app* (mit allen von SchILD*app* verwalteten Daten) wird auf Ihrem Tablet/Smartphone verschlüsselt und in einem geschützten Systembereich gespeichert, auf den nur SchILD*app* Zugriff hat. Einzige Ausnahme bilden Geräte, auf denen das sogenannte „Rooten“ durchgeführt wurde. Auf diesen Geräten erhalten die Anwender erweiterte Systemrechte (Root-Rechte) und können so auf den speziellen, von SchILD*app* verwendeten Systembereich zugreifen. Unabhängig von der Zugriffsmöglichkeit bleiben alle Daten weiterhin AES-256 verschlüsselt und sind so vor unberechtigtem Auslesen geschützt. ribeka empfehlt jedoch SchILD*app* nicht auf „gerooteten“ Geräten zu verwenden.

4. Wie lange werden die Daten von SchILDapp gespeichert?

Alle in SchILD*app* verwalteten Daten werden normalerweise ein Halbjahr („Abschnitt“) gespeichert. Das bedeutet, dass gespeicherte Daten mit Beginn des nächsten Halbjahres gelöscht bzw. durch neue Daten aus SchILD überschrieben werden. Eine Ausnahme bilden Mobilgeräte von Lehrkräften, die zum Zeitpunkt des Halbjahreswechsels nicht mehr an der Schule beschäftigt sind. In diesen Fall werden die Daten maximal ein Kalenderjahr gespeichert. Nach Ablauf des Kalenderjahres werden die Daten bei der ersten Verwendung von SchILD*app* gelöscht.

5. Werden Daten von SchILDapp an andere Geräte / Server gesendet?

SchILD*app* sendet keine Daten an externe Stellen, weder an „ribeka GmbH“ noch an dritte Personen. Es werden keine Nutzungsstatistiken oder sonstige Daten über SchILD*app* erhoben und/oder weitergeleitet. Alle in SchILD*app* vorhandenen sowie alle eingegeben Daten werden halbautomatisch (d.h. automatisch, aber erst nach expliziter Aufforderung durch den Anwender) über den schuleigenen Kommunikationsserver (Webserver) in die SchILD-Datenbank (SchILD-NRW, SchILD*zentra*l) Ihrer Schule übertragen. Die Übertragung von Daten erfolgt immer verschlüsselt (über https bzw. SSL/TLS). Abhängig von der genutzten SchILD-Installation (-NRW oder-*zentral*) werden die Daten vom Kommunikationsserver entweder direkt in die SchILD-Datenbank übertragen (direkte Synchronisation) oder für eine manuelle Synchronisation in einer zusätzlichen Webdatenbank auf den schuleigenen Webserver gespeichert.

6. Wie wird die Datenbank von SchILDapp verschlüsselt?

Alle von SchILD*app* verwendeten, sowie alle über SchILD*app* eingegebenen Daten werden mit dem Verschlüsselungsalgorithmus AES-256 sicher verschlüsselt.

7. Wie wird die Datenkommunikation verschlüsselt?

Die Kommunikation zwischen SchILD*app* und SchILD*web* wird durch die Verwendung von SSL/TLS respektive HTTPS verschlüsselt und sicher ausgeführt. Das bedeutet, dass alle Daten, die über das Internet verschlüsselt geschickt werden, so dass dritte Personen diese Daten nicht lesen können. **HTTPS - Hypertext Transfer Protocol Secure** (englisch für „sicheres Hypertext-Übertragungsprotokoll“) ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen. Es stellt eine Transportverschlüsselung dar.

8. Impressum

ribeka GmbH
Johann-Philipp-Reis-Str. 9
53332 Bornheim/Rheinland
Telefon +49 (0)2222-990600
Fax +49 (0)2222-990601
E-Mail info@ribeka.com
www.ribeka.com

Gründungsjahr: 1996 GmbH 1999
USt-IDNr.: DE812773290
Registergericht: Amtsgericht Bonn
Registernummer: HRB 8423
Vertretungsberechtigte Geschäftsführer:
Erich Berger, Dr. Jürgen Richter