ePrivacyApp

ePrivacyseal GmbH

Criteria catalogue

"ePrivacyApp"

Technical evaluation

January 2019

The "ePrivacyApp" a seal of approval for data security from ePrivacyseal GmbH certifies that the applicant's product complies with the criteria specified in more detail in the following criteria catalogue, which are based on the requirements for data security under German data protection law, the EU GDPR and the current state of the art.

The examination relates solely to the security issues described below. A legal evaluation is **not** associated with this.

In detail, this confirms compliance with the following requirements:

I. Formal requirements

Di The examination of the App is first carried out to determine whether the formal prerequisites for the proper establishment and execution of a contractual relationship for installation on the User's terminal device have been fulfilled. The following questions are of importance in this respect:

1. General

- What kind of app is provided?
- Is the app precisely named?
- Is there an exact versioning (version number and version date) of the app?
- Who is the provider of the app?
- Could the app be installed successfully?
- Were other unnoticed installations of other apps or other software performed in addition to the app?
- Is there a consent of the user for this?
- Is there an age recommendation for using the app in the App Store?
- Does the app contain a reference to a privacy statement?

Note: There is no legal verification of the validity of the consent.

2. Login options

- Is it possible to use the app without registration?
- Is it possible to use the app without naming personal data?
- Is the functionality limited without registration?
- With which other apps can the user login / synchronize the app (e.g. Facebook login)?
  - o Which data are forwarded to third parties by such SDKs?
  - o At what point does a data transfer to such third parties take place?
- Can the user register with an e-mail address?
- Can the user change his data?
- Can the user delete his data?
- Does the user receive confirmation that the data has been deleted?

II. Data security – core requirements

The app provider must demonstrate that sufficient technical and organizational security measures for the protection of personal data have been implemented in his app. In this respect, the following questions are relevant:

1. Data flow

- Does the app generate traffic?
- What types of traffic are generated?
  - o Functional data inbound and outbound to ensure the functionality of the app
  - o Statistical data on the use of the app
  - o Personal data, e.g. for the generation of user profiles
- Where does data traffic come from and where does it go?
  - o Data is generated / collected / received "natively" in the context of the underlying app
  - o Data is generated / collected / received within the code of a third party provider
- Is data traffic generated by the app?
- What types of traffic are generated?

2. Incoming and outgoing data

- Is incoming data encrypted?
- Is outgoing data encrypted?
- Are confidential data records (e.g. user name, password, e-mail) additionally encrypted?
- Is the encryption state of the art?
- What key length is used to encode confidential data records?

- Can encrypted / hashed confidential data be decoded with relatively little effort?
- Is a Salt used for hashing?

  - Can a man-in-the-middle attack be carried out to read the data traffic?

  - Does the user receive a warning about a potentially unsecure connection?

  - Can the traffic be manipulated?
- Is it possible to cause damage to third party data?
- Can security measures be circumvented?

  - Can information from uninvolved third parties be collected via the app?

  - Is there an authenticity check on the validity of the SSL certificate (SSL pinning)?

  - Can potentially harmful content be accessed via the app?

3. Use of tracking cookies and Ad-ID's

- Are tracking cookies used in the case of a web app?
- Do the cookies contain personal data (e.g. IP address, mobile phone number, Ad-ID)?
- Do the cookies contain a timestamp?
- Are Ad-IDs (e.g. IDFA, GAID, etc.) used to play user-based advertising?
- Are Ad-IDs used for other purposes?
- Does tracking of minors/children take place?
- Is a potential opt-out also effective within the app?

4. Access to personal data

- Is the directories of the device accessed (e.g. contact data, calendar, etc.)?
- Is exact location data accessed (e.g. GPS coordinates)?
- Is the hardware of the device accessed (e.g. microphone, camera)?
- Is the media memory (photos, videos, etc.) accessed?
- Are the rights granted by the app necessary for the functionality of the app?
- Are data records transmitted unsolicited?
- Is it possible, if not absolutely necessary for the functionality of the app, to restrict / block the access described above?

5. Transfer of master data

- Which identifiers of the device are accessed by the app (e.g. IMEI, UDID) and which are sent?
- Is the IP address transmitted during a request or response?
- Is the MAC address transmitted to the network interface of the device?
- Is the SSID (name of the Wi-Fi network to which the device is connected) transmitted?
- Is the mobile carrier (telephone provider: e.g. Telekom, O2, etc.) transmitted?
- How is this data stored on the device or on the server side by the app provider?
- Is the user's phone number transmitted?

Hamburg, ePrivacy GmbH