Einsatz von Google Firebase Cloud Messaging zum Versand von Push-Mitteilungen an die Sorgeberechtigten

Dass Stay Informed großen Wert auf die Einhaltung datenschutzrechtlicher Vorschriften legt, zeigt sich in der Auswahl der Unterauftragnehmer: Wir achten darauf, dass Unternehmenssitz und Datenverarbeitung in Deutschland sind. Wir wählen Dienstleister, die ihrerseits keine oder nur deutsche Unterauftragnehmer haben. Auch verwenden wir keine Dienstleister, deren Eigentümer ihren Sitz im EU-Ausland haben.

Eine Ausnahme hiervon bildet der Dienst zur Benachrichtigung verbundener Mobilgeräte und Web-Browser. Der Benachrichtigungsdienst informiert App-Nutzer über den Eingang neuer Nachrichten aus der Einrichtung. Ein solcher Dienst wird von den meisten Apps auf Mobilgeräten verwendet und als „Push-Service“ bezeichnet.

Trotz umfangreicher Suche nach Alternativen haben wir uns beim Benachrichtigungsdienst für Google Firebase Cloud Messaging (**FCM**) entschieden. Die Gründe hierfür erläutern wir in diesem Dokument. Auch soll es der verantwortlichen Stelle bei ihrer Beurteilung der Zulässigkeit von FCM in der Kita-/Schul-Info-App helfen.

Unsere Argumente auf den Punkt gebracht

Nach Prüfung der Rechtslage, der Verträge mit Google, der technischen Rahmenbedingungen und der von uns ergriffenen Maßnahmen sind wir als Auftragsverarbeiter davon überzeugt, dass der Einsatz von FCM für die Kita-/Schul-Info-App zulässig ist. Unsere wesentlichen Argumente in Kurzform:

- Es werden keine Nachrichteninhalte verschickt, lediglich optional die „Betreff“-Zeile.
- FCM verwendet nur pseudonyme IDs und wird nur zur Benachrichtigung verwendet, nicht für Inhalte.
- Die FCM-Einstellungen sind datensparsam eingestellt: nur zur Verbesserung von FCM selbst.
- Unter iOS, in Web-Apps und ohne Play Services kann Google keinen Personenbezug herstellen.
- Die datenschutzrechtlichen Verträge mit Google sind komplex, aber grundsätzlich in Ordnung.
- FCM unterliegt vermutlich nicht der US-Rechtsprechung zur Telekommunikationsüberwachung.
- Für typische App-Nutzer gibt es keine hinreichend zuverlässig funktionierenden Alternativen.
- Unter Android mit Google Play Services hat der Nutzer der Datennutzung durch Google bereits vorher zugestimmt (und diese ist umfangreicher als die *zusätzliche* Verknüpfung „benachrichtige die App“).

Wir sind der Meinung, dass ein angemessenes Datenschutzniveau erreicht wird, die technisch-funktionalen Verknüpfungen nicht unter die vom EuGH monierten Überwachungsbefugnisse der USA fallen.

Auf den folgenden Seiten stellen wir ausführlich dar, wie wir zu dieser Einschätzung kamen.

Fortschreibung dieses Dokuments

Google hat die Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten in Drittländer vom 04.06.2021 am 27.09.2021 adaptiert. Das überarbeitete Vertragswerk (s.u.) stellt eine Verbesserung dar, u.a. weil die SCCs die vom EDSA geforderten „zusätzliche Garantien“ beinhalten.

Aufgrund von US-Handelssanktionen kann FCM nicht auf neueren Huawei-Geräten verwendet werden. Um die App auch für Sorgeberechtigte nutzbar zu machen, die ein solches Gerät besitzen, prüfen wir derzeit technisch und rechtlich, ob und wie der Huawei Push Service ohne Datenschutzprobleme eingebunden werden kann.

Alternativen für Push-Dienste

Zunächst haben wir nach Lösungen gesucht, die komplett ohne einen Dienst von Google auskommen. Dazu müssten unsere Apps regelmäßig unsere Server fragen, ob Nachrichten für sie da sind. Neben Lastproblemen auf dem Server würde dies dazu führen, dass die Mobilgeräte mehr Strom verbrauchen. Zudem beenden neuere Android-Versionen solche Apps, sodass deren Nutzer manuell Ausnahmen im Energiemanagement ihres Mobilgeräts vornehmen müssten. Aufgrund der Vielzahl unterschiedlicher Hersteller und Geräte führt dies zu erheblichen Problemen. Hinzu kommt, dass Apple dies für iOS-Geräte überhaupt nicht erlaubt.

Folglich haben wir uns deutsche/europäische „datenschutzkonforme“ Anbieter von Benachrichtigungsdiensten angesehen und bei deren technischer Evaluierung festgestellt, dass diese für die eigentliche Zustellung auch FCM verwenden. Da sich hier kein Datenschutz-Vorteil ergibt, sondern nur ein zusätzlich zu verwaltender Anbieter hinzukäme, haben wir auch von alternativen Benachrichtigungsdiensten Abstand genommen.

Folglich bleibt derzeit nur FCM als technisch hinreichend zuverlässige Lösung übrig und muss geprüft werden.

Technische Beschränkungen

Zunächst haben wir versucht, die Datenverarbeitung für FCM geographisch einzuschränken. Dies ist nicht möglich: Die Benachrichtigungsdienste werden von Google weltweit verteilt erbracht. Dies gilt selbst für Kunden, die ansonsten Europa oder Deutschland als Standort für ihre Daten bei Google festgelegt haben.

Danach haben wir hinterfragt, wofür die durch FCM verarbeiteten Daten verwendet werden. Standardmäßig werden sie zur Verbesserung aller Google-Produkte verwendet. Dies kann durch den FCM-Administrator eingeschränkt werden. Dies haben wir selbstverständlich getan. Die Verwendung der Daten zur Verbesserung von FCM selbst lässt sich nicht deaktivieren. Dies finden wir aber auch angemessen, schließlich möchten auch wir einen optimal funktionierenden Benachrichtigungsdienst.

Art der Daten und deren potenzielle Nutzung durch Google

Nun haben wir uns angesehen, welche Daten anfallen könnten und was Google damit machen könnte. FCM stellt eine logische Verknüpfung zwischen einem Dienst (der benachrichtigen möchte) und unserer App auf dem Mobilgerät der Sorgeberechtigten her. Hierzu werden pseudonyme Dienst-, Geräte- und App-Nummern (IDs) erzeugt, zugewiesen und schließlich zur Verteilung der Benachrichtigungen verwendet. Diese IDs sind zunächst nicht personenbezogen und allein mit ihrer Hilfe kann eine Person nicht identifiziert werden.

An dieser Stelle muss zwischen Plattformen unterschieden werden: Unter iOS kann Google die Geräte-ID nicht zuordnen, da nur Apple die Person kennt. Auch bei Web-Apps ist keine Zuordnung durch Google möglich – solange der Browser datenschutzkonform eingestellt und der Nutzer nicht bei Google angemeldet ist. Android-Geräte ohne Google Play Services können sich gar nicht erst an FCM registrieren.

Übrig bleiben die (typischen) Android-Nutzer mit Google Play Services. Diese Nutzer haben aber der Nutzung ihrer Daten durch Google bereits bei der Einrichtung ihres Mobilgeräts zugestimmt, oft auch für persönlichere Daten. Viele Android-Nutzer haben auch weitere Apps installiert, die Benachrichtigungen per FCM empfangen. Das „Problem“ ist also allein die Tatsache, dass Google hier mehrere Rollen als Anbieter bzw. Erbringer von Dienstleistungen hat: FCM für Stay Informed, Play Services für Android, und Play Store für den Kunden.

Auftragsverarbeitung und angemessenes Datenschutzniveau

Im nächsten Schritt haben wir die von Google bereitgestellten Verträge geprüft. Deren Struktur ist zwar kompliziert, enthält aber alle Zusicherungen, die ein US-Anbieter derzeit sinnvoll machen kann. Auch hat Google die Nutzung zu eigenen Zwecken korrekt abgegrenzt und ausgewiesen. Hier die Vertragsstruktur:

Name des Vertragsdokuments	**Stand** (Prüfung)	**Internet-Adresse** (Quelle)
Terms of Service for Firebase Services	2020-10-19	https://firebase.google.com/terms
Firebase Data Processing and Security Terms	2021-09-27	https://firebase.google.com/terms/data-processing-terms
Subprocessors	2021-09-23	https://firebase.google.com/terms/subprocessors
SCCs EU P2P, Google Exporter	2021-09-27	https://firebase.google.com/terms/firebase-sccs-eu-p2p-google-exporter
SCCs EU P2P	2021-09-27	https://firebase.google.com/terms/firebase-sccs-eu-p2p
Google APIs Terms of Service	2021-11-09	https://developers.google.com/terms/
Google C2C Data Protection Terms	2021-09-27	https://business.safety.google/gdprcontrollerterms/
Google Privacy Policy	2021-07-01	https://policies.google.com/privacy
123 Google API Services User Data Policy	2020-09-03	https://developers.google.com/terms/api-services-user-data-policy
Privacy and Security in Firebase	2021-11-08	https://firebase.google.com/support/privacy
Google Cloud Platform Terms of Service	2021-09-21	https://cloud.google.com/terms/

Google gewährleistet vertraglich die Vertraulichkeit der verarbeiteten Daten. Daher kann die Sicherstellung des angemessenen Datenschutzniveaus auf die USA beschränkt werden. Angesichts dessen, dass es sich bei FCM um eine technisch-funktionale Verknüpfung handelt, fallen diese nach unserer Auffassung nicht unter die vom EuGH als problematisch dargestellten US-Rechte zur Telekommunikationsüberwachung. Daher halten wir die vertraglichen Zusicherungen für ausreichend.

Datensparsame Umsetzung und Abschaltoption

Wir haben FCM so eingebunden, dass möglichst wenig Daten übermittelt werden. Eine frühere Version unserer Lösung konnte nur benachrichtigen: „Kita-/Schul-Info-App hat eine neue Nachricht“. Dies wurde von den Sorgeberechtigten als unzureichend empfunden und führte zur dringenden Bitte mehrerer Einrichtungen, wenigstens einen Betreff in der Benachrichtigung mitsenden zu können.

Wunschgemäß haben wir die Funktionalität so erweitert, dass optional ein Betreff mitgesendet werden kann. Es ist die Aufgabe der Einrichtung darauf zu achten, dass dieser keine sensiblen Informationen enthält.

An dieser Stelle sei noch einmal betont: Nachrichteninhalte und zugehörige Antworten werden nie über Benachrichtigungen transportiert. Sie werden von der App immer direkt von unserem Server abgeholt.

Unterschiede zwischen Push- und E-Mail-Benachrichtigungen

Nutzer, die sich per E-Mail über den Eingang neuer Nachrichten benachrichtigen lassen, erhalten diese E-Mails nicht über FCM. Auch per E-Mail erfolgt nur eine Benachrichtigung, die Nachricht selbst wird nicht per E-Mail versendet.

Stand: 23.12.2021