ePrivacyseal GmbH

Kriterienkatalog

„ePrivacyApp“

Dezember 2017

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?

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

2. Anmeldeoptionen

- Ist die Nutzung der App ohne Anmeldung mit 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)?
- 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

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?
- Woher kommt und wohin geht der Datenverkehr (WHOIS)?
- Ist die Datenschutzerklärung über die App aufrufbar?
- Wird der Nutzer über den Umfang des Datenverkehrs in der Datenschutzerklärung aufgeklärt?

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

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, vertrauliche Daten dekodiert und mit einem verhältnismäßig geringem Aufwand dekodiert werden?

- 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?
- 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?
- Ist die Übernahme der Anmeldung über einen Angreifer möglich (Session Highjacking)?
- Ist die App, unabhängig von der Gerätesperre, passwortgeschützt?
- Kann das Passwort mit einem Brute-Force-Angriff gehackt werden?
- Greifen bei mehrfacher Falscheingabe des Passwortes zusätzliche Sicherheitsmaßnahmen der App?

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

- Werden Tracking-Cookies, im Falle einer Web-App eingesetzt?
- Wird über die Tracking -Cookies in der Datenschutzerklärung informiert?
- 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?
- Wird der Nutzer darüber in der Datenschutzerklärung informiert?

- Werden alle mit der App verbundenen Werbetreibenden in der Datenschutzerklärung der App aufgelistet?
- Findet ein Tracking von Minderjährigen statt?
- Hat der Nutzer die Möglichkeit dem Tracking zu widersprechen und sich über das Tracking zu informieren?
- Geschieht dies in verständlicher Weise?
- Ist ein potentielles Opt-Out auch innerhalb der App wirksam?

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

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?

5. Übertragung von Stammdaten

- Auf welche Identifier des Devices werden von der App zugegriffen (z.B. IMEI, UDID, IMEI)?
- 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?

III. Allgemeine Grundsätze

1. Grundsätze der Datenvermeidung und Datensparsamkeit

Die Gebote zur Datenvermeidung und Datensparsamkeit („Datenminimierung“, Art. 5 DSGVO) müssen berücksichtigt werden. Bei der Auswahl und Gestaltung der App ist daher der Grundsatz, nur so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen, zu berücksichtigen.

- Werden personenbezogene Daten im Rahmen der Nutzung der App erhoben und gespeichert und/oder an den App-Anbieter übertragen? Falls ja: Erfolgt dies verschlüsselt und entsprechen die eingesetzten Verschlüsselungstechnologien den aktuellen Standards?

- Werden personenbezogene Daten an den App-Anbieter übertragen, wenn die App nicht genutzt wird (z.B. GPS-Lokation)?

- Werden personenbezogene Daten an Dritte übertragen (z.B. Werbenetzwerke)?

- Werden personenbezogene Daten, soweit dies nach den Verwendungszwecken möglich ist und dies keine im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert, im Rahmen der Nutzung der App anonymisiert oder pseudonymisiert? Falls ja: Entsprechen die eingesetzten Verschlüsselungstechnologien den aktuellen Standards?

- Werden nur die personenbezogenen Daten erhoben bzw. verarbeitet und genutzt, die für den Verwendungszweck unbedingt erforderlich sind?

- Sind ausreichende Maßnahmen getroffen worden, die Menge der zu verarbeitenden Daten möglichst gering zu halten? Wenn ja, welche?

- Werden bei jedem Verwendungsschritt ggf. nicht mehr für den ursprünglichen Verarbeitungszweck erforderliche Daten umgehend gelöscht?
- Wie wird die Löschung bzw. Anonymisierung und Pseudonymisierung der Daten umgesetzt?
- Erfolgt die Anonymisierung bzw. Pseudonymisierung zum frühestmöglichen Zeitpunkt?
- Ist im Falle einer Pseudonymisierung von Daten gewährleistet, dass diese Daten nicht mit wenig Aufwand wieder „depseudonymisiert“ werden können?

Anmerkung: Eine juristische Prüfung der Erfüllung der Voraussetzungen von Art. 5 DSGVO erfolgt nicht.

2. Transparenz

Beschreibung der App im entsprechenden App Store Dem Nutzer muss eine klar verständliche Beschreibung des angebotenen Produkts bzw. der angebotenen Dienstleistung zur Verfügung gestellt werden.

- Wird dem Nutzer eine klar verständliche Beschreibung des angebotenen Produkts bzw. der angebotenen Dienstleistung zur Verfügung gestellt?
- Wird in dieser Beschreibung der Fluss der Datenverarbeitung sowie etwaige Datenübermittlungen bzw. Zugriffsrechte hinreichend deutlich? Werden die Informationspflichten der §§ 13 ff. TMG beachtet?
- Ist die angegebene Kontaktinformation im App Store valide?
- Werden Push-Notifications versendet, die nicht für den expliziten Betrieb der App von Nöten sind (z.B. Werbung)?
- Wird der Nutzer im Falle eines Updates über Neuerungen der App informiert?
- Ist die Datenschutzerklärung vor einem potentiellen Login aufrufbar?
- Ist die Datenschutzerklärung stets aufrufbar?
- Ist die Datenschutzerklärung offline aufrufbar?
- Ist ein Impressum im App Store und in der App vorhanden?

- Wird der Nutzer über den Zweck der einzelnen Rechte der App informiert?
- Geschieht dies in verständlicher Weise?

Anmerkung: Eine juristische Prüfung der Wirksamkeit der Datenschutzerklärung ist damit nicht verbunden.

3. Informationspflichten

Die App muss die folgenden Informationspflichten erfüllen:

- Enthält die App eine ausreichende Anbieterkennzeichnung?
- Gibt es ein den Anforderungen von § 5 TMG entsprechendes Impressum?
- Wird der Nutzer in klar verständlichen Worten im Rahmen einer Datenschutzerklärung über die Datenverarbeitung, insbesondere Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten hinreichend aufgeklärt?
- Ist die Unterrichtung über die Datenerhebung korrekt und vollständig?
- Falls die Daten auch außerhalb der EU/EWR verarbeitet werden: Wird der Nutzer darüber informiert?
- Falls Nutzungsprofile erstellt werden: Wird der Nutzer darauf sowie auf sein Widerspruchsrecht hingewiesen?
- Erfolgt eine ausreichende Information über Cookies, Weblogs, Analyse- bzw. Tracking-Dienste, etc.?
- Ist die Datenschutzerklärung jederzeit abrufbar?
- Ist die Datenschutzerkärung versioniert?

Soweit eine Weitervermittlung von Daten zu einem anderen Diensteanbieter erfolgt:

- Wird dem Nutzer diese Weitervermittlung angezeigt?
- Geschieht dies in verständlicher Weise?

Anmerkung: Eine juristische Prüfung der Wirksamkeit der Datenschutzerklärung ist damit nicht verbunden.

4. Privacy Settings

- Sind nutzerspezifische Einstellungen möglich, z.B. für Zugriff auf Kontaktdaten, Kalenderdaten, Mediendaten, Geodaten, usw.?
- Ist ein Betrieb der App auch möglich, wenn nutzerspezifische Einstellungen deaktiviert werden?
- Wie wirken diese Einstellungen und um welche Einstellungen handelt es sich?
- Kann die App auf einem Gerät mit erweiterten Nutzerrechten ausgeführt werden (Rooting, Jailbreaking)?

5. Kundenkommunikation

- Ist eine Kontaktinformation innerhalb der App angegeben, durch welche der Nutzer den App-Anbieter oder einen verantwortlichen Support kontaktieren kann?
- Ist die Kontaktinformation valide?
- Wird auf eine potentielle Nutzeranfrage über Bedenken bezgl. des Datenschutzes innerhalb einer Woche geantwortet?
- Wird auf eine potentielle Nutzeranfrage über Bedenken bezgl. des Datenschutzes adäquat geantwortet?
- Können unbeteiligte Dritte Datensätze einer bestimmten Zielperson erfragen (Social Engineering)

6. Peripheriegeräte

- Kann die App mit einer Peripherie interagieren (z.B. über Bluetooth)?
- Können über die Peripherie Datensätze ausgelesen werden?
- Können über die Peripherie Datensätze manipuliert werden?

7. Bezahlvorgänge

- Können In-App-Käufe getätigt werden?
- Verlaufen diese In-App-Käufe über das Betriebsystem oder müssen zusätzliche Zahlungsdaten eingegeben werden?
- Können durch In-App-Käufe Daueraufträge entstehen?
- Wird der Nutzer darüber informiert?
- Geschieht dies in verständlicher Weise?

8. Sicherheit der Verarbeitung:

Die Antragsteller haben unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zweck der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Um die Einhaltung nachweisen zu können, wird folgendes geprüft:

- Hat der Verantwortliche interne Strategien festgelegt und Maßnahmen ergriffen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun? Solche Maßnahmen könnten unter anderem darin bestehen, dass

- die Verarbeitung personenbezogener Daten minimiert wird,
- personenbezogene Daten so schnell wie möglich pseudonymisiert werden,
- Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird,
- der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und
- der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern.

- Wurde das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen berücksichtigt und unter gebührender Berücksichtigung des Stands der Technik sichergestellt, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen?

Hamburg, ePrivacy GmbH