

## Overview: How We Preserve Privacy and Maintain Security

Paragraphs 1-5 describe the flow of a reference implementation of PEPP-PT's mechanisms. Paragraph 6 gives a very brief glimpse at how we maintain information and infrastructure security. Please get in touch with our partner managers to receive a full documentation package on privacy and security.

### 1) Anonymous identifier donation.

Each PEPP-PT phone broadcasts over a short distance a temporarily valid, authenticated and anonymous identifier (ID) that cannot be connected to a user. Proximity between phones of other PEPP-PT users are estimated by measuring radio signals (Bluetooth, etc.) using well tested and calibrated algorithms.

### 2) Logging the proximity history.

When PEPP-PT phone A is in epidemiologically sufficient proximity to PEPP-PT phone B over an epidemiologically sufficient period of time, as determined by the measurements, the anonymous ID of phone B is recorded in the encrypted proximity history stored locally on phone A (and vice versa). No geolocation, no personal information or other data are logged that would allow the identification of the user. This anonymous proximity history cannot be viewed by anyone, not even the user of phone A. Older events in the proximity history are deleted when they become epidemiologically unimportant.

### 3) Usage of the proximity history: two modes of operation.

Mode 1

If a user is not tested or has tested negative, the anonymous proximity history remains encrypted on the user's phone and cannot be viewed or transmitted by anybody. At any point in time, only the proximity history that could be relevant for virus transmission is saved, and earlier history is continuously deleted.

Mode 2

If the user of phone A has been confirmed to be SARS-CoV-2 positive, the health authorities will contact user A and provide a TAN code to the user that ensures potential malware cannot inject incorrect infection information into the PEPP-PT system. The user uses this TAN code to voluntarily provide information to the national trust service that permits the notification of PEPP-PT apps recorded in the proximity history and hence potentially infected. Since this history contains anonymous identifiers, neither person can be aware of the other's identity.

### 4) Country-dependent trust service operation.

The anonymous IDs contain encrypted mechanisms to identify the country of each app that uses PEPP-PT. Using that information, anonymous IDs are handled in a country-specific manner:

Mode 1

If both anonymous IDs of phone A and B are from the same country, the anonymous ID of the potentially infected party can be marked, so that when this party's app enquires about his or her status, the app will be informed about the possible exposure.

Mode 2

If an anonymous ID of phone B is identified as being associated with another country than phone A, information associated with the anonymous ID of phone B is transmitted to the national trust service of the other country. This transmission is fully encrypted and digitally signed. Further processing is done by

the national trust service of the country that issued the app.

## 5) Healthcare Processing

A process for how to inform and manage exposed contacts can be defined on a country by country basis.

## 6) Information and Infrastructure

All procedures, mechanisms, standards and code at PEPP-PT is continuously monitored by our security team. In parallel national cyber security agencies and national data protection agencies inspect all of the above line-by-line on a regular basis and sign. We have always asked and continue to motivate security activities to get in touch to review and improve our code or procedures.

Anything released to the public is checked that way to prevent unintended effects in procedures or code exist and potential loopholes are closed swiftly.

## Our View on the Current Situation

The COVID-19 pandemic poses a major threat for countries around the world. In response to the rapidly growing number of cases and the danger of overburdening health systems, many countries have begun lockdowns to slow the spread of the new coronavirus. Since a long-term lockdown is not economically viable, the urgent question arises as to how an open society and economy can be maintained without risking a collapse of the healthcare system.

Experience in some Asian countries has shown that widespread testing, combined with isolation of confirmed cases and quarantine of their contacts, is an important part of a successful control strategy. The current bottlenecks in testing capacity are likely to be eliminated in the coming weeks. The challenge then will be to isolate confirmed cases and their contacts in a way that is compatible with our shared understanding of privacy in European democracies.

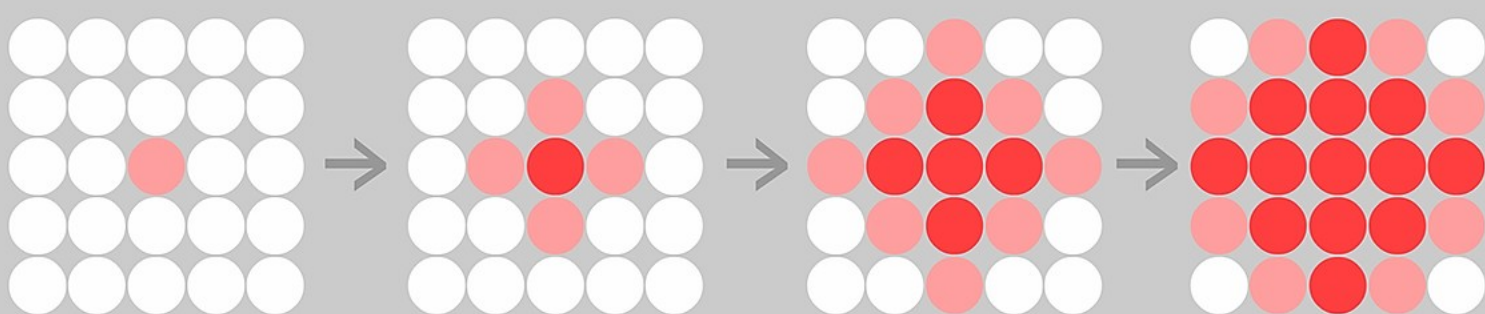
## The Approach

Contact tracing is a proven method to help contain the spread of infectious diseases. The aim is to inform the relevant contacts of infected cases as quickly as possible about the possibility of infection, in order for the right measures to be taken in a timely manner. In the case of SARS-CoV-2, a large proportion of transmissions occur through droplets that travel only over a certain distance (about 2 metres). Thus, “contacts” are people that may have been exposed to the virus in this way, through physical proximity. That’s why the PEPP-PT initiative uses the term "proximity tracing".

As far as COVID-19 cares, there are 3 kinds of people:



If we do nothing, here's what happens to a neighborhood with one Patient Zero:

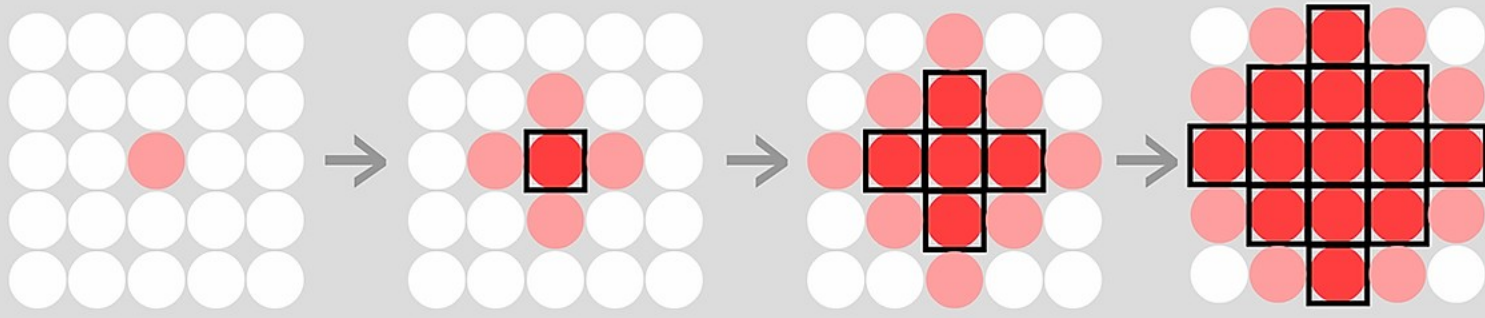


We get a wave of infections. of course.



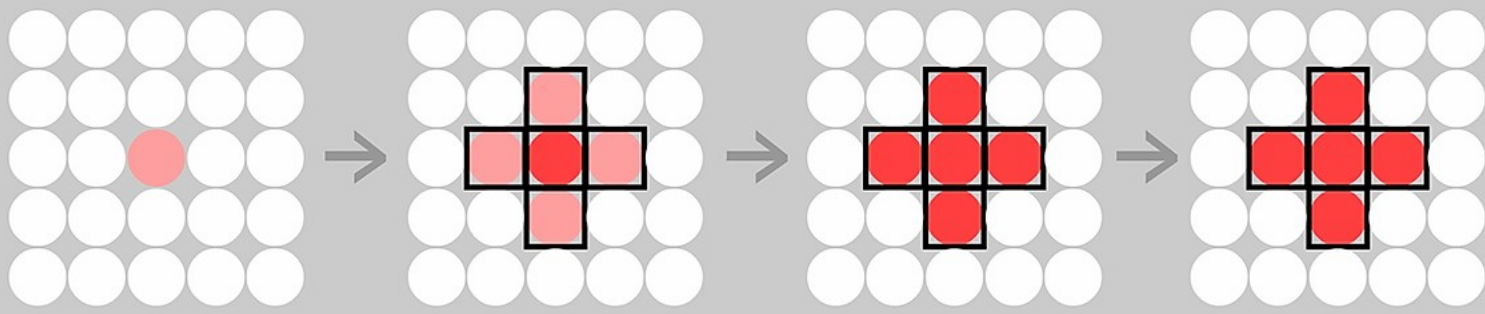
Why get a wave of infections, of course.

Here's what happens if, when someone finds out they're infected, they immediately self-isolate:



Alas, people are contagious *before* showing symptoms!  
We're one step *behind* the virus.

But here's what happens if, when someone finds out they're infected, they *and their close contacts* self-isolate:



The chain of transmission is broken! By finding & isolating close contacts, we're *one step ahead*.

CC0/Public Domain:  
remix & reuse freely!

by Marcel Salathé (epidemiologist)  
& Nicky Case (visualizer)

Isolation of contacts is necessary to prevent further transmissions. This approach has been shown to be effective for various diseases. The challenge in the current situation is the speed with which the new coronavirus spreads, as well as the already high case numbers. If the case numbers fall down to low levels due to the different intervention measures, rigorous testing and rapid quarantine of contacts can prevent further large outbreaks - until a vaccine is available.

Technology can make a decisive contribution to efficient and widely supported proximity tracing. But technology must be used and deployed responsibly. For this reason we - a team of scientists and developers in several European countries - have been working together for some time to build a non-profit initiative supplying amongst other services a technical solution that makes proximity tracing via smartphones possible. We don't track people and we don't get the data about who they are and where they have been, we only trace the virus to inform about exposure risks. Our approach is called "Pan-European Privacy-Preserving Proximity Tracing", this is why we are calling ourselves PEPP-PT.

## The Principles Diving Us Forward

The development of this technology is based on three basic principles. Firstly, it is the result of close European cooperation. Only in this way can we bundle the expertise on the continent in an efficient and targeted manner. Secondly, the technology should be internationally applicable, i.e. interoperable across national borders. In doing so, the technology will facilitate the resumption of international business and personal travel. And thirdly, the technology should be in line with the General Data Protection Regulation (GDPR).

**A health crisis must not lead to a weakening of privacy that so many generations before us have fought for.**

Developing such a system is a challenge, but one that is worth taking up. PEPP-PT is a core technology that provides an internationally applicable proximity tracing mechanism. Based on it, each country can develop its own app, and provide its own secure infrastructure. This allows each participating country to

implement its own operational follow-up in coordination with the local health authorities for the needs of the local people. Each country must also be able to convince its own citizens to participate in such a system. The underlying technology, which is being developed in constant exchange with data protection experts and ethicists, should make an important contribution to enabling cross-border proximity tracing while respecting privacy. It is scalable and open, and can be used by any country.

# BETTER TOGETHER. CONTACT US.

JOIN US

© Made 2020 by

***portvier***



[Cookie](#)

[Imprint](#)

[Data Prot](#)