COVID-19: A Governance Model for Digital Proximity Tracing

Core elements of a governance model for a digital tracing and alarm system

A result of a sub-group within the network «Digital Self-Determination» (Digitale Selbstbestimmung)

developed in the context of the Hackathon VersusVirus (https://www.versusvirus.ch) from 3 to 5 April 2020

Authors:[1]

Roger Dubach
Andrin Eichin
André Golliez
Dominique Keller
Christian Laux
Thomas Schneider
Martin Steiger

[1] The authors have drafted this report in their personal capacity.

A. Vision

Digital technologies, such as applications for mobile phones (apps), are important instruments in the fight against the COVID-19 crisis.

Digital technologies have the **potential** to supplement and reinforce already existing political and epidemiological measures. Especially when considering a possible exit strategy and a relaxation of existing measures, digital technologies to contain the Coronavirus, such as tracing apps, will become increasingly important. The use of these apps allows to warn individuals about possible infections at an early stage, thus isolating them quickly and minimising the risk of another wave of infections. Such a reduction in risk could favour a relaxation of restrictions on movement or economic freedoms. However, in order to have such an impact, these digital technologies must be widely used. This in turn requires a sufficient amount of trust among the population. In addition, the app and the underlying concepts must be easy to understand and just as easy to use.

Digital technologies, however, can also involve **risks**. Even before the crisis, the uncontrolled collection and use of data have become a source of legitimate concern. In the context of this crisis, concerns about state and corporate surveillance and the associated fear about the loss of fundamental freedoms have become even more relevant. Some are worried that our society might be unable to get rid of technological surveillance measures once this crisis is over. Such a price would be too high: we would trade our freedom against our health.

We firmly believe that using digital technologies to combat this crisis **should not boil down to a choice between fundamental freedoms and health**. We should be able to guarantee and enjoy basic freedoms such as privacy and health at the same time. In Switzerland, people should be at the centre of digital transformation - even in times of the Coronavirus. The development of digital tools in the fight against the virus should be used for the benefit and empowerment of all people. To ensure this however, we require new structures that enable the individual to actively control the digital transformation in the COVID-19 crisis.

The use of digital tools requires a framework that guarantees such a balance and empowers everyone to act independently in the digital space. This document defines key elements for the creation of a governance model in the context of the COVID 19 crisis. It is intended to support the deployment of an efficient tracing and alarm system by suggesting a framework that would ensure the necessary acceptance of the widest possible spread. On the one hand, these core elements are of a general nature and, on the other hand, they are based on the different impact levels, namely on the technical level, the domestic level and the international level.

The principles of digital self-determination are laid down in the Swiss Federal Council's "Digital Switzerland" strategy. In the context of these principles, the network “Digital Self-Determination” was formed to enable citizens, companies and public institutions to use the full potential of the data economy while ensuring our liberal and democratic values. With the core elements of a governance model presented in this paper, the authors want to contribute to the effort of ensuring that these values continue to be respected in the best possible way - even in the context of the COVID 19 crisis.

B. Explanations

In this document, the interaction between apps, protocols and IT infrastructures (data centres, devices, servers, operating software, etc.) for tracing possible infections and alerting the people concerned is referred to as a Tracing and Alarm System. To have the desired effect such a system must be embedded in an ecosystem that encompasses various data spaces, actors, processes and policies. Ultimately, this is about defining all the relevant interactions between the active actors (see below) and the relevant technical processes.

1. COVID-19 Data Spaces

A central data storage with a definable access concept is here referred to as a **data space**. Within the overall ecosystem, we have identified the following data spaces: a) the data space of the tracing and alarm system, b) a data space with directly-identifying personal data and c) a data space with other relevant data. The points at which data are collected and possibly processed are referred to as data sources.

a) Data space of the tracing and alarm system

An app for tracing and alarming will generate data. First, on the user's mobile phone and second, on a central infrastructure.[2] Specifically, this refers to randomly generated (ideally encrypted) identification data of the mobile device as well as any other information (e.g. date, time, duration, location, proximity - this additional information might not be provided depending on the solution). Only contacts from the last *n* days[3] in which an infection could have occurred are stored. Older contact information is deleted on a rolling basis.

b) Data space with directly-identifying personal data

Outside the tracing and alarm app, additional data is collected to contain the coronavirus. This typically includes data collected through the health system or through voluntarily submitted information from users. Depending on the data source, it can be directly-identifying data (e.g. name, gender, age, place of residence etc.) or refers to particularly sensitive data related to health (e.g. test results, medical information on the general state of health or previous illnesses).

c) Data space with other relevant information

This data space includes all other data relevant to the goal of tracking and containing the coronavirus. The source could be individuals, but also other forms of data collections that build the basis for aggregated data. These could for example include aggregated geo-localisation and movement data (e.g. travel routes, whereabouts as well as information about contacts with other people etc.).This data is especially relevant from a social perspective.

d) Connected data spaces

In principle, the data spaces described above can be connected with each other. This would create a new sort of data space with different data storage and handling implications. Those links and connections as well as the specific properties of the resulting data storage cannot yet be predicted. For

[2] See the annex for a more detailed explanation.

[3] This number must be defined in an epidemiologically effective and scientifically supported manner. For this reason, this paper refrains from giving any value for reference.

this reason, risk assessments for these data spaces are not possible and would be premature. However, a comprehensive governance mechanism also requires a method to control data spaces, which result of these connections. The basic principle in such a case should be that hidden data usage must be prevented: Additional connections to other data (spaces) may only be created if the risks have been identified, assessed and transparently communicated as part of an implementation project. Implementation projects must adhere to the governance model.

2. Actors

National tracing and alerting systems involve different actors at national, international and transnational levels.

a) National actors

In the Swiss context, national actors include the Swiss Federal Administration (in particular the Federal Department of Home Affairs (FDHA) and the Federal Office of Public Health (FOPH)). The Federal Administration is responsible for national coordination efforts. Other actors include the operators of the tracing and alarm system, cantonal authorities, research institutions and various actors in the Swiss health system.

In addition, a National Data Trust or Trust Centre[4] ("nationaler Datentreuhänder") should ensure the framework so that data can be reliably collected, managed, exchanged and used. The main task of the National Data Trust/Trust Centre is to ensure compliance with the governance model. In the context of the Federal Epidemic Diseases Act (Epidemiengesetz, EpG), Art. 54 f. EpG and Art. 58 ff. EpG are taken into account.[5] According to Art. 58 Para. 1 EpG, a suitable third party could already be commissioned to fulfil the role of a data trustee (i.e. the operator of the National Data Trust or Trust Centre). In cooperation with the governance model, the National Data Trust/Trust Centre keeps oversight on the necessary safeguards and ensures that the population is confident in using the technological solutions. In addition, it contributes to make relevant data publicly available, while ensuring that people remain in control of their data.

b) International actors

The governance model is destined to enable Switzerland to strengthen and coordinate its relations with other countries when implementing digital measures in the fight against COVID-19. In order to tackle the challenges of this global pandemic successfully, operational and strategic collaboration, based on the principles of digital self-determination, is essential. The same applies to relations with international organizations (e.g. the UN ecosystem, standardisation organizations, etc.).

c) Transnational actors

A governance model is only complete if it takes into account that Switzerland will also be influenced or challenged by other, transnationally acting third parties. These include providers of protocols (e.g. Pan-

[4] Within the framework of digital self-determination, a National Data Trust/Trust Centre could have various competencies and can be both a private law and a public law construct. In the present case, the idea of National Data Trust/Trust Centre closely follows the stipulations in the EpG.

[5] According to today's legal situation, this governance model should be read as a whole in the light of the Federal Epidemic Diseases Act (Epidemiengesetz, EpG): Provisions on the processing and disclosure of personal data in an epidemic as well as on the notification system, including responsibilities for compliance with data protection, are regulated in the EpG under Chapter 7, Section 2, in particular Articles 58-60, and in the more specific Ordinance on Combating Communicable Human Diseases (Epidemic Ordinance, EpV) under Chapter 6, Section 4 (Art. 88) and Section 5 (Art. 89 –99). In the medium term, however, the governance model outlined here could be included in the EpG and, if necessary and desirable, be adapted as part of a change in the law).

European Privacy-Preserving Proximity Tracing, PEPP-PT) or technical solutions (e.g. technology companies) as well as scientists. It is also important to take the necessary measures to protect against the harm that could be done by unlawful attackers.

C. Recommendations

A clear governance model is required to ensure a functioning and secure tracing and alarm system as well as guarantee the necessary confidence of both data users and data subjects in the ecosystem. In the following, we propose core elements for this governance in the form of recommendations:

- Systems: The recommendations should help to design all technical systems (apps, networks and other IT infrastructures) and the organs used to operate these systems in a digitally self-determined way.

- Data spaces: The data spaces based on these technical systems have to be subject to a control mechanism which guarantees the respect of fundamental principles as well as the concept of digital self-determination.

- Actors: In addition, the governance model should form the basis for an oversight and coordination of the actors involved in the systems and the operation of the data spaces. This document also provides core elements for this aspect.

In line with the vision set out above, the recommendations aim to create trust and motivate people to make their data available to the system - in the knowledge that their data will be safe and can be used both for the benefit of themselves as well as that of society as a whole. Accordingly, the objective is to have a governance model that is as simple as possible: it should provide easy-to-understand guidance and enable maximum protection for the population.

The recommendations are divided into three categories: (a) the technical level; (b) the national level; and (c) the international level. They are supplemented by general recommendations: these are the key elements of governance and as such must always be adhered to.

1. General recommendations

Core elements of general nature	
1.1	The use of digital technologies to combat the COVID 19 crisis must not boil down to a choice between freedom and health. In particular, the tracing and alarm system must under no circumstances lead to citizens being surveilled (neither by the state nor by private entities).
1.2	Within the framework of the legal system, citizens have the greatest possible control over their data and the processes and decisions based on this data.
1.3	Citizens can assess the impact of their actions in the digital space. There is transparency as to how and for what purpose(s) their data is recorded, processed and used, in which data spaces the data is stored, how and by whom their data is managed and who has access to it.

1.4	The use of digital applications is voluntary. Citizens should be able to freely pass on data.
1.5	The right to a copy and other rights of data subjects under data protection law (namely information, inspection, correction and deletion) are guaranteed.

2. Technical level

On the technical level, the recommendations relate to the specific design of the tracing and alarm system. This consists of the following three components: firstly, a basic protocol; secondly, the development of software (app, either integrated into an existing application or as a new solution to be developed); and thirdly, the operational infrastructure of the operating organization.

Core elements for the basic protocol of the tracing and alarm system	
2.1	The basic protocol must not lead to the tracing and alarm system becoming a surveillance instrument (neither by the state nor by private individuals).
2.2	The basic protocol guarantees anonymity and is compatible with data protection law.
2.3	All data that can be anonymized or encrypted without impeding the goals of tracing and alarming shall be anonymized or encrypted. Data is generally stored decentrally on the end device of the user.
2.4	The basic protocol only provides for the disclosure of data (this also includes uploading to a data space or transferring it to other participants) if this is absolutely necessary. Data is only centralized with the explicit consent of the user.[6] Even after consent, users must be protected as best as possible.
2.5	An alarm can only be initiated by an authorized specialist (e.g. doctor).

Core elements about apps within which the alarm system is embedded	
2.6	The app must not lead to the tracing and alarm system becoming a surveillance instrument (neither by the state nor by private individuals).
2.7	The app guarantees anonymity and must not violate data protection law. If links to people can be derived from the origin of the app from an app store, the state must take appropriate measures.
2.8	The use of the app and the disclosure of data is voluntary. The app follows the central principles of data protection law: data minimisation and privacy by design. The app provides voluntary and transparently explained consent mechanisms (“opt-ins”). Data spaces are designed so that at any time the revocation of consent is implemented immediately and automatically at the data level.
2.9	Users must be informed in a simple and understandable manner about the purpose, technical functionality and legal consequences of using the app. Terms and Conditions must be drafted as simple and understandable as possible (see also core sentence 3.15).

[6] Storage in central data rooms should only take place if there is an important epidemiological need for this and the general recommendations (core elements 1.1–1.5) are not undermined thereby. The public should be consulted appropriately before implementation.

2.10	The source code of the app (including the basic protocol) is freely available and can be freely changed and used subject to the obligation to give credits to the authors.

Core elements on operational infrastructure and organization	
2.11	The company/organization operating the app submits to the governance model defined here. The above core elements must be adhered to throughout. The core elements 2.12 and 2.13 also apply.
2.12	The principle of data minimisation applies. It is implemented by automatically deleting data, unless users expressly consent to the extended storage for a limited period of time in advance (applies to data storage on the mobile phone as well as data storage in data spaces, if such occurs at all).
2.13	IT infrastructures for operating the app and / or data spaces must be secured by the operators against unauthorized access by third parties or their own personnel.

3. National Level

At the national level, we suggest recommendations for federal institutions and other agencies in Switzerland. At this level, recommendations for the design of the National Data Trust are essential.

Core elements on the responsibility and role of federal and cantonal authorities	
3.1	The federal and cantonal authorities, as per their competencies, shall have the overall oversight and responsibility. The coordination role at the federal and cantonal levels are to be performed by the responsible bodies.
3.2	The principle of proportionality must be strictly adhered to. Authorities shall apply it throughout the planning and implementation cycle (in particular, the principles of suitability, necessity and balancing of interests must be adhered to).
3.3	If, from a civil liberties perspective, a less invasive measure is possible then this measure should be chosen even if, as a consequence, other goals can no longer be achieved. Section 3.4 is reserved.
3.4	If the mission of protecting civil liberties has the effect that a tracing and alarm system is not possible or cannot meaningfully be implemented, the authorities examine possible restrictions of the affected civil liberties, applying the principle of proportionality. If those restrictions are necessary, mitigating measures shall be introduced where possible. The intervention must be strictly limited in time and must be completely rolled-back once it is no longer necessary.
3.5	The authorities, within their competencies, ensure that this governance model is enforced.

Core elements with regard to the National Data Trust/Trust Centre)	
3.6	The National Data Trust / Trust Centre) shall be operated by the Confederation, by the cantons, or by third parties commissioned by them.

3.7	The National Data Trust / Trust Centre operates the relevant data spaces (those that are considered justified in the sense of the above provisions and are implemented accordingly).
3.8	The National Data Trust / Trust Centre always adheres to the purpose limitation principle. Data must be processed exclusively for the purposes of anonymous tracing and anonymous alarming (alarming without personally addressing the individual, and without listing the individual as a suspected case in any directory).
3.9	The National Data Trust / Trust Centre ensures that all the data it manages is protected against access by unauthorized third parties.
3.10	The National Data Trust / Trust Centre ensures that organisations operating the apps are suitable carriers for tracing and alarm systems. This suitability must be verifiable and continuously verified.

Core elements regarding data sharing within Switzerland	
3.11	If possible, data exchange must be automated via system interfaces (application programming interfaces, APIs).
3.12	Both the state and third parties are prohibited from using data beyond the original purpose (tracing and alerting system) as long as the respective users have not given their explicit consent.
3.13	Further use of data should not require any further technical implementation measures, provided that users have voluntarily given their consent. Users can withdraw their consent at any time (core elements as per section 2.8 shall apply accordingly).
3.14	Anyone wishing to use shared data must submit to this governance model. Anyone using shared data shall be subject to the control of the National Data Trust / Trust Center.
3.15	Any use of data shall be communicated in a transparent manner. The communication shall be substantially comprehensive, using simple language. The main aspects shall be set out in such a way that the affected individuals can always properly assess to what extent they could be exposed to risks if they consent to the extended use of data.

4. International level

The third level includes recommendations for coordination and the sharing of best practices with international actors, as well as mechanisms for promoting the principle of digital self-determination on a global level.

Core elements for coordination and exchange with international actors	
4.1	Switzerland should actively seek coordination with other countries (especially our neighbouring countries as well as other countries with heavy inbound or outbound traffic to and from Switzerland) and with international organizations (e.g. the WHO) in order to ensure the interoperability of technical applications, in particular the tracing and alarm system.
4.2	System boundaries should be set up towards states that cannot guarantee Switzerland's governance model. System boundaries can be built in a way to take into account the special needs of other countries, provided that these needs and the resulting risks for users are

	communicated transparently and reliably.
4.3	Switzerland should actively promote the international exchange of experience with respect to the use of digital applications to combat COVID-19. Namely, Switzerland should contribute its own experience and gather experience from other countries. Existing international committees and forums can be used to facilitate the rapid transfer of knowledge and exchange of best practices.
4.4	In order to counter the risks of international mobility, regulations should be coordinated at the international level so that not every country introduces its own entry regime. It is assumed here that system integration between national systems is made possible via system bridges (“data feeds”).
4.5	Switzerland should strive to ensure that the general core elements (paragraphs 1.1 - 1.5) as well as the core elements under paragraph 2 will be respected by the international partners with whom Switzerland integrates the respective tracing and alarm system.

Core elements regarding international data sharing	
4.6	The exchange of personal data or personally identifiable data should take place in an anonymized manner and should only serve the purpose of notifying (“alerting”) potentially infected people. The data exchange must not lead to the alarm system becoming a surveillance instrument of a government.
4.7	Switzerland shall conclude an international agreement with foreign partners defining the conditions under which data can be exchanged between national systems.
4.8	Switzerland shall transparently disclose the basic protocol of its tracing and alarm system to other countries and demand the same in return.
4.9	If possible, Switzerland ensures compliance with the governance model at hand. In any case, the core elements in sections 1.1 - 1.5 must not be compromised.
4.10	Switzerland ensures that other countries commit to complying with the core elements set out in this paper. Other countries shall not use data contrary to the original purpose as set out in section 3.8. Sections 3.11 - 3.15 are reserved. In any case, data retention (see core element 2.12) must be limited.

Core elements with regard to other third parties	
4.11	The governance model defines standards to meet cyber security requirements, which are subject to democratically legitimate control.
4.12	Technical offerings from foreign providers must be checked for compatibility with the governance model. Transparency must be emphasised, and a democratically legitimized review must be carried out.
4.13	The parameters of the protocol must be checked for compatibility with the governance model. Transparency must be emphasised, and a democratically legitimised review must be conducted.
4.14	Established scientific opinions must be integrated in a proactive manner, whereby the principles of transparency and democratically legitimised review must be observed.

4.15.	Switzerland should introduce new criminal standards, should this be necessary to effectively deter third parties from snooping into any data exchanges via the Bluetooth interface on the mobile phone.

* * *

Annex

Technical & functional processes of a tracing and alarm system

To put it simply, a tracing and alarm system works as follows: Via Bluetooth or Bluetooth Low Energy (Bluetooth LE, BLE), the mobile devices connected to the system and in critical proximity[7] to one another for longer than a specified time, exchange their encrypted identities. Via this process an encrypted log of contacts is created on each party's device. As soon as a user of the system has tested positive for the coronavirus an alarm is sent to all contacts present in that log via a trusted service (and after approval by the responsible doctor). Depending on the protocol definition, this message can also contain the location of the encounter and a time stamp.[8]

Protocols based on symmetric encryption

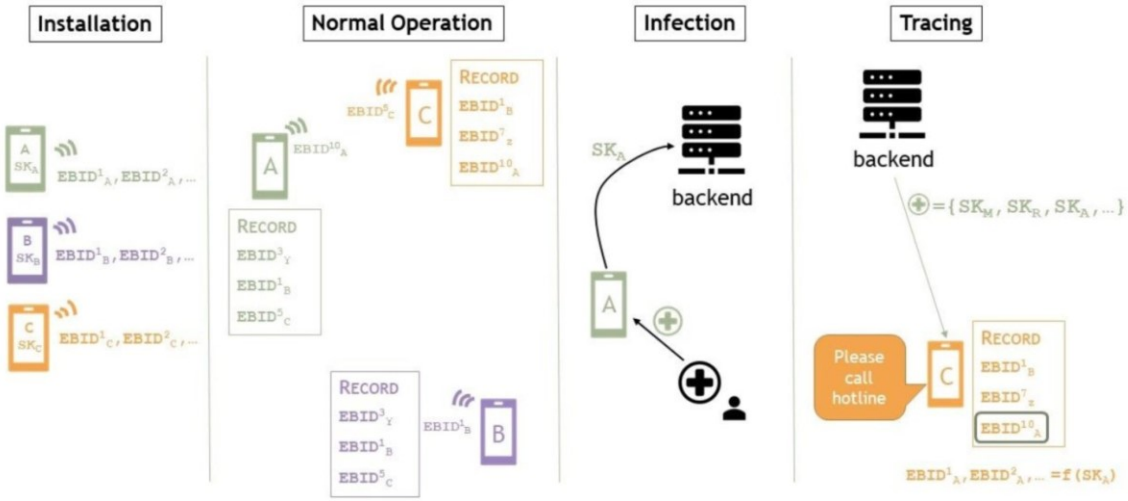

Figure 1: Phases in the decentralized proximity tracing system

(**Source:** documents/DP3T - Data Protection and Security.pdf at master · DP-3T/documents.)

Explanation of step "Installation" in figure 1: At the core of a symmetrical encryption model are small, constantly changing identification files ("tokens") that are quickly issued by a master key (master seed) on the cell phone.

Explanation of the step "Normal Operation" in Figure 1: The mobile phone continuously sends the latest token to the public, via Bluetooth, so that a person in physical proximity can save the token on their mobile phone. This is how "proximity" is determined as a starting point.

[7] «Epidemiologically sufficient proximity in epidemiologically sufficient period of time» (https://www.pepp-pt.org/content).
[8] For further references to the PEPP-PT project see https://github.com/DP-3T/documents.

Explanation of the step “Infection” in Figure 1: Anyone who registers as infected (or is only allowed to report as infected after being checked by a doctor) now publishes their master key to the network.[9]

Explanation of the “Tracing” process step in Figure 1: Users that have been tracked in the log of the person reported as infected (in Figure 1 this is person A) now receive a message (for example: “Please call hotline now”). In Figure 1, person C is such a recipient. This means that anyone who has been in the vicinity of the infected person for a sufficiently long time can see that they could also have been infected.

Discussion of a protocol based on symmetric encryption

Publication of the location history to an open group of recipients: Any recipient who has received one of the countless tokens can reconstruct the sender's movement profile (usually for the past 14 days); for this usually is tied to the master key as a whole.

Snooping: One consequence of symmetric encryption is that a powerful antenna installed near a public place can passively record data traffic via the Bluetooth interface. Since it thus knows the token of the person later infected, this antenna can also reconstruct the person's movement profile. Those who can afford an antenna can potentially snoop.

Conclusion: A protocol with symmetric encryption therefore does not meet at least two of the requirements according to the work of Cho / Ippolito / Yu (see Cho / Ippolito / Yu, Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs).

Discussion of a protocol with centralized data storage

No anonymity: It is important to understand that an app that is downloaded from an app store can be linked to a person (re-identifiability from the perspective of the Swiss federal institutions). There is thus no anonymization. This is relevant insofar as data storage occurs not only locally (on the mobile device) but at a central data storage location too.

Profile formation: If central data is stored, profiling is possible. This should be assessed in light of the claim that surveillance must be made impossible (and also measures having the same effect).

[9] «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.» (https://www.pepp-pt.org/content).