1. Motivation

The recording and tracking of contacts and thus possible infections through the encounter of persons infected with SARS-CoV-2 and others could considerably reduce the speed at which the pandemic spreads. Although centralized tracking by means of mobile phones seems technically possible, it raises considerable concerns about data protection. The state or whoever would collect and evaluate this data would be in a position to carry out total surveillance of citizens. This surveillance could possibly set a precedent for other, possibly less urgent cases.

However, it is also possible to achieve effective and efficient tracking, while fully respecting the privacy of the subscribers, by involving each affected individual. The solution presented should thus comply with the data protection rules of the EU-GDPR.

2. requirements

1. The application should efficiently and effectively identify and motivate people to be tested for infection in order to effectively contain the spread of the pandemic
2. The process should be automated where necessary and desirable. The users should also be involved in the process themselves.
3. The privacy of the persons should be protected as far as possible and necessary.
4. It should not be possible to centrally track the behavior of the users or the whereabouts of the users.

3. Method

An application would be installed on each participant's mobile phone that continuously monitors signals on the Bluetooth interface. If two participants approach each other, the phones exchange information. For this purpose, a secret key was generated when the app was installed and in addition, each mobile phone generates a random numerical code as a temporary ID[1] at certain intervals, e.g. every hour.

When approaching each other, the mobile phones exchange their temporary ID, and each mobile phone transmits its encrypted position to the other and, if necessary, a more precise distance between the parties determined via NFC. The mobile phones store the data in a local database[2].

- the time at which the exchange took place,
- the own temporary ID,
- the temporary ID of the other person and
- the position encrypted by the other person and

[1] E.g. a 20 digit number

[2] In order to avoid errors in the later allocation, the mobile phones should synchonise their stored data to time, position and distance in a suitable way

- if possible, the determined distance.

Due to the temporary character of the IDs and the encrypted positions, the entries in the database are to be considered as anonymously as possible.

If a person is tested positive for Covid19, parts of the data of this person can be read out with the help of a trustworthy institution, e.g. the health care organisation or the analysis laboratory, and transferred to a publicly accessible database. The data would be stored covering the potentially infectious period of time

- the dates on which the exchange took place,
- the related encrypted positions
- the corresponding own temporary IDs and
- the corresponding temporary IDs of the communication partners.

Optionally, other information is also conceivable, such as the distance or information about the infectious person, such as age or gender could be included[3]. The scope of this information could be determined by the trustworthy institution of data protection authorities It is important, however, that only the other contact person can decipher the exact positions from the published data.

Using simple database queries for their own temporary IDs and the corresponding times, people can determine whether they have been in the vicinity of an infectious person. These queries can be performed regularly and automatically. An algorithm is used to determine the risk of infection based on the duration and, if necessary, the distance of the encounter. The app notifies the person of this risk if the value exceeds a certain threshold. To an extent yet to be determined, the person will be informed about the approximate time and place of the potentially infectious encounter as well as any further information about the infectious person. On the basis of this information, each person concerned can decide whether he or she wishes to be tested for Covid-19 infection.

4. essential aspects

Positive aspects

- The involvement of those affected leads to a targeted identification of potentially infectious encounters, presumably better than would be possible via a centralized application. Thus, the affected persons can make a decision based on the more precise circumstances, as far as he/she still remembers them. He or she may have been wearing protective equipment at the time or may remember that someone in the immediate vicinity coughed or handed something to him or her.

[3] If the encryption is carried out as public-key encryption with temporary key pairs, it is possible to make the additional information about the infectious person available only to the persons concerned

- The notification of the affected persons can be done very promptly and automatically via the app.

Privacy concerns

- The affected and possibly infected person may be able to identify the infecting party on the basis of information on the place and time of the meeting. However, this problem cannot be solved completely. The processing should be covered by DSGVO Art. 6 para. 1 d) (vital interest) and e) (public interest) and possibly b) (law).
- Third parties could use the application to obtain information without authorization by means of queries specifying false temporary IDs. However, since the positions are encrypted and the temporary IDs are changed regularly, the information content is very low. A link to data collected elsewhere, e.g. data collected using a self-operated app at busy points, would in principle make identification possible. Ultimately, however, this is no different from the (illegal) technical possibilities of tracking people in public places if they have activated the wireless interfaces of their mobile phones.