Evaluation of the Corona-Warn-App: How user privacy remains protected

The evaluation aims to examine the effectiveness of the Corona-Warn-App. There are two voluntary ways for app users to participate:

1. Event-based survey: Users who receive a notification of an “increased risk” (= red warning) are asked to participate in an online survey.
2. Event-independent analysis of epidemiologically relevant usage data of the Corona-Warn-App. This analysis is based on a voluntary and privacy preserving data donation by users.

For both the online survey and the donation of epidemiologically relevant usage data, the privacy of the users remains protected. In order to guarantee this protection and to ensure the authenticity of the data collected, various procedures are used, which are explained below.

### 1 Online survey

The online survey is triggered by an event in the Corona-Warn-App: the notification of an “increased risk” (= red warning). With this warning, the user is given the opportunity to participate in an online survey.

**1. User receives notification of increased risk**
- Status information with link to online survey is shown.

**2. User clicks on link to survey**
- Proof of authenticity (real device + app installed) is requested by the operating system.

**3. User participates in survey**
- One Time Password (OTP) is created and stored on the smartphone.
- Upon successful verification of the proof of authenticity, the request is processed (forwarding to the survey/storage of the data).

### 2 Donation of epidemiologically relevant usage data

Users have the option of voluntarily and continuously providing epidemiologically relevant usage data from their Corona-Warn-App for scientific evaluation without revealing their identity. This option can be activated in the Corona-Warn-App via the „data donation“ function.

**1. Data donation**
- As of version 1.13 of the Corona-Warn-App, users can voluntarily provide epidemiologically relevant usage data for evaluation. Consent can be revoked at any time.

**2. Evaluated data**
- Examples of epidemiologically relevant usage data: information on risk calculation, test results and the sharing of individual random IDs after a positive test result. In addition, information on age and region can be provided.

**3. Authenticity check**
- The technical usage data is requested once a day for upload to the CWA server. To prevent misuse, proof of authenticity (real device + app installed) is requested by the operating system. Proof of authenticity is transferred to the server.

**4. Upload after proof of authenticity**
- If the proof of authenticity is successfully verified, the epidemiologically relevant usage data are made available for evaluation.

Note: For reasons of clarity, some processes are presented schematically or simplified. Published by: Robert Koch-Institut, Berlin, March 2021.
Further information: www.rki.de/covid-19, coronawarnapp@rki.de