Prüfunterlagen für die Applikation

„Diabetes Tagebuch + Companion“

Ansprechpartner: **jommi UG**
Brunnenstraße 23
D-40223 Düsseldorf
Telefon: +49-(0)-211-468 38768

Version: Plattform: iOS, Version 1.5.1, 19.09.2019

Technische Überprüfung:

Plattformunabhängigkeit/Plattform	Die App ist für iOS verfügbar. Sie funktioniert auf iPhones und iPads. Die App ist nicht unbedingt für alle iPads optimiert.
Datentransport verschlüsselt ja/nein (https/http)	Der Datentransport der App läuft verschlüsselt via https ab.
Registrierung	Eine Registrierung ist für die kostenfreie Nutzung nicht erforderlich. Der Nutzer ist vor dem ersten Start angehalten, gesundheitsbezogene Angaben (Gesundheitsziel, anvisierte tägliche Schrittzahl, Größe, Gewicht, Geschlecht, Geburtsdatum) zu tätigen. Es ist direkt aus der App heraus möglich, über den Menupunkt „Lösche alle Daten…für immer“ gesamthaft die eingegeben Nutzerdaten zu löschen.
Nutzung von Analyse-Diensten (z.B. Google Analytics) und Werbenetzwerken	Die Datenschutzerklärung informiert darüber, dass der mobile Service auf anonymisierter Basis Daten über Fehler/Abstürze der App via Apple oder Google Analytics nutzen kann. Die Datenschutzerklärung informiert zudem darüber, dass Cookies angelegt werden und hier zwecks Analyse des Nutzungsverhaltens Google Analytics verwendet wird. Die Informationen werden auf Servern in die USA übertragen. Nach Herstellerangaben wird die IP-Adresse des Nutzers hierbei nicht mit anderen Daten/Informationen des Nutzers verknüpft.

	Es werden keine Werbenetzwerke seitens der App verwendet.
Benötigte Zugriffsmöglichkeiten	Die App benötigt die Erlaubnis, sich mit Apple Health zu verbinden, um Gesundheitsdaten zu lesen und in der App anzeigen zu können. Die Daten bleiben nach Herstellerangaben auf dem Gerät (wird direkt beim ersten Start der App abgefragt) In-App-Käufe möglich.
Analyse der AGB/Datenschutzangaben	Die Datenschutzerklärung ist in der App aufrufbar sowie über den AppStore (http://www.foodlabelling.net/privacy/). Sie ist für die Webseite und für die Nutzung mobiler Angebote bzw. Apps erstellt worden. Die Datenschutzerklärung ist unter „Privacy Policy“ ausschließlich auf Englisch verfügbar. Die Datenschutzerklärung informiert über Zweck und Art der Datenerhebung, das verantwortliches Unternehmen, das Anlegen eines Accounts, Cookies, Datensicherheit und Kontaktmöglichkeiten. Die Daten werden nach Herstellerangaben grundsätzlich lokal auf dem Endgerät gespeichert. Der Hersteller sichert zu, dass keine Daten an Dritte weitergegeben werden bzw. dies auch nicht Teil des Geschäftsmodells ist. Ein Datenschutzbeauftragter wird nicht in den Privacy Policy namentlich genannt. Es ist ein Link (http://www.foodlabelling.net/contact/) hinterlegt, der eine Kontaktaufnahme zwecks datenschutzrechtlicher Fragen ermöglicht. Auf der Webseite (https://www.jommi.de/de/impressum/) ist Herr Fabian Oertel als Datenschutzbeauftragter genannt. Ein vollständiges Impressum ist in der App vorhanden. Die Datenschutzerklärung wurde zuletzt am 03. September 2019 aktualisiert.

App-Monitoring – allgemeine Informationen

Bei der durchgeführten Analyse bzw. beim Monitoring von Apps geht es darum, sicherheits- und datenschutzrelevante Aspekte der App zu bewerten. Dabei geht es zunächst um **Plattform(un-)abhängigkeit**, d.h. es wird einerseits untersucht, ob die Apps grundsätzlich auf den beiden größten App-Plattformen von Apple/iOS (und ggf. weiteren Anbieter) verfügbar sind und auf verschiedenen Endgeräten funktionieren und für diese optimiert sind. Anschließend wird die Sicherheit der Datenströme und des Datentransports bewertet. D.h., es wird überprüft, 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 und insbesondere zu schauen ist, welche Daten bzw. Kommunikationsvorgänge über eine http-Verbindung transportiert werden.

Es wird weiterhin erfasst, ob für die App-Nutzung eine **Registrierung** vorgenommen werden muss und welche Daten dabei anzugeben sind (E-Mail, Login über Facebook, Angabe persönlicher oder gesundheitsbezogener Informationen etc.). Idealerweise ist keine Registrierung notwendig, das Anlegen eines Nutzerkontos kann jedoch je nach angebotenen Funktionalitäten notwendig werden. Überprüft wird auch, ob sich der der Nutzer mit seinem Klarnamen anmelden muss oder ggf. auch eine „anonyme“ (funktionsfähige) E-Mail-Adresse und Nutzernamen verwenden kann. Werden bestimmte Sicherheitsanforderungen an die Auswahl des Passworts (z.B. Mindestzeichenanzahl etc.) gestellt, wird dies zusätzlich hervorgehoben

Im Anschluss wird analysiert, ob die Anwendung **Webtracking-Dienste**, bspw. Google Analytics, verwendet und ob dies **DSGVO-konform** erfolgt. Die Nutzung entsprechender Webanalyse-Dienste ist rechtlich grundsätzlich legal und entspricht den berechtigten Interessen der Hersteller, sofern bestimmte Voraussetzungen erfüllt werden. Der Hersteller ist etwa angehalten, die Rechtsgrundlage zu nennen, transparent in der Datenschutzerklärung über das Webtrackings zu informieren (Tool, Betreibergesellschaft, welche Daten werden gespeichert und verarbeitet) eine Anonymisierung der IP-Adresse des Nutzers vorzunehmen, eine Widerspruchsmöglichkeit sowie eine Opt-Out-Option/ein Opt-Out-Cookie anzubieten. Sicherzustellen ist auch, dass das auftragsdatenverarbeitende Webanalyse-Unternehmen, sofern es in einem Drittstaat wie den USA Daten verarbeitet, nach der EU-US-Privacy-Shield (Grundlage für Datenübermittlungen in die USA, mit dem bestimmte Nutzerrechte, z.B. Recht auf Auskunft, verbunden sind) zertifiziert ist. In

diesem Zusammenhang wird auch überprüft, ob seitens des Entwicklers **Werbenetzwerke** in der App verwendet werden.

Anschließend folgt eine Zusammenstellung der Zugriffsrechte bzw. **App-Berechtigungen**, die der Nutzer der App gewähren muss. Dabei handelt es sich sowohl um „normale“ Berechtigungen, die für eine stabile Anwendung notwendig sind, als auch um weitergehende und ggf. zustimmungspflichtige Berechtigungen. Hier geht es nicht allein um die Anzahl der Berechtigungen, sondern vielmehr um die Notwendigkeit und Nachvollziehbarkeit (z.B. benötigt ein „einfaches“ Symptomtagebuch im Regelfall keinen Zugriff auf den ungefähren oder genauen Standort)

Des Weiteren werden abschließend noch die **Allgemeinen Geschäftsbedingungen (AGB**) bzw. die **Datenschutzerklärung** des jeweiligen App-Herstellers analysiert. Zunächst wird überprüft, ob es sich um eine separate, für die App erstellte Datenschutzerklärung oder eine allgemeine Datenschutzerklärung (auch für die Internetseiten des Herstellers) handelt. Der Fokus bei der Datenschutzerklärung liegt auf den 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. Bei dieser Analyse spielt es eine Rolle, ob die Informationspflichten gemäß der Datenschutzgrundverordnung eingehalten werden, diese beinhalten die Informationen zu:

- Datenschutzbeauftragter mit Kontaktdaten
- Zweck der Verarbeitung (personenbezogener) Daten
- Beschwerderecht bei der zuständigen Aufsichtsbehörde
- Verantwortliche Einrichtung/Person mit Kontaktdaten
- Speicherdauer
- Rechte des Betroffenen (Auskunft, Berichtigung, Löschung, Einschränkung)

Zudem wird überprüft, ob Auskunft zum Speicherort der Daten gegeben wird (Deutschland, EU, Drittstaaten). Auch ein **vollständiges Impressum** sowie eine Aufklärung über die Grenzen der App sind hierbei wichtig.

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 (rechtswidrig) an Dritte weitergibt. Ein Weiterverkauf der Daten kann nicht zweifelsfrei ermittelt werden. Offenkundig wird lediglich, ob die AGBs dies erlauben würden oder ausschließen.