Prüfunterlagen für die Applikation

„lumind“

Ansprechpartner: Kevin Röhl
Dolziger Str. 7
10247 Berlin
Telefon: 0176 913 434 98
E-Mail: mail@lumind.de

Version:

Plattform: iOS, Version 0.6.2, Versionsdatum 06.03.2018

Technische Überprüfung

Plattformunabhängigkeit/Plattform	Die App ist ausschließlich für iOS-basierte Geräte (iPhone, iPad, iPod touch; ab iOS 10.3 oder neuer) verfügbar.
Datentransport verschlüsselt ja/nein (https/http)	Der Datentransport dieser App läuft zu großen Teilen verschlüsselt/via https ab. Unverschlüsselte Kommunikationsströme betreffen keine sensiblen bzw. datenschutzrelevanten Aspekte (bspw. Verbindung zur Webseite von lumind).
Nutzung von Analyse-Diensten (z.B. Google Analytics)	lumind informiert darüber, dass die Analyse-Dienste „Crashlytics“ und „Answers“ von Google verwendet werde. Weiterhin wird die Anwendung „Fabric“ verwendet, um allgemeine Nutzungsstatistiken zu erheben. Die Informationen werden an lumind in anonymisierter Form weitergegeben, Rückschlüsse auf die Person sind auf diese Weise laut Entwickler nicht möglich.
Benötigte Zugriffsmöglichkeiten	Die App erfordert Zugriff auf Mitteilungen, wie Hinweise und Töne, um die Nutzer an die Anwendung der App erinnern zu können. Diese Funktion kann jedoch deaktiviert werden; die App ist weiterhin bis auf die Erinnerungsfunktion nutzbar.
Analyse der AGB/Datenschutzangaben	Die Erklärung zum Datenschutz und zu den AGBs sind direkt in die App integriert.

	Sie sind ebenso auf der Webseite von lumind zu finden. Die Datenschutzerklärung weist auf wichtige Aspekte des Datenschutzes wie „Erhebung, Verarbeitung und Nutzung personenbezogener Daten“, „Nutzung von Analysediensten und Cookies“, „Rechte des Nutzers“, „Einwilligung in die Datenverarbeitung“ und „Ansprechpartner“ hin. Den Angaben zum Datenschutz ist zu entnehmen, dass personenbezogene Daten erhoben werden. Dazu gehören konkret: „Daten zum Nutzer-Account“ (Nutzername, E-Mail, Passwort (verschlüsselt); ggf. Profileinstellungen (der Blutzuckerzielbereich und bevorzugte Messeinheit); Daten zur Blutzuckermessung, erhoben über ein kompatibles Messgerät (Datum, Uhrzeit, Blutzuckermesswert). Die Daten werden lokal sowie ggf. auf dem eigenen Server gespeichert. Die Datenschutzerklärung macht darauf aufmerksam, dass die Datennutzung im Rahmen des angebenden Zwecks der App erfolgt (z.B. Erinnerung an die regelmäßigen Blutzuckermessintervalle). Es werden nach Herstellerangaben ohne Zustimmung des Nutzers keine Daten an Dritte weitergegeben. Die Löschung von erhobenen Daten kann durch die Löschung der App auf dem mobilen Endgerät erfolgen. Ein Impressum mit Angabe von Kontaktmöglichkeiten ist vorhanden. Die App ist auch ohne Anlegen eines Kontos bzw. Accounts nutzbar, bspw. können Reminder (Erinnerung an die nächste Blutzuckermessung gemäß einem festgelegten Intervall) genutzt werden.

Fazit	Kein Hinweis für Sicherheitsrisiken oder datenschutzrechtlich kritische Passagen. Siegel kann daher vergeben werden.

App-Monitoring

Allgemeine Informationen

Bei der durchgeführten Analyse bzw. beim Monitoring von Apps geht es darum, die Sicherheit der Datenströme und des Datentransports zu testen, d.h. zu testen, ob die Daten über eine gesicherte **https**-Verbindung übertragen werden. Dies gilt insbesondere für sensible und persönliche Daten, wie etwa Passwörter oder Angaben zum Gesundheitszustand. Zur Analyse der Kommunikation der Apps wird Charles Proxy verwendet.
Erfolgt die Kommunikation über ein http-Protokoll, zeigt dies an, dass die Kommunikation **unverschlüsselt** ist.
Werden viele Datenströme mit Verwendung eines **http**-Protokolls angezeigt, ist dies ein Anzeichen dafür, dass bei dieser App genauer hingesehen werden sollte. Entscheidend ist dabei konkret die Frage, welche Daten bzw. Kommunikationsvorgänge über eine http-Verbindung transportiert werden. Handelt es sich dabei nur um einfache Bilddateien der Apps, etc. und nicht um personenbezogene Daten, ist dies natürlich weniger kritisch.
Des Weiteren wird die **Plattform(un-)abhängigkeit** der Apps analysiert, d.h. es wird einerseits untersucht, ob die Apps grundsätzlich auf den beiden größten App-Plattformen von Apple/iOS und von Google/Android fehlerfrei auf verschiedenen Endgeräte funktionieren. Die Ergebnisse dieses Tests können auch von den Angaben der Entwickler und Hersteller mitunter abweichen. Die Analyse zur Sicherheit der Datenströme erfolgt entsprechend auf beiden Plattformen.

Des Weiteren werden abschließend noch die Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen App-Herstellers analysiert – mit Fokus auf Angaben zum Datenschutz bzw. zur herstellerbezogenen Nutzung der bereitgestellten Daten – mit dem Ziel, die zuvor analysierten Ergebnisse mit den Angaben in den AGBs abgleichen zu können und eventuell vorhandene Widersprüche bzw. noch offene Fragen an den Hersteller herausfiltern zu können. Dieser Schritt rundet die Gesamtbewertung ab.

Hinzugefügt werden muss in diesem Zusammenhang, dass über dieses Verfahren und aus rechtlichen Gründen nicht zu erkennen oder herauszufinden ist, was konkret mit den erhobenen Daten passiert bzw. ob der Hersteller die Daten an Dritte

weitergibt. Ein Weiterverkauf der Daten etwa kann nicht zweifelsfrei ermittelt werden. Offenkundig wird lediglich, ob die AGBs dies erlauben würden oder ausschließen.

Plattformunabhängigkeit/Plattform	
Datentransport verschlüsselt ja/nein (https/http)	
Nutzung von Analyse-Diensten (z.B. Google Analytics)	
Benötigte Zugriffsmöglichkeiten	
Analyse der AGB/ Datenschutz-/Sicherheitsangaben	