ePrivacyseal GmbH

Kriterienkatalog

„ePrivacyApp“

Technische Begutachtung

Januar 2019

Das Gütesiegel „ePrivacyApp“ für Datensicherheit der ePrivacyseal GmbH zertifiziert dem jeweiligen Antragsteller, dass sein Angebot mit den im nachfolgenden Kriterienkatalog näher spezifizierten Kriterien im Einklang steht, die sich an den Anforderungen an Datensicherheit auf der Basis des deutschen Datenschutzrechtes, an der zukünftigen Datenschutz-grundverordnung und dem aktuellen Stand der Technik orientieren.

Die Prüfung bezieht sich dabei allein auf die nachfolgend beschriebenen sicherheits-technischen Fragestellungen. Eine juristische Bewertung ist damit **nicht** verbunden.

Im Einzelnen wird damit die Einhaltung folgender Anforderungen bestätigt:

I. Formale Anforderungen

Die Überprüfung der App erfolgt zunächst dahingehend, ob die formalen Voraussetzungen der ordnungsgemäßen Begründung und Abwicklung eines Vertragsverhältnisses zur Installation auf dem Endgerät des Users erfüllt sind. Von Bedeutung sind insoweit folgende Fragestellungen:

1. Allgemeines

- Welche Art von App liegt vor?
- Wird die App exakt bezeichnet?
- Gibt es eine exakte Versionierung (Versionsnummer und Versionsdatum) der App?
- Wer ist der Anbieter der App?
- Konnte die App erfolgreich installiert werden?
- Wurden neben der App andere unbemerkte Installationen anderer Apps oder sonstiger Software durchgeführt?
- Gibt es dafür eine Einwilligung des Nutzers?
- Existiert eine Altersempfehlung für die Nutzung der App im App Store?
- Befindet sich in der App ein Verweis auf eine Datenschutzerklärung?

Anmerkung: Eine juristische Prüfung der Wirksamkeit der Einwilligung erfolgt nicht.

2. Anmeldeoptionen

- Ist die Nutzung der App ohne Anmeldung möglich?
- Ist die Nutzung der App ohne Nennung von personenbezogenen Daten möglich?
- Ist die Funktionalität ohne Anmeldung eingeschränkt?
- Mit welchen anderen Apps kann sich der Nutzer anmelden / sich die App synchronisieren (z.B. Facebook Login)?

- Welche Daten werden durch solche SDKs an Dritte weitergeleitet?
- Ab welchem Zeitpunkt geschieht eine Datenübermittlung an solche Dritte?

- Kann sich der Nutzer mit einer E-Mail-Adresse anmelden?
- Kann der Nutzer seine Daten verändern?
- Kann der Nutzer seine Daten löschen?
- Erhält der Nutzer eine Bestätigung über die Löschung der Daten?

II. Datensicherheit – Grundlegende Anforderungen

Der App-Anbieter muss darlegen, dass in seiner App hinreichende technische und organisatorische Sicherheitsmaßnahmen zum Schutz personenbezogener Daten implementiert worden sind. Insofern sind folgende Fragen von Relevanz:

1. Datenverkehr

- Wird von der App Datenverkehr generiert?
- Welche Arten von Datenverkehr werden generiert?
  - Funktionale Daten ein- sowie ausgehend zur Gewährleistung der Funktionalität der App
  - Statistische Daten über die Benutzung der App
  - Personenbezogene Daten, beispielsweise zur Generierung von Nutzerprofilen
- Woher kommt und wohin geht der Datenverkehr?
  - Daten werden „nativ“ im Rahmen der zugrunde legenden App generiert / erhoben / erhalten
  - Daten werden im Rahmen von Code eines Drittanbieters generiert / erhoben / erhalten

2. Eingehende und ausgehende Daten

- Werden eingehende Daten verschlüsselt?

- Werden ausgehende Daten verschlüsselt?
- Werden vertrauliche Datensätze (z.B. Nutzername, Passwort, E-Mail) zusätzlich verschlüsselt?
- Entspricht die Verschlüsselung dem aktuellen Stand der Technik?
- Mit welcher Schlüssellänge werden vertrauliche Datensätze kodiert?
- Können verschlüsselte / verhashte vertrauliche Daten mit einem verhältnismäßig geringem Aufwand dekodiert werden?
    - Wird für das Verhashen ein Salt verwendet?
- Kann ein Man-in-the-Middle Angriff durchgeführt werden, um den Datenverkehr auszulesen?
- Erhält der Nutzer eine Warnung über eine potentiell unsichere Verbindung?
- Kann der Datenverkehr manipuliert werden?
    - Ist es möglich dadurch Schaden an Daten Dritter anzurichten?
    - Können dadurch Sicherheitsmaßnahmen umgangen werden?
- Können Informationen unbeteiligter Dritter über die App erhoben werden?
- Findet eine Authentizitätsprüfung über die Validität des SSL Zertifikates statt (SSL Pinning)?
- Können potentiell jugendgefährdende Inhalte über die App aufgerufen werden?

3. Einsatz von Tracking-Cookies und Ad-ID‘s

- Werden Tracking-Cookies, im Falle einer Web-App eingesetzt?
- Enthalten die Cookies personenbezogene Daten (z.B. IP-Adresse, Handynummer, Ad-ID)?
- Enthalten die Cookies einen Timestamp?
- Werden Ad-ID’s (z.B. IDFA, GAID, usw.) verwendet, um nutzerbasierte Werbung auszuspielen?

- Werden Ad-ID’s für sonstige Zwecke verwendet?
- Findet ein Tracking von Minderjährigen statt?
- Ist ein potentielles Opt-Out auch innerhalb der App wirksam?

4. Zugriff auf persönliche Daten

- Wird auf Directories des Devices zugegriffen (z.B. Kontaktdaten, Kalender etc.)?
- Wird auf exakte Lokationsdaten zugegriffen (z.B. GPS-Koordinaten)?
- Wird auf die Hardware des Devices zugegriffen (z.B. Mikrofon, Kamera)?
- Wird auf den Medienspeicher (Fotos, Videos, usw.) zugegriffen?
- Sind die Rechte, welche die App einräumt, für den Funktionsumfang der App von Nöten?
- Werden ungefragt Datensätze übermittelt?
- Is es möglich, sofern für die Funktionalität der App nicht zwingend notwendig, den oben beschriebenen Zugriff zu beschränken / unterbinden?

5. Übertragung von Stammdaten

- Auf welche Identifier des Devices werden von der App zugegriffen (z.B. IMEI, UDID, IMEI) und welche werden versendet?
- Wird die IP-Adresse bei einem Request oder Response übermittelt?
- Wird die MAC-Adresse der Netzwerkschnittstelle des Devices übermittelt?
- Wird die SSID (Name des WLAN-Netzwerkes mit dem das Device verbunden ist) übermittelt?
- Wird der Mobile Carrier (Telefonanbieter: z.B. Telekom, O2, usw) übermittelt?
- Wie werden diese Daten auf dem Device oder serverseitig von dem App-Anbieter gespeichert?
- Wird die Telefonnummer des Nutzers übermittelt?

Hamburg, ePrivacy GmbH