Data Protection Impact Assessment for the Corona App

Kirsten Bock
kirsten.bock@fiff.de

Christian Ricardo Kühne
demian@fiff.de

Rainer Mühlhoff
rainer.muehlhoff@fiff.de

Měto R. Ost
meto.ost@fiff.de

Jörg Pohle
joerg.pohle@fiff.de

Rainer Rehak
rainer.rehak@fiff.de

Version 1.1 – April 15, 2020

Forum InformatikerInnen für Frieden und
gesellschaftliche Verantwortung (FIfF) e. V.

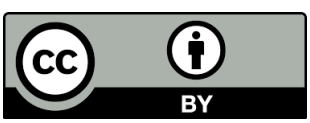
Contact: dsfa-corona@fiff.de

https://www.fiff.de/dsfa-corona

https://www.fiff.de/dsfa-corona

Version 1.1 published April 15, 2020.
Version 1.0 published April 14, 2020.

Document available here:
https://www.fiff.de/dsfa-corona



Summary and Findings

Since the SARS-CoV-2 virus started to spread across Europe in early 2020, public and political debates have increasingly centred around a technological solution to this most pressing problem. Could the pandemic possibly be contained by employing tracing apps on everyone's smartphone? These systems would automatically record all users' interpersonal contacts and thus make it possible to quickly trace the infection chains. Then, potentially exposed individuals could be efficiently tracked to isolate them at an early stage of infection.

States such as Singapore, South Korea and Israel have adopted some of the more radical approaches, strategies that represent, from the point of view of European legal systems, disproportionate infringements of fundamental rights. In response, European app initiatives have recently been formed, in particular the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) consortium, which is seeking to develop a corona tracing app with a commitment to data protection -– or at least to "privacy", which is not the same thing. Thus, there are tracing systems that are currently being designed that are comparatively more data protection friendly than others, even within Europe. For some weeks now, the accompanying media discourse has also conveyed the idea of corona apps *made in Europe* that might respect the "privacy" of all users and comply with the EU General Data Protection Regulation (GDPR).

However, data protection by design is not just a question of implementation, but a more complex consideration in need of precise and detailed discussion. The GDPR itself requires operators of large-scale data processing systems to produce a **data protection impact assessment (DPIA)** if the systems pose high risks to fundamental rights and freedoms. In our report, we show that a corona tracing system falls into this category. A DPIA is a structured risk analysis of data processing – compiled before operation – which identifies and evaluates possible consequences for fundamental rights.

Looking at the planned corona tracing systems, we are dealing with a large-scale social experiment that involves digital behaviour recording under state supervision in Europe. The effectiveness and implications of such apps cannot yet be predicted and it can be assumed that different variants will be rolled out and evaluated across the EU. The consequences in terms of data protection and thus in terms of fundamental rights will potentially not only affect individuals but also society as a whole. For this reason, it would be relevant for the public discussion to both prepare and publish a DPIA. Since none of the parties involved has so far presented a complete and generally accessible DPIA, and even the submitted *privacy impact assessments* are incomplete, we – a group of scientists and data protection experts organised in the NGO Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF, Forum of Computer Professionals for Peace and Societal Responsibility) – wish to present such a data protection impact assessment as a proactive and constructive contribution.

Overview of the data processing

In this DPIA, we refer to the primarily discussed frameworks and concept proposals for a European corona tracing app, which are based on near field sensor technology using Bluetooth Low Energy (BTLE). These particularly include PEPP-PT[1], the Decentralized Privacy-Preserving Proximity Tracing project (DP-3T[2]), and a general concept summarised by Chaos Computer Club spokesperson Linus Neumann[3]. Among these projects, the PEPP-PT project offers a framework – i.e. it does not offer a concrete app, but rather a specification for a suitable data processing system. Hence, within this framework, different implementations – i.e. concrete systems/applications – are conceivable; the DP-3T is one of the concrete proposals. The PEPP-PT framework basically allows each European nation to develop its own application. The framework thus strives to offer some national degrees of freedom while ensuring cross-border interoperability.

In this context, a key finding of our investigation is that the frameworks considered here – especially PEPP-PT – **do not specify important technical characteristics and process properties that have serious implications for data protection**. It is possible to roughly differentiate between at least three system architectures, all compatible with the PEPP-PT framework:

a) **A centralised architecture**: The anonymity of users and confidentiality of contact events is only provided with regard to outside entities, i.e. other users or external actors; the operators and involved authorities can, however, identify all users and connect them to recorded contact histories.

b) **A partially decentralised architecture**, which also allows for **epidemiological research** (e.g. DP-3T): Users and contact events are only concealed from other users and third parties; the server can de-anonymise positively tested users. The system also has a data donation function, by which users can choose to share their contact histories for epidemiological research. If done so, positively tested users' contact events would become visible to operators and authorities.

c) **A completely decentralised architecture** (see Neumann 2020): Users remain anonymous towards other users and third parties and their contact events would also remain secret. Operators and authorities can de-anonymise positively tested users but not their contact history. Epidemiological research is not possible.

Operators and authorities can ...	Type a	Type b	Type c
... de-anonymise all users	yes	no	no
... de-anonymise positively tested users	yes	yes	yes
... de-anonymise all contact events	yes	partly	no

[1] Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) (2020). URL: `https://www.pepp-pt.org/` (visited on 04/08/2020)

[2] Carmela Troncoso et al. (2020). *Decentralized Privacy-Preserving Proximity Tracing.* White Paper Version: 10th April 2020

[3] Linus Neumann (2020). *"Corona-Apps": Sinn und Unsinn von Tracking.* URL: `https://linus-neumann.de/2020/03/corona-apps-sinn-und-unsinn-von-tracking/` (visited on 04/09/2020)

Our **DPIA mainly refers to the most data protection friendly type, type c**, however, where useful, we also take the technical details of type b into consideration.

First, we conclude that **even the decentralised version entails serious vulnerabilities and risks** that have to be dealt with (for details see our full DPIA). Second, a comparison of the centralised and decentralised types shows that **essential data protection properties depend on the decision to opt for either a centralised or decentralised version.** Therefore, a PEPP-PT compliant version would not necessarily be data protection friendly.

Important insights, risks and solution approaches

We now summarise some key insights and outline some risks and solution approaches:

1. **The often stressed voluntariness of the app is illusory.** The use of the app as a prerequisite for relaxing the current corona quarantine is possible and is even already being discussed. People would then have to present the app before accessing public or private buildings, rooms or events. It is also conceivable that employers might swiftly adapt those practices to reopen their establishments more quickly by implementing such voluntary protective measures. This scenario would lead to *implicit coercion to use the app* and result in extremely unequal treatment of those who do not use the app. Since not everyone owns a smartphone, this would also discriminate against already disadvantaged groups.

2. **Without a capacity to intervene and a narrow purpose limitation, the protection of fundamental rights will be at stake.** There would be a high risk that mistakenly detected exposure events (false positives, for example, by contact measurements through walls between two apartments) would result in the unjustified imposition of self-isolation or quarantine. To prevent this, there is a need for legal and actual possibilities to effectively intervene, such as the recall of incorrect disease notifications, the deletion of incorrecly registered contact events with an infected person and the possibility to contest restrictions imposed as a result of the data processed. So far, none of the proposed systems account for that.

3. **All proposed tracing systems process personal data concerning health.** The procedure consists of processing contact data on smartphones, the transmission of this data to a server after the diagnosis of an infection and finally the distribution of this data to all other smartphones for testing for possible contacts with infected people. All data on a smartphone is personal data, related to the user of the device. Since only people who test positively transmit data to the server, the data transmitted constitutes data concerning health. The data processing is thus clearly subject to the GDPR.

4. **The anonymity of users must be enforced by a combination of legal, technical and organisational measures.** References to a natural person can only be effectively and irreversibly separated from the processed data through a multidimensional approach so that the resulting data is anonymous. All the proposals lack such an explicit separation process. In this DPIA, we have laid out legal, technical and organisational requirements that can be implemented to ensure effective and irreversible separation in practice – only under these

conditions can the resulting non-identifying infection-indicating data be stored on the server and distributed to all other apps.

For a comprehensive explanation of the risks and weaknesses, please refer to the respective chapters within the DPIA.

Generally, the data protection perspective sees **the essential risks of data processing as relating to the operators of a data processing system.** Therefore, it is strictly necessary that the barriers to improper processing – e.g. processing exceeding the purpose of the data processing – consist of an effective mix of legal, technical and organizational measures – and do not just entail the operators paying lip service to data protection. Measures taken must be actively made verifiable and documented clearly.

Open source development of the server and app software including all components – for example, in the form of free software – is an essential prerequisite for transparency regarding the implementation of data protection principles. This applies to data protection supervisory authorities but especially also to the data subjects and all members of (civil) society. Only then can confidence and trust be established among people not familiar with the details of information technology.

Third parties may also pose risks to fundamental rights. This does not primarily refer to hackers, but more to commercial actors like large platform operators or state bodies. These organisations may benefit from an increased volume of available tracking data since, first, the Bluetooth module must be permanently kept active for the corona app and, second, through access to extensive data stored in private actors' silos.

A data protection analysis considers the entire processing and its context, not only the app used for it.

In the public discourse and in the app projects we examined here, data protection is still reduced to the protection of privacy, i.e. to maintaining secrecy and confidentiality with regard to operators and third parties and in relation to aspects of IT security like encryption. This limited view not only ignores the considerable social and political fundamental risks we have identified in this impact assessment, it even obfuscates them.