

München, den 21. Juli 2021

Stellungnahme des Staatsinstituts für Frühpädagogik und Medienkompetenz (IFP)

Neue Studie „We may share the number of diaper changes“: A Privacy and Security Analysis of Mobile Child Care Applications von Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban und Matteo Große-Kampmann, veröffentlicht am 7. Juli 2022

Ein Team an IT-Sicherheitsexperten hat in dieser Studie erstmals eine systematische technische Datenschutz- und Sicherheitsanalyse von 42 KitaApps (Android) durchgeführt. Die Studie kommt zu dem Ergebnis, dass viele KitaApps teilweise erhebliche Sicherheitsmängel aufweisen und der Schutz sensibler Daten von Kindern gefährdet ist. Bei einzelnen Apps ist es den Autoren sogar gelungen, aufgrund unsicherer Speicherung auf Daten von Kindern (z. B. Fotos und Videos) zuzugreifen. Sie gehen davon aus, dass KitaApps auch in ihrer iOS-Version dieselben Mängel aufweisen.

Das IFP setzt sich in seinen Projekten im Rahmen der Bayerischen Digitalisierungsstrategie für die Kindertagesbetreuung bereits seit 2018 für den Einsatz von KitaApps zur Unterstützung bei mittelbaren pädagogischen Aufgaben ein. Leider ist es uns als frühpädagogischem Forschungsinstitut nicht möglich, eine tiefergehende technische Analyse dieser Apps durchzuführen. Deswegen begrüßen wir die Arbeit des fachkundigen Forschungsteams und versprechen uns daraus einen Gewinn für die zukünftige Entwicklung bei der Sicherheit von sensiblen personenbezogenen Daten von Kindern.

Im Einzelnen stellten die Forscher insbesondere folgende Probleme fest:

- Einsatz vieler Third-Party Libraries und Tracker
- Datenabfluss an Dritte ohne Genehmigung dafür oder Information darüber
- Einsatz unsicherer Cloudspeicher
- Einsatz veralteter und daher anfälliger Verschlüsselungstechnologie
- Unterstützung veralteter und daher anfälliger Versionen von Betriebssystemen
- Abfrage vieler – teils problematischer – App-Berechtigungen
- Fehlerhafte Datenschutzzinformationen

Nach Ansicht des IFP ist der Kitaträger als Verantwortlicher im Sinne des Datenschutzrechts für die Einhaltung aller datenschutzrechtlich relevanten Regelungen verantwortlich. Darunter fällt auch Art. 32 DSGVO, der zum Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit verpflichtet.

Im Rahmen des zwischen dem Kitaträger und dem App-Anbieter vorliegenden Auftragsverarbeitungsverhältnisses (Art. 28 DSGVO) bleibt der Kitaträger weiterhin für die Einhaltung des Datenschutzes verantwortlich. Die Zusammenarbeit darf nur mit Auftragnehmern erfolgen, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen (TOM) so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz betroffener Personen gewährleistet ist. Im Rahmen des Vertrags über die Auftragsverarbeitung (AVV) muss geregelt werden:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten und betroffene Personen
- Rechte und Pflichten der Vertragsparteien

Eine ausführliche Darstellung des notwendigen Inhalts des AVV ist in der [IFP-Expertise „Kita-Apps – Apps und Softwarelösungen für mittelbare pädagogische Aufgaben in der Kita“](#) (2., überarbeitete Auflage 2021, S. 52 f.) enthalten. Im Rahmen des AVV wird klargestellt, dass der App-Anbieter als Auftragnehmer nicht selbst über die Verarbeitung oder Verwendung personenbezogener Daten entscheiden kann. Außerdem muss klargestellt werden, welche Unterauftragnehmer des App-Anbieters Zugriff auf welche personenbezogenen Daten erhalten. Durch die Festlegung von Art und Zweck der Verarbeitung sollte von vornherein das Tracking und die Übermittlung – gleichgültig ob zu Analyse- oder zu Werbezwecken – von Daten an Dritte ausgeschlossen werden. Wenn trotzdem ein Datenabfluss an Dritte oder der Einsatz von Tracking-mechanismen vorkommt, handelt der Auftragnehmer vertragswidrig.

Da davon auszugehen ist, dass die meisten zwischen Kitaträgern und App-Anbietern abgeschlossenen AVV diese Anforderungen einhalten, da es sonst niemals zu einer Auftragserteilung hätte kommen dürfen, legt die nun veröffentlichte Studie eine offenbar große Diskrepanz zwischen vertraglichen Vereinbarungen und deren Umsetzung nahe.

In der Studie wurden **14 Anwendungen untersucht**, die auch in der o. g. **IFP-Expertise zu KitaApps beschrieben** werden. Diese 14 Anwendungen sind *Care, Famly, HoKita, Kidling, KigaRoo, KiKom, Kindy, Kita-Info-App, Kitaportfolio, Leandoo, LiveKid, Nembørn, Sdui* und *Stramplerbande*.

Kitaträgern, die eine der 42 untersuchten Apps in ihren Kitas bereits einsetzen oder zukünftig den Einsatz von KitaApps planen, ist zu empfehlen, dass gemeinsam mit den App-Anbietern das weitere Vorgehen besprochen wird. Zunächst sollte festgestellt werden, ob der AVV den gesetzlichen Vorgaben entspricht. Insbesondere die dort festgelegten technischen und organisatorischen Maßnahmen und das zum AVV gehörende IT-Sicherheitskonzept sollten unter Berücksichtigung der aktuellen Befunde kritisch überprüft werden. Dabei ist darauf zu achten,

- dass Trackingmechanismen nicht nur vertraglich ausgeschlossen werden, sondern auch tatsächlich nicht implementiert wurden (z. B. durch Verwendung von Libraries wie Google Firebase o. ä.),
- dass kein ungewollter Abfluss personenbezogener Daten stattfindet,
- dass regelmäßig Sicherheitsupdates erfolgen,
- dass Verschlüsselungstechnologie nach dem aktuellen Stand der Technik verwendet wird,
- dass keine ungewollten Zugriffe auf Datenbanken und Speicherclouds möglich sind,
- dass im Einklang mit dem Prinzip der Datenminimierung der Zugriff auf Funktionen von Endgeräten (z. B. Kamera, Kalender, Speicher, Kontakte etc.) so gering wie möglich gehalten wird.

Die Anbieter der in der Studie untersuchten Apps wurden vor der Veröffentlichung durch das Forschungsteam kontaktiert und auf die Sicherheitsmängel hingewiesen. Wir gehen deshalb davon aus, dass seriöse Anbieter die Sicherheitsmängel bereits beseitigen konnten oder an deren Beseitigung arbeiten.

Dennoch zeigt die Studie ein Problem auf, das sich vielen Kitaträgern stellt. Eine tiefgehende technische Datenschutz- und Datensicherheitsanalyse der eingesetzten KitaApps ist den Trägern kaum möglich, sodass eine Diskrepanz zwischen den im AVV festgelegten Regelungen und Maßnahmen und der Umsetzung durch den App-Anbieter – sei diese bewusst oder unbewusst – nicht aufgedeckt werden kann.

Das Forschungsteam leistete in der Studie das, was das IFP schon lange fordert, nämlich eine tiefgehende technische Analyse durch kompetente Stellen. In der [Expertise „Nutzung digitaler Medien für die pädagogische Arbeit in der Kindertagesbetreuung“](#), die das IFP im Auftrag des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) anfertigte und im April 2020 erschien, empfehlen wir, das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Aufgabe der technischen Datenschutz- und Sicherheitsüberprüfung von KitaApps zu betrauen und einen Prozess zur regelmäßigen Zertifizierung der Datensicherheit der KitaApps auf Bundesebene zu etablieren (S. 79). In der o. g. IFP-Expertise zu KitaApps wiederholen wir dieses Anliegen (S. 68).

Ansprechpersonen am IFP:

Eva Reichert-Garschhammer

Stefan Knoll