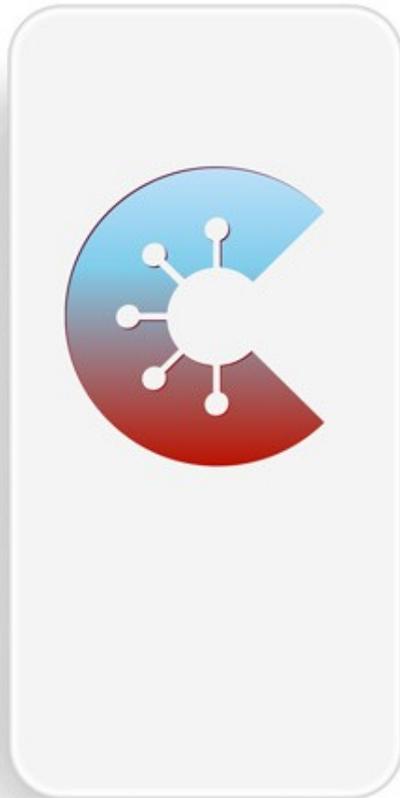


# CORONA-WARN-APP

**ERSTE INFOS FÜR INTERESSIERTE...**

# GEGENSTAND DER FOLIEN



DIE CORONA-WARN-APP:

**WIRD MIT  
JEDEM NUTZER  
NÜTZLICHER.**

Jetzt die Corona-Warn-App herunterladen  
und Corona gemeinsam bekämpfen.



# GRUNDLAGE: API VON GOOGLE UND APPLE

- » Die grundlegenden Funktionen zur Kontaktverfolgung werden vom Betriebssystem des Smartphones (iOS/Android) über eine Schnittstelle zur Verfügung gestellt (Exposure Notification API).
  - » iOS: ab Version 13.5
  - » Android: ab Version 6.0 mit aktuellen Google Play Services
- » Die Funktionen liegen brach, wenn keine entsprechende App installiert ist.
- » Schnittstellen und Design der API sind offengelegt.
  - » Siehe z. B. [https://en.wikipedia.org/wiki/Exposure\\_Notification](https://en.wikipedia.org/wiki/Exposure_Notification)
- » Vorteile:
  - » Tracing-Apps können nur die angebotenen Funktionen nutzen.
  - » User kann erkennen, welche App die Funktionen nutzt.
  - » User kann Nutzung der Funktionen unterbinden.

# TEMPORÄRE AUSWEISE: TAGESSCHLÜSSEL UND ID

- » Auf dem Smartphone wird alle 24 Stunden ein Tagesschlüssel generiert.
  - » Offizielle Bezeichnung des Tagesschlüssels: Temporary Exposure Key (TEK).
  - » Größe: 128 Bit
  - » Jeder Tagesschlüssel wird zufällig erzeugt. Er ist weder mit einem Konto, noch mit einer Geräte-ID oder mit irgendwelchen anderen Merkmalen verknüpft.
- » Aus dem Tagesschlüssel (TEK) wird auf dem Smartphone alle 10-20 Minuten eine ID generiert.
  - » Offizielle Bezeichnung der ID: Rolling Proximity Identifier (RPI).
  - » Größe: 128 Bit
  - » Jede ID (RPI) wird ausschließlich aus dem Tagesschlüssel erzeugt. Sie ist weder mit einem Konto, noch mit einer Geräte-ID oder mit irgendwelchen anderen Merkmalen verknüpft.

# WELCHE DATEN TAUSCHEN SMARTPHONES AUS?

## » Aussenden:

Das Smartphone sendet via Bluetooth Low Energy (BLE) 4-5x pro Sekunde die aktuelle ID (RPI) aus.

## » Empfangen:

Das Smartphone lauscht auf gesendete IDs (RPI).

- » Wie intensiv das Gerät lauscht ist nicht exakt festgelegt.
- » Empfohlen: mindestens alle 5 Minuten einmal lauschen.

# WAS SPEICHERT DIE APP?

- » Die App speichert die lokal erzeugten Tagesschlüssel (TEK).
- » Zusätzlich speichert sie für jede empfangene ID (RPI) die folgenden Informationen ab:
  - ID (RPI)
  - Datum und Uhrzeit des Empfangs
  - Dauer
  - Signalstärke (Entfernung)
- » Der Nutzer kann diese Informationen nicht einsehen.
- » Er kann sie aber jederzeit löschen.
- » Zusätzlich „altern“ die Informationen:  
Sie werden nach 14 Tagen automatisch gelöscht.

# WAS PASSIERT BEI EINEM POSITIVEN TEST?

- » Bei einem positiven Test werden die Nutzer gebeten, über die App ihre Tagesschlüssel (TEK) auf einen zentralen Server zu übertragen.
- » Das positive Testergebnis wird vom zentralen Server anonym verifiziert, um bösartige Infektionsmeldungen zu verhindern.

# WIE WIRD DER NUTZER GEWARNT?

- » Die Apps laden zyklisch die Liste aller (von den infizierten Nutzern der App freiwillig zur Verfügung gestellten) positiven Tagesschlüssel (TEK) herunter.
- » Aus den positiven Tagesschlüsseln (TEK) werden auf dem Gerät die entsprechenden positiven IDs (RPI) erzeugt und mit empfangenen IDs (RPI) verglichen.
- » Treffer werden von der App ausgewertet. Je nach Anzahl und Intensität der Treffer gibt die App eine Warnung aus und berät den Nutzer, was er nun konkret tun sollte.
- » Der Nutzer wird nicht über den Zeitpunkt der Exposition, die beteiligten IDs oder Tagesschlüssel informiert, damit der Infizierte möglichst nicht identifiziert werden kann.

# CORONA-WARN-APP: OPEN SOURCE

- » Der Quellcode der App und des zentralen Servers sind offen einsehbar (Open Source).
- » Analyse der Quellcodes zeigt:
  - » Die App ist nicht in der Lage, den Aufenthaltsort des Smartphones zu bestimmen.
  - » Die Funktionen der App und des Servers sind detailliert beschrieben und nachvollziehbar – es sind keine „merkwürdigen“ oder versteckten Funktionen vorhanden.
  - » Die App registriert sich nirgends.
  - » App und Server können nicht über das Internet ferngesteuert werden.
  - » Die empfangenen IDs (RPI) werden ausschließlich lokal auf dem Gerät gesammelt und niemals über Netzwerkverbindungen übertragen.
  - » Die Tagesschlüssel (TEK) verbleiben lokal auf dem Gerät, bis der Nutzer sie (nach einem positiven Test) freiwillig überträgt oder sie (automatisch) gelöscht werden.
  - » ...

# MEIN GANZ PERSÖNLICHES FAZIT

**DIE CORONA-WARN-APP IST KEINE  
SPIONAGESOFTWARE.**

**GANZ IM GEGENTEIL!**

**ICH HABE DIE CORONA-WARN-APP  
BEREITS INSTALLIERT.**

**INSTALLIEREN SIE DIE APP UND  
SCHÜTZEN SIE LEBEN.**