DATA PROTECTION IMPACT ASSESSMENT REPORT

CONTENT

I. BACKGROUND INFORMATION

1. General Information

Project Name	DP^3T Contact Tracing System	
Assessment Completed by:	Document Owner:	**EPFL** – Ecole polytechnique fédérale de Lausanne (Prof. Edouard Bugnion)
	External Legal Adviser:	***id est* avocats Sàrl** (Michel Jaccard & Alexandre Jotterand)
Document version	Version 1.0, 01.05.2020	

2. Project Outline – What Is It That Is Being Planned?

"*Decentralised Privacy-Preserving Proximity Tracing*", in short **DP^3T**, is a secure and decentralised privacy-preserving proximity tracing software system ("**DP^3T**" or the "**system**").

Its goal is to simplify and accelerate the process of identifying people who have been in contact with a person tested positive to the SARS-CoV-2 virus ("**COVID-19**"), thus providing a technological foundation to help slow the spread of the virus.

The system aims to minimise privacy and security risks for individuals and communities and guarantee the highest level of data protection. It further aims at ensuring that the deployment of a proximity tracing technology for the purpose of addressing the COVID-19 virus will not result in governments obtaining surveillance capabilities which will endanger civil society.

The system generally complies with best practices in the industry, including the requirements specified by the European Data Protection Board ("**EDPB**") in its Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (the "**EDPB Guidelines 04/2020**"). This document contains in enclosure a detailed analysis of DP^3T's compliance with the requirements set out by the EDPB in the "analysis guide" attached to the EDPB Guidelines 04/2020.[1]

3. Description – Why Is the Project Being Undertaken?

There is growing interest from politicians and health authorities around the world in technological approaches to help individuals and countries navigate and fight the COVID-19 pandemic.

In the period of the crisis during which governments intend to ease the restrictions that were imposed on the population (lockdown, social distancing, etc.), the fact that COVID-19 asymptomatic people can still spread the virus poses a new challenge, reinforcing the need to trace people at risk in the early stages of the disease, and to trace interactions that may have taken place with people whom an individual cannot reach out to".

[1] See below Section VII. pp. 43 ff. The EDPB Guidelines 04/2020 may be accessed at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

One suggested approach has been to make use of Bluetooth signals on personal smartphones to provide a system that informs users about encounters with individuals who have since tested positive for COVID-19.

However, the proposed infrastructures underlying such proximity tracing systems vastly differ in their privacy and security properties. Some proposals may fail to protect highly sensitive data, or have the potential to be misused or extended far beyond their initial purpose and the lifetime of the crisis.

This is all the more important given the global nature of this challenge and the fact that the pandemic reaches across borders and jurisdictions with different levels of fundamental rights guarantees, in times where many governments are functioning under states of exception.

Among different approaches, there are currently two categories of solutions that propose setting up infrastructure tasked specifically to only collect data needed to fulfil the proximity tracing needs of health authorities or epidemiologists (which are referred to as "designs to minimise data collection"):

- **Centralised models** attempt to minimise data by generating and keeping track of ephemeral identifiers distributed to users which can be used to construct the contact graph of a user only in the case they are infected. The generation of identifiers and generation of contact graphs are done on a server which is often assumed to be controlled by a government or another "trusted" entity. Any identifiers that an infected individual uploads to the system that he or she has observed can be resolved by the server into a persistent identifier that can be used to single-out an at-risk user. This model assumes that the entity running the server shall not misuse the data and capabilities of the server in cases beyond managing infection progression, for example, at the request of law enforcement, border control or intelligence agencies. Such protection relies on the protection of the central server which can potentially be repurposed into a 'data grab' model (i.e. a model that relies on a disproportionate collection of personal data in time of crisis, and assumes legal protections will be sufficient to protect populations which is often not the case).
- **Decentralised models** are designed to keep as much data on user devices as possible. Methods are introduced to strictly control data flows in order to avoid accumulating any contact data on a centralised server. This means that a server exists but only to enable people to use their own devices to trace contacts. The server is not trusted with personally identifiable information at all, cannot use any identifiers to single out an individual, nor does it provide any individual with the identifiers they should broadcast, and therefore is much less vulnerable to function creep than all other solutions.

While other international initiatives currently focus on centralised models, as is the case of the Pan-European Privacy-Preserving Proximity Tracing project ("PEPP-PT")[2], the international consortium that developed the DP^3T system[3] reached the conclusion, after careful consideration, that a decentralised model must be preferred.[4] This follows the legal requirement to build in technical and organisational measures to ensure that only the personal data strictly necessary for the purpose of the system are processed, in line with data protection by design and by default.[5]

---

2 As of the date of writing, France's and UK's systems follow a centralised design based on PEPP-PT (see: https://www.ft.com/content/d2609e26-8875-11ea-a01c-a28a3e3fbd33; https://www.swissinfo.ch/eng/european-coronavirus-app-platform-gains-traction-with-governments/45699466). Germany indicated on 28.04.2020 that for privacy reasons, it was abandoning its plan for a centralised design in favour of a decentralised solution (https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J)

3 The consortium members are listed below in Section I.7., p 8.

4 See also the "Contact Tracing Joint Statement: Date 19th April 2020" signed by 579 researchers and scientists (as of 28.04.2020) around the world (https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/)

5 Art. 25(2) GDPR.

By relying on a decentralised architecture[6], DP^3T better protects the privacy of the individuals and mitigates the risks generally associated with centralised designs, which include:

- intrinsic vulnerabilities of centralised data minimisation models, including the risk of the system being attacked and compromised, in breach of the security principle;
- limitations of the effectiveness of legal safeguards and the impossibility of true anonymisation;
- the system being repurposed, leading to function creep and breaches of the purpose limitation principle; and
- loss of trust, leading to lack of adoption and significant numbers of false negatives, endangering the accuracy principle.

The EDPB considers that a decentralised solution generally is more in line with the data minimisation principle than a centralised one.[7] The European Parliament has also expressed its preference for decentralised solutions in a recent resolution.[8]

4. Functionality – How the System Works?

The functioning of the DP^3T system is described in detail in the white paper[9] available on the GitHub webpage of the project.

An explanatory comic is also available in many languages on another GitHub webpage,[10] as well as a summary of the project.[11]

In a nutshell, the decentralised system underpinning DP^3T works in four phases:

1. **Installation**: an app (the "**User App**") is installed by individuals ("**Users**") on their compatible smartphones from either the Apple App Store or the Google Play Store. Google and Apple have made common efforts to develop an API that will allow the detection of close contacts between iOS-iOS, Android-Android, and iOS-Android devices, using the same algorithm.[12]

   The installation requires agreeing to receive notifications (pop-ups) and enabling Bluetooth. The installation and setting up of the User App do not require the Users to create a login nor to provide any other personal data.

2. **Normal operation**: Users continually run the User App, which broadcasts via Bluetooth an ephemeral, pseudo-random ID representing the User ("**EphIDs**") and also record pseudo-random IDs of other Users observed from smartphones in close proximity, together with the duration and an approximate indication of time (e.g. April 2).

   All data remains exclusively on the User device (each User App storing its secret key (SK) and the EphIDs that have been recorded from the devices in close proximity).

---

6 Despite being decentralised, DP^3T has a backend. There is, however, no central point of trust for security and privacy. All critical operations (creating EphIDs and matching observations) are done locally in each phone. The backend server is only needed to ensure availability and does not maintain any sensitive information. Attackers would not gain anything by compromising the backend. All privacy-sensitive information is decentralised, and stored on individual phones.

7 EDPB Guidelines 04/2020, § 42 and footnote 18.

8 "European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences" (2020/2616(RSP)), para 52.

9 https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

10 https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon

11 https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf

12 Apple and Google have released a joint specification describing their system support for privacy-preserving proximity tracing on iOS and Android.

3. **Handling COVID-19 positive patients**: Healthcare providers diagnose individuals that have tested positive for COVID-19 (no distinction being made between those that use the User App and the others). After a positive diagnosis, the healthcare provider will ask the individuals if they have installed the User App and if they are willing to send their EphIDs to the backend server to facilitate contact tracing. If the User opts in, they proceed as follows:

   (i) The healthcare provider generates an authorisation code for the User, e.g., in the form of a QR code.[13] The healthcare provider shows this QR code to the User.

   (ii) The User instructs her app to scan the QR code to obtain this authorisation code.

   (iii) The User App opens an encrypted TLS connection to the server and sends to the backend server (a) the authorisation code and its secret key (SK), or (b) a compact representation of the EphIDs it has broadcast during the infectious window.[14] This upload does not include the push-notification identifier.

   (iv) When the backend server receives the upload, it verifies the authorisation code, and stores the secret key (SK) and the uploaded EphIDs. It does not store any other information related to the upload (such as IP addresses or time).

   The identity of the User cannot be derived from the data stored by the server or by the User App of other Users.[15] Before a voluntary upload, no data other than the EphIDs broadcast via Bluetooth leaves the User device.

   The authorisation process described above aims at ensuring, in accordance with the requirements set out by the EDPB,[16] that only data of COVID-19 positive persons, as confirmed by a healthcare professional, is uploaded to the backend server.

4. **Decentralised contact tracing**: The User App of each User (i) periodically queries the backend server for the information uploaded by COVID-19 positive Users and (ii) locally reconstructs the corresponding EphIDs of COVID-19 positive patients, in order to determine whether the User was in physical proximity of a COVID-19 positive person and potentially at risk. If this was the case, the User App can inform the User and recommend certain actions (e.g. to self-isolate, go to a testing centre, etc.).[17]

Additionally, DP^3T protocol may allow Users – if this functionality is implemented[18] – to voluntarily provide anonymous data to epidemiology research centres.[19]

DP^3T provides built-in, strong, mathematically provable support for privacy and data protection goals and minimises the personal data required to what is necessary for the tasks envisaged. Furthermore, DP^3T aims at strictly limiting how the system can be repurposed through the application of cryptographic methods and prevent misuse and function creep.

[13] Country-specific. This can also be a single-use, 9-digit code, that is randomly generated by the system (and serves the same purpose).
[14] This is country-specific: DP^3T protocol may be implemented in order to send (and later store) either the secret key (SK) or the compact representation of the broadcast EphIDs.
[15] See below Section II.3. pp. 15 ff.
[16] EDPB Guidelines 04/2020, § 46.
[17] These actions are country-specific.
[18] See below Section I.10. p. 12 for information on the scope of this report.
[19] The data which may be provided for this purpose includes aggregates of day and time of exposure to COVID-19 positive Users (but not the identity or even EphIDs of these Users). Users would experience no detriment from refusing to provide such data, in line with GDPR, recital 42.

5. Purpose – What Is the Purpose of Collecting the Information Within the System?

The DP^3T system is intended to be deployed during the COVID-19 pandemic and pursues the aim of fostering private and public health by early detection of potential exposition to the virus.

Its sole purpose[20] is to quickly inform contacts of a COVID-19 positive person that they may have been exposed through close-range physical proximity with a COVID-19 positive person. The goal of proximity tracing is to determine who has been in close physical proximity to a COVID-19 positive person, without revealing the contact's identity or where this contact occurred. After contact, the person receives instructions on which further actions to take (this part is country-specific).

The intent behind the system is to inform individuals that they may have been at risk before they become contagious, thus stopping (or slowing down) the spread of COVID-19.[21] This is based on current scientific understanding of epidemiologists, which indicates that pre-symptomatic carriers of COVID19 can be contagious up to 2-3 days before the onset of symptoms, but that the disease also has a latency period.

The DP^3T system does not aim to provide the following functionalities:

- **Monitoring compliance with governmental measures**: the DP^3T system cannot be used for the purpose of monitoring compliance with quarantine or confinement measures, social distancing or other measures imposed by the government.[22]
- **Tracking COVID-19 positive patients**: once infected patients report themselves, the DP^3T system does not attempt to track them, nor does it provide a mechanism to ensure that they comply with medical orders. The goal of the app is to avoid asymptomatic users unknowingly spreading a disease. Diagnosed users are assumed to be responsible and take precautions if necessary when going into the public, for instance to a doctor's appointment. Therefore, the system is not designed to detect contacts with infected patients after their diagnosis and does not attempt to detect or prevent misbehaviour. The reason being that the gain in utility (one irresponsible person being under control) does not justify the loss of privacy for other well-behaved infected Users. Moreover, this is not a location-tracking app and cannot determine when a user is "in public."
- **Finding hotspots or infected users' trajectories**: the DP^3T system does not attempt to identify locations that have a concentration of infected people. This is a design decision. The purpose of the application is limited to the two goals specified above, which enable to collect and process specific data. In particular it avoids collecting location data, which is highly sensitive and very difficult to publish in a privacy-preserving way.[23]

[20] This conforms with EDPB Guidelines 04/2020 "PUR-1" requirement (p. 14).
[21] The idea behind contact tracing in general is to clinically interview a newly confirmed case and all of her recent contacts (during the contagious period) and make a determination of quarantine. For proximity-tracing, the intend is to notify cases where the two subjects do not know each other. The subject at risk, who receives notification from her phone, voluntarily calls the hotline and follows a clinical interview, which may also lead to a diagnosis that self-quarantine is the appropriate choice. This process is voluntary, and the interview protocol is the responsibility of the public health authorities
[22] This conforms with EDPB Guidelines 04/2020 "PUR-2" requirement (p. 14).
[23] This conforms with EDPB Guidelines 04/2020 "PUR-3" requirement (p. 14).

6. Privacy Impacts – What Are the Potential Privacy Impacts of this Project?

In General

DP^3T is a contact tracing system aiming to be used on a large scale by the population of a country to help combat the COVID-19. Any such system may have an important impact on the privacy and other fundamental rights and freedoms of individuals if appropriate safeguards are not put in place.

As underlined by the EDPB,[24] individuals should not have to choose between an efficient response to the COVID-19 crisis and the protection of their fundamental rights. The DP^3T system aims to provide an effective solution to fight the COVID-19 crisis, while protecting individual privacy.

In particular, DP^3T is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on proximity information regarding with respect to other users.

The use of the DP^3T will mainly imply that the required data will be collected for each User to determine the persons with whom a specific User has interacted. Although the system relies on the collection of information that cannot be linked to individuals (non-personal data), such information may relate to the health of the Users, if they decide to upload their data following a positive diagnosis for COVID-19. The risk of individuals being identified cannot be entirely excluded.[25]

High-Level Risks and Mitigations

The type of data being collected on Bluetooth connections could reveal information about families, societies, and communities. To address this issue, the DP^3T system has been designed to ensure it is never centralised, and such a risk does not materialise.

Digital contact tracing processes require input data to trigger an at-risk status, typically a test result. Such data is likely to be characterised as sensitive data under data protection laws. DP-3T has been designed in order to avoid that a central server or other users have any way with means reasonably likely to be used to discover the infection status of someone else through attacks on the protocol itself.

However, it should be noted that contact tracing of every type brings privacy risks even if carried out carefully. Individuals in small communities may receive alerts and calls which, when compared, lead them to identify (rightly or wrongly) the source of their at-risk status. This is similarly the case for manual contact tracing and for automatic contact tracing. While risks of attacks that can reveal such information from just one user of the app may be mitigated, social processes will always present a privacy risk to others where any form of contact tracing is involved.

The DP^3T system must form part of a national strategy, and the information provided to Users determined to be at-risk, and the data protection implications of any action they are expected to take beyond that, falls outside of the scope of this report.[26] Nevertheless, it is worth stating that depending on what the app implementing the DP^3T protocol asks the Users to do, and the legal effects that the notification produces have, the provisions of the GDPR on automated decision-making may be triggered. This would require either a basis in the law of the State deploying the system laying down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or another lawful basis stated in Art. 22(2) GDPR and the implementation of a process ensuring that individuals can obtain human intervention on the part of the controller, to express their point of view and to contest the decision.[27]

[24] EDPB Guidelines 04/2020, §§ 8 and 49.
[25] The risk of identification is analysed in details in Section II.3. pp. 15 ff. and Section V. pp. 33 ff.
[26] See below Section I.10. p. 12.
[27] Art. 22(3) GDPR.

Potential risks to the Users' privacy are analysed below in Section V. pp. 33 ff.

7. Stakeholders – Who Is Involved in the Project?

1. Project Owner | Consortium

The development and design of DP^3T are being carried out by an international consortium of technologists, legal experts, engineers and epidemiologists with a wide range of experience (the "**Consortium**"). The Consortium is led from EPFL in Switzerland by Prof. Carmela Troncoso, a leading expert in privacy, and has called upon experts from various countries including Belgium, Germany, Italy, the Netherlands, Switzerland and the United Kingdom.

The Consortium consists of people with a wide range of experience including:

- Prof. Edouard Bugnion: Co-Founder of VMWare, Former Vice President at Cisco
- Prof. Srdjan Capkun: ERC Awardee, Fellow of the ACM, Director of the Zurich Information and Privacy Centre
- Prof. James Larus: Former Director of Research and Strategy for Microsoft eXtreme Computing Group
- Prof. Kenny Paterson: Fellow of the International Association of Cryptologic Research, Former Manager at Hewlett-Packard Laboratories Europe
- Prof. Mathias Payer: ERC Awardee
- Prof. Bart Preneel: Former President of the International Association of Cryptologic Research, Fellow of the International Association of Cryptologic Research.
- Prof. Nigel Smart: ERC Awardee, Former Vice President of the International Association of Cryptologic Research, Fellow of the International Association of Cryptologic Research, Co-Founder of UnBound Tech.

Other persons involved in the project include:

- EPFL: Prof. Carmela Troncoso, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel
- ETHZ: Prof. David Basin, Dr. Jan Beutel, Dennis Jackson
- KU Leuven: Dr. Dave Singelee, Dr. Aysajan Abidin
- TU Delft: Prof. Seda Gürses
- University College London: Dr. Michael Veale
- CISPA: Prof. Cas Cremers
- University of Oxford: Dr. Reuben Binns
- University of Torino/ISI Foundation: Prof. Ciro Cattuto
- Eticas Foundation: Dr. Gemma Galdon Clavell

2. Users

The system is designed to be used by as many individuals as possible among the populations of countries affected by COVID-19.

3. Backend Server

The backend server is needed to ensure availability of the system and to enable people to use their own devices to trace contacts. The backend only hosts the information that is voluntarily transmitted by Users who have been diagnosed by healthcare professionals with COVID-19 and makes that information available. It does not store any privacy-sensitive information.

The role of backend will generally be assumed by national health authorities or other public bodies. From a data protection point of view, the backend will act as data controller of the data that is contained in the central server.[28]

It must be noted that the DP^3T is designed as a decentralised system; it therefore by design limits the control of the backend server on data processing activities that are carried out on the system. The backend server, and thus the government body responsible for it, has no control on the data that is stored on User phones. Its role as data controller is therefore limited.

In Switzerland the role of backend will be assumed by the Federal Office for Statistics ("**FOS**"), which will act as controller (*maître du fichier*; *Inhaber der Datensammlung*) of the information stored on the central server. The FOS will delegate the technical development, hosting and maintenance of the infrastructure necessary for the deployment and operation of DP^3T to the Swiss Federal Office of Information Technology and Telecommunication ("**FOITT**"). It is recommended that the role and responsibilities of each federal authority be clarified in an ordinance of the Federal Council.[29]

4. Authorisation Server

The authorisation server hosts the cryptographic keys that are used to verify that only Users who have been diagnosed positive to COVID-19 by a recognised healthcare professional can upload their data to the backend server. The implementation of the authorisation process (for instance by means of a QR code or otherwise), and the authorisation server on which it runs, are country-specific and outside of the DP^3T protocol.[30]

In Switzerland, responsibility for the authorisation server will be assumed by the Federal Office of Public Health ("**FOPH**"), which will delegate its operation to the FOITT.

5. The Steering Committee

In each country (or region) where it is deployed, the governance of the contact tracing system should be entrusted to a steering committee composed of scientists, government representatives and other stakeholders (Steering Committee).

The role of the Steering Committee will be defined on a country-basis, but its tasks should at a minimum include[31]: (i) progressively validating the effectiveness of the system from a public health point of view, based on a pre-agreed evaluation protocol and (ii) auditing, controlling and if necessary adapting the correctness of the algorithm used to measure the risk of infection.

6. Operating System Providers | Apple and Google

Apple and Google run the operating system on which the User App will run (as it is the case for all apps installed on smartphones). In this capacity, they will only provide a push notification service, the same as for any app and will be aware that the User App has been installed.

---

[28] The EDPB considers that the national health authorities could be the controllers (see EDPB Guidelines 04/2020, § 25).
[29] In accordance with Art. 16 para**.** 2 of the Swiss Federal Data Protection Act (FDPA; RS 235.1).
[30] They fall outside the scope of this report (see Section I.10. p. 12).
[31] In accordance with the requirements GEN-4 and FUNC-3 set out in EDPB Guidelines 04/2020.

It must be noted that the final specifications of the application programming interfaces (APIs) that will be made available by Apple and Google – and of the changes that will be introduced to their respective operating systems – to power contact tracing systems such as DP^3T, are not yet known (as of the date of this report). Accordingly, the exact role assumed by Apple and Google will have to be reassessed once this information is available.[32]

7. Healthcare professionals

Hospitals and other healthcare providers help ensure that the DP^3T system is accurate. They provide to their patients that are tested positive to COVID-19 the authorisation code that is required for the Users who opt to send their EphIDs to the central server.

Healthcare professionals do not access any information about Users that is generated by the DP^3T system.

8. Other Stakeholders

Other stakeholders will vary, depending on the manner the system is deployed in each country or region, but may include:

- **network and access providers**: they provide the infrastructure through which information is sent to and from the backend server and Users' devices. The information in transit is encrypted using TLS protocol; therefore, its content cannot be viewed by such providers.
- **User App Editor**: the editor of the User App can be the controller or another entity, depending on the choices made by the government in each country/region. The editor of the User App will know how many downloads occur on a daily basis but has no access to the content of the User App.

8. Need for a Data Protection Impact Assessment?

The DP-3T system is designed for national (or regional) deployments, but its protocol is scalable internationally. The requirement for a data protection impact assessment ("**DPIA**") will therefore have to be analysed on a country-by-country (or regional) basis.

DP^3T is currently intended to be deployed in Switzerland. Pursuant to the Swiss Federal Data Protection Act ("**FDPA**")[33], there is no mandatory obligation to carry out a DPIA. This DPIA is therefore carried out on a voluntary basis, following best practices.

In case of deployment in countries that are subject to the GDPR, the need of a DPIA must be assessed in accordance with Articles 35 and 36 GDPR, which require that a DPIA be carried out before the implementation in case the processing is likely to result in a high risk to the rights and freedoms of natural persons. In its Guidelines 04/2020, the EDPB concluded that a DPIA must be carried out prior to deployment of a contact tracing system, "*as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution)*"[34]. The EDPB further recommends the publication of the DPIA.

Furthermore, we note that the Consortium is working on a protocol to allow "roaming" and cross-border notifications, but only for people that cross borders. In this case, it is possible that the GDPR will apply to the processing of activities carried out outside of the Swiss border, based on

[32] See below Section IV.19 p. 29f for further information on data processed by operating systems.
[33] RS 235.1
[34] EDPB Guidelines 04/2020, § 39.

Article 3(2)(b) GDPR (monitoring of the behaviour of individuals that takes place within the European Union).

9. Previous Data Protection Impact Assessments or Other Form of Personal Data Compliance Assessment Made On This Project?

There has been no previous data protection impact assessment made in relation to the DP^3T project.

However, the DP^3T project has been evaluated on several occasions by the Swiss Federal Data Protection and Information Commissioner (*Préposé fédéral à la protection des données et la transparence*; *Eidgenössischer Datenschutz- und Öffebtlichkeitsbeauftragter*) ("**FDPIC**").

After its evaluation of the second version of the DP^3T project, the FDPIC noted in its public release dated 17.04.2020[35] that:

- DP^3T presents improvement from the point of view of data protection compared to the previous version of the project reviewed by it, in particular due to the decentralised approach adopted by DP^3T.
- it is positive from a data protection point of view that the central server, in accordance with the principle of data minimisation, only receives anonymous keys from users infected by COVID-19 that cannot be traced back to the identity of the persons concerned.
- the user is only informed locally, via the application stored in his phone, that he was in the vicinity of an infected (and anonymous) user.
- from the point of view of the protection of privacy and in view, the FDPIC generally advocates a decentralised approach in the context of the DP^3T project.

In an additional public release dated 21.04.2020, the FDPIC noted that it was currently analysing the data protection aspects of DP^3T and that it generally required to be demonstrated that an appropriate statutory basis pursuant to Art. 17 FDPA existed.[36]

The UK's Information Commissioner's Office also expressed its opinion that the DP^3T system is **"***aligned with the principles of data protection by design and by default, including design principles around data minimisation and security***"**.[37]

Furthermore, the Consortium has published several documents reviewing privacy and security aspects of the DP^3T system, including:

- an overview of data protection and security elements;[38] and
- a detailed privacy and security risk evaluation.[39]

35 https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news.html#-2047719826.
36 https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news.html#-1228430769.
37 Information Commissioner's Office (17.04.2020) Opinion on *Apple and Google joint initiative on COVID-19 contact tracing technology*, page 14. (note this opinion states that, because of their similarity, 'a number of the points included in this Opinion regarding the CTF are equally applicable to the DP-3T protocol').
38 https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf
39 https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf

10. Scope of This Data Protection Impact Assessment Report

Protocol

As further described in the white paper, the DP^3T system can technically be implemented in a privacy-preserving manner using two different protocols:

- one is an extremely lightweight system at the cost of limited tracing of COVID-19 positive patients under very specific conditions ("low bandwidth protocol"); and
- the other design is a variant of the first one and provides extra privacy properties at a small increase in bandwidth ("unlinkable decentralised proximity tracing protocol").

This report analyses the data protection impact of the first of these two designs only (low bandwidth protocol design). It must be noted, however, that the second design is a variant of the low bandwidth protocol design and that the content of this report will often apply equally to the second design. The main difference is that the second design does not require disseminating a public list of the keys corresponding to COVID-19 positive individuals. Instead, the ephemeral identifiers of infectious individuals are hashed and stored in a Cuckoo filter, which is then distributed to users of the system.

Country-specific functionalities

Secondly, DP^3T is a system that is scalable on an international level. This report covers the system generally and does not cover its specific implementation in each country. Accordingly, processes and applications that are designed to be country-specific are outside of the scope of this report.

As an example, the backend server, which is part of the DP^3T protocol, is designed to only accept data from Users who have received an authorisation from a healthcare professional. However, how this authorisation will be granted and how the authorisation server will host the authentication keys are country-specific and therefore outside the scope of this report.

Unretained features

As further described in the white paper, the DP^3T system has initially been designed to also enable users to voluntarily share data with epidemiologists. The purpose is to help epidemiologists (and health authorities) better understand how COVID-19 spreads, thus providing the basis to adopt policies better suited to prevent further infections.

This purpose for the processing of personal data with the DP^3T system is not covered by the analysis we have carried out. The reason for this is that the stakeholders of the project decided not to enable this functionality in the current version of the system.

If the implementation of the additional purpose is considered at a later stage, a data protection impact analysis pertaining to this functionality should be considered.

Current Version and Knowledge

Finally, DP^3T is a fast-evolving system which is being implemented during a period when knowledge is evolving at a quick pace (particularly regarding the scientific understanding of COVID-19).

This report covers the system in its current form and is based on the knowledge available at the date of writing of this report.

II. THE DATA INVOLVED

1. Introduction

The DP^3T contact tracing system has been designed to minimise data collection and processing.

The only information that a contact tracing system needs to provide is whether a user might have been exposed to the virus through close-range physical contact. The system does not need to reveal to anyone **who** the potential contagious contact was with, or **when** and **where** it happened.

Accordingly, the DP^3T system relies on the collection and sharing of ephemeral identifiers that cannot be directly linked to any individual. It is considered that under normal operation, none of the data that leaves a User's device must be characterised as personal data, as no actor has the ability to re-identify it with means reasonably likely to be used.

However, reidentification of individual users cannot be entirely excluded and is inherent to any proximity tracing system. The simplest example is the User that never leaves her home, except once in a month to buy groceries in a shop which is empty except for the owner. If this User meets no other person in her way to and from the shop, and is notified by the system that she was in close proximity to an infected person, she will know that this person was the shop owner.[40]

Apart from the risk – unlikely in most cases – of re-identification, there are additional ethical, non-data protection-related, reasons to treat the entire pipeline of information shared in the system with the same obligations that would apply if personal data was being processed, and to seek informed consent at every relevant point even when a different legal basis (e.g. the law or task in the public interest) may be appropriate to rely on.

In particular, the effectiveness of the system relies on its large adoption by the population, which can only be achieved if trust is built and maintained.

2. Data being collected

Secret Key (SK)

Upon installation, the User App generates a secret key (SK), that is stored on the User's device.[41]

The SK in only shared in case a User is diagnosed with COVID-19 and opts in to notify the backend (in which case the User's SK is sent to the backend server via an encrypted TLS connection and stored).

Ephemeral Identifiers (EphIDs)

Devices with the User App installed broadcast ephemeral identifiers (**EphIDs**) via Bluetooth. EphIDs are generated pseudo-randomly by the device, derived from the secret key (SK) of the phone.

Each User App locally stores on the device of the User the EphIDs that it broadcasts, together with coarse timestamps.[42]

In addition, the User App receives the EphIDs that are being broadcast by nearby devices and locally stores a record of each received EphIDs with the following information:

---

[40] This risk of re-identification is described in details in Section V pp. 33 ff.
[41] The secret key (SK) is then regularly renewed, in principle once every 14 days (exact duration will be defined on country-by-country basis).
[42] The duration of timestamps may be adapted. Recommended precision is at least 6h.

- received EphID;
- corresponding proximity, duration, and approximate time window (morning/afternoon/night and the date)[43]

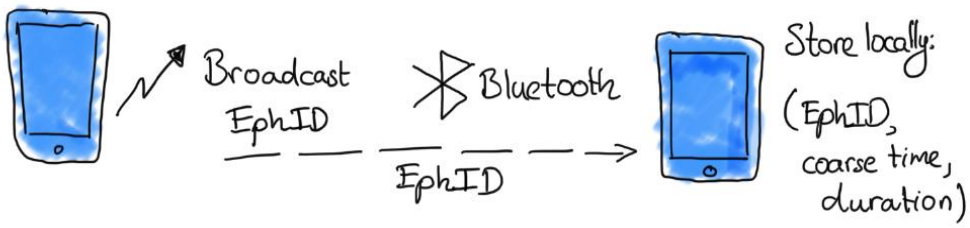

Figure AA: Processing and storing of observed `EphIDs`.

These records are stored locally on the Users' device and are never sent anywhere.

EphIDs are information relating to individuals. These individuals cannot be *directly* identified by EphIDs. Determining whether EphIDs must be characterised as personal data depends primarily on the possibilities of indirectly identifying the individuals concerned, e.g. by singling them out. This aspect is addressed below in Section II.3.

Irrespective of their characterisation or not as personal data, the storing and collection of EphIDs (which are Bluetooth emitted data stored on devices) possibly triggers the application of either (i) Article 5(3) of the ePrivacy Directive; (ii) Article 45(c) of the Swiss Telecommunication Act (**TCA**), and/or (iii) additional national regulations, in each case depending on the respective territorial and material scope of these regulations.[44] The requirements of these regulations differ:

- ePrivacy Directive: the storing of information on the Users' device or gaining access to the information already stored is allowed only if (i) the User has given consent[45] or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the User (which is the contact tracing system). In the matter at hand, the storage and sharing of EphIDs are strictly required for the purpose of providing the server requested by the Users (which is to be informed).
- Swiss TCA: processing is permitted only: (i) for telecommunications services and charging purposes; or (ii) if users are informed about the processing and its purpose and are informed that they may refuse to allow processing. Again, the processing of EphIDs is required in the matter at hand for the services that are provided to users.
- Additional applicable national regulation**:** requirements must be assessed on a case-by-case basis.

Location Data

We refer here to location data as "*all data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment*

[43] These elements are country-specific and will have to be defined by the Steering Committee in a manner that at least guarantees the effectiveness of the system, while limiting to the fullest extent possible the risk of identification and of physical tracking of individuals.

[44] Depending on their respective territorial and material scope.

[45] The notion of consent in the ePrivacy Directive remains the notion of consent in the GDPR and must meet all the requirements of consent as provided by art. 4(11) and 7 GDPR (see EDPB Guidelines 04/2020, § 11, footnote 6).

of a user of a publicly available electronic communications service (as defined in the e-Privacy Directive), as well as data from potential other sources, relating to:

- the latitude, longitude or altitude of the terminal equipment;
- the direction of travel of the user; or
- the time the location information was recorded."[46]

The DP^3T system does not collect location data (for instance GPS data or mobile phone metadata), but only the contact information of other Users (in the form of pseudo-random EphIDs). Furthermore, it is not possible to associate location of past events as all matches are made locally on the User's device and no location data (e.g. GPS) is used.

Traffic data about the Upload

(Infected) Users who upload their IDs with the authorisation code do so via a specific web service whose origin indicates location at the time of upload, and from an IP-connected device.

This information is generally considered as personal data and could potentially be considered as location data.

However, this information is not stored by the backend server, nor used.

Furthermore, the upload does not include the push-notification identifier.

Information relating to children

Use of DP^3T is not restricted to persons of a specific age. The minimum age to use the User App, and the process for authorisation by parents/legal guardians is country-specific and will have to be defined in the User App documentation/protocol, in accordance with applicable data protection laws (e.g. Art. 8 GDPR).

3. Personal data

In General

This section analyses in more detail whether the information that is processed through the DP^3T system, and in particular EphIDs, must be characterised as personal data.

"*Personal data*" are defined information relating to an identified or identifiable person.[47] In relation to individuals, this notion is generally considered to have the same meaning under Swiss law and European law.

Recital 26 of the GDPR specifies that "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

In the context of digital contact tracing, the EDPB stated that such reasonability test "must take into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the

[46] EDPB Guidelines 04/2020, p. 13.
[47] See Art. 3(a) FDPA and Art. 4(1) GDPR.

GDPR. The EDPB further stated that "Evaluating the robustness of anonymisation relies on three criteria: (i) singling-out (isolating an individual in a larger group based on the data); (ii) linkability (linking together two records concerning the same individual); and (iii) inference (deducing, with significant probability, unknown information about an individual)."[48]

In Breyer (C-582/14, § 43) the CJEU set out that the wording of the law "suggests that, for information to be treated as 'personal data' […], it is not required that all the information enabling the identification of the data subject must be in the hands of one person." In that case, the CJEU further noted that the test of means reasonably likely to be used to identify a natural person would however not be met "if the identification of the data subject was prohibited by law".

In the matter at hand, it must therefore be considered whether the information processed through the system – and in particular the EphIDs that are collected and stored – are personal data, thus determining if such information can be considered as relating to an identified or identifiable person, taking into account all lawful means reasonably likely to be used. In order to assess whether this is the case, one must differentiate between the various stakeholders of the system:

Data locally stored on the User's device

Each User App locally stores on the device of the User the EphIDs that it broadcasts, together with coarse timestamps, as well as the secret key (SK) generated. This information relates to the User of the device, who can be identified (any person who access the device can determine that the data pertain to the user of that device).

The information about a User that is locally stored on the User's device must therefore be considered as personal data.

Data stored by the backend server

The backend server can only access the information of Users tested positive to COVID-19 (and with the consent of such Users). The backend server only accesses a compact representation of the EphIDs that the Users have broadcast during the infectious window.[49] This information does not permit to identify the individuals to which the information relates.

The backend server will know that a person has been tested positive to COVID-19, but cannot know the identity of this person. No contact information is made available.[50] The backend server cannot, even by aggregating the information made available by several Users who uploaded their information, know that Users have been co-located, or whether they have been in contact with a limited or a large number of people.

The only possibility for the backend server to identify the Users that upload their information would require the backend server to store and process the traffic data about the upload. Processing this information is contrary to the DP^3T system and would contravene data protection laws, since this processing activity is not necessary to achieve the purpose of the system. In the national deployment of the system, technical and legal actions can be undertaken to ensure that the backend server cannot access and process this information.[51]

As a result, although the information stored on the backend server will relate to individuals, the DP^3T system can be implemented in a manner ensuring that the operator of the server cannot identify (directly or indirectly) such individuals, taking into account all lawful means available to the controller

[48] EDPB Guidelines 04/2020, §§ 16-17.
[49] Alternatively, the system may also be implemented so that the backend server only receives the authorisation code and its secret key (SK) of Users tested positive to COVID-19. This has no impact on the analysis.
[50] See Section VI.1, pp. 33 ff.: risk PR6 describes the information that the backend server may infer by aggregating the data of several Users.
[51] These actions are described in Section VI.2, pp. 38 ff. in relation to risk PR6.

or others. Therefore, it must be considered, in line with the principles laid down above, and the test set out in Breyer (C-582/14, § 43), that the information stored on the backend server cannot be characterised as personal data from the point of view of the operator of the backend server.[52]

It must be noted that no computation is carried out on the backend server. The backend server transmits information about new COVID-19 positive EphIDs to Users' devices, which then compute infection risk locally, on the Users' device. This comes with the important benefit that the server cannot learn the social graph of infected Users, which is data that could easily be repurposed and misused in ways that individuals would not reasonably expect and may not wish.[53]

Data stored locally about other Users

Each User App stores locally the EphIDs that are broadcast by nearby devices, together with the corresponding proximity, duration, and approximate time window. In addition, the User App will upload information from the backend server about the EphIDs of COVID-19 positive Users and locally compute the risk of infection.

This information is pseudonymised and cannot be attributed to a specific individual without the use of additional information. As long as a User does not voluntarily submit its data to the central server after having been tested positive to COVID-19, this information cannot be used to trace a specific individual.

The risk of identification of COVID-19 positive Users is analysed in detail in this report.[54] In a nutshell, it cannot be excluded that a User notified that she or he has been in close proximity with an individual tested positive to COVID-19 may identify that individual. For this reason, the information stored on other Users' devices must be characterised as personal data.[55]

More specifically, this information will relate to the individuals' health, and must therefore be considered as sensitive data within the meaning of Art. 9 GDPR and 3 FADP.

Conclusion

The system is designed to avoid identification of individual Users and uses technical solutions to ensure that all data is pseudonymised. Identification of individuals to which the data relates is in most cases impossible, but cannot be entirely excluded. For this purpose, taking the system as a whole, the information that is shared between Users through their use of the app must, at some points, be characterised as personal data.

It must be noted, however, that as long as the system is adequately deployed, the information that is stored by the backend will not be characterised as personal data from the point of view of the operator of the backend server.

---

52 Of a contrary opinion: BOCK/MÜHLOFFPOHLE, *Data Protection Impact Assessment for the Corona App*, Version 1.5 – 24.04.2020 (https://www.fiff.de/dsfa-corona), p. 65.

53 In its public release on the French "StopCovid" mobile application project (which is based on the "ROBERT"'s protocol), the French data protection supervisory authority (CNIL) considered that its analysis of the technical protocol of said app confirmed that the application will process personal data and will be subject to the GDPR. This is however a consequence of the design of the ROBERT's protocol – which contrary to DP^3T is centralised. In such a system, the central server can associate long-term identifiers with ephemeral Bluetooth identifiers. Therefore, from the point of view of the server, users are pseudonymous and not anonymous. This is not the case of DP^3T

54 See Section VI.1, pp. 33 ff.: risk PR2 "*Learning the identity of COVID-19 positive close contacts (identification)*".

55 It must be noted, however, that establishing an effective side database would likely require breaking the law by surveilling individuals without an effective lawful basis (e.g. illegitimately using covert cameras directed outward from the person, see Ryneš (C-212/13)), which would be contrary to the re-identification test set out by the CJEU in Breyer (C-582/14). Therefore, identification of individuals on a large-scale basis cannot be considered as likely.

As stated above, independently from the characterisation of the information shared in the system as personal data or not, there are additional ethical, non-data protection-related, reasons to treat the entire pipeline of information with the same obligations that would apply if personal data was being processed.[56]

[56] See above Section II. 1 p. 13

III. CONSULTATION PROCESS

Public Debate

The deployment and use of a tracking system for the purpose of combatting the COVID-19 epidemic has been the subject of a large public debate, in Switzerland and abroad.

On 21.04.2020, the European Data Protection Board issued its Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.[57] Additionally, several data protection supervisory authorities issued statements or publicly commented on the deployment of contact tracing systems. In addition to the public releases of the FDIPC referenced above,[58] the following communications to reference a few:

- The UK Information Commissioner's Office (ICO) released on 17.04.2020 an Opinion on the combatting of COVID-19 through data and another Opinion on Apple and Google joint initiative on COVID-19 contact tracing technology (which also refers to the DP^3T system);
- Marie-Laure Denis, head of the French Commission nationale de l'informatique et des libertés (CNIL), publicly debated the risks and merits of contact tracing system in a hearing of the French National Assembly. Additional, the CNIL published on its website a public release on the French "StopCovid" mobile application project.

According to a survey carried out by the consulting firm Deloitte of 1,500 people aged 16 to 64 living in Switzerland, the Swiss population is generally in favour of tracing the chains of infection of the COVID-19 via the movement data revealed by smartphones (with 64% of those polled being either in favour or rather in favour of the system, and of the remaining 36% of sceptics, only a small minority of 14% categorically rejecting the solution, even if anonymous).[59]

Open Source

The DP^3T project is open-source. Everyone may freely access and audit the source code and documentation of the system on the project's GitHub webpage.[60] This complies with the 3rd general requirement set out by the EDPB in its EDPB Guidelines 04/2020 (GEN-3, p. 14).

57 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf
58 Section I.9. p. 11.
59 https://www.rts.ch/info/suisse/11270302-les-suisses-prets-a-sacrifier-leur-localisation-pour-eviter-le-covid19.html; https://www2.deloitte.com/ch/en/pages/press-releases/articles/switzerland-supports-tracking-infection-chains-via-smartphone.html.
60 https://github.com/DP-3T

IV. ASSESSMENT

	Question	Response	Assessment & Possible Required Action (acceptable / non-acceptable / acceptable subject to corrective measures)
Purposes	1. What are the purposes of the project? Are they clearly identified and defined purposes?	**Yes.** As stated above (see Section I.5. p. 6.), the DP^3T system aims at preventing the spread of the COVID-19. The purpose of the system is to inform contacts of a COVID-19 positive person that they may have been exposed through close-range physical proximity with an infected person.[61]	Acceptable
	2. Does the project involve the use of existing personal data for new purposes?	**No.** DP^3T avoids relying on data collected by existing commercial or public infrastructures that were not set up for the goal of proximity tracing (for instance triangulation between cell phone towers, data provided by operators, or GPS locations).	Acceptable
	3. Are potential new purposes likely to be identified as the scope of the project expands?	**No.** DP^3T is designed to minimise the risks of data use for new purposes.	Acceptable

[61] See above Section I.10. p. 12 for information about the functionalities of the system that are out of scope of this report.

Legal compliance – is it fair and lawful?	4. Legal basis for processing the information	Legal basis for processing the information will have to be defined on a country-by-country basis. In Switzerland, as recommended by the EDPB, access and use of the DP^3T system will occur on a **voluntary basis**. The voluntary basis implies in particular that individuals who decide not to or cannot use the system must not suffer from any disadvantage at all (which include not benefitting from advantages offered to Users).[62] The mere use of contact-tracing applications on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When EU public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it is possible that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR. As regards Swiss Federal authorities, they may process personal data if there is a statutory basis for doing so (Art. 17 FADP). In its Guidelines 04/2020, the EDPB recommended in that respect that: - "*The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application.* - *A clear specification of purpose and explicit limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved. The categories of data as well as the entities to (and purposes for which, the personal data may be disclosed) should also be identified. Depending on the level of*	**Acceptable subject to corrective measures:** - Each implementing country must determine if appropriate statutory basis is in place or if another lawful basis[67] is applicable - It is further recommended to ensure in law and in fact that Users have to disclose neither the status of the app nor the mere existence on a device to third parties. - Access controls for public and private buildings, etc. based on disclosing the app status should be prevented.

[62] See EDPB Guidelines 04/2020, § 24.

[67] In Switzerland, Art. 59 of the Federal Act on Epidemics generally authorises public authorities to process personal data (including health data) for the purpose of identification of infected persons for the purpose of combatting epidemics. An ordinance of the Federal Council is recommended to clarify the scope and content of the processing activities. See also ABBEG/KNECH, Contact Tracing App. Kann eine mögliche Nutzungspflicht Freiheiten schaffen? in www.jusletter.ch, 24 April 2020.

		interference, additional safeguards should be incorporated, considering the nature, scope and purposes of the processing. - […] *as soon as practicable, the criteria to determine when the application shall be dismantled and which entity shall be responsible and accountable for making that determination*."[63] If the data processing of personal data is based on another legal basis, such as consent (Art. 6(1)(a) GDPR) for example, the controller will have to ensure that the strict requirements for such a legal basis to be valid are met. It must be noted, however, that the DP^3T system is designed to prevent the backend server, which will often be a public body[64], from accessing any personal data. As long as the data that is stored on the, or accessed by, the backend server cannot be characterised as personal data, the requirements laid down in the GDPR or the FDAP do not apply. Regarding the lawfulness of the processing, as indicated above, the DP^3T system involves storage and/or access to Bluetooth information (in the form of EphIDs) from the Users' devices, which (independently from any processing of personal data) requires a lawful basis.[65] Additionally, depending on the nature of the prescribed intervention when a risk notification is provided, in particular whether it is significant or whether it brings a legal effect, the DP^3T system may be considered a decision within the meaning of Art. 22 GDPR. This requires a lawful basis under that Article to be established for such a decision, and the implementation of safeguards in line with Art. 22 and national law.[66]	

63 See EDPB Guidelines 04/2020, § 31
64 In Switzerland, it is assumed that this role will be assumed by federal authorities (being FOT, in collaboration with FOPH and FOITT).
65 See above Section II.2.
66 See also above Section I.6. p.7.

	5. If the processing activities rely on consent, how will consent be obtained and recorded, what information will be provided to support the consent process? How can consent be withheld or later withdrawn?	In general: The use of the User App will be optional for individuals. Individuals who want to participate in the DP^3T system and will have to download the User App and confirm their consent upon its installation. Users can at any time delete their User App (or simply stop using it), in which case no more data will be generated. In case of infection: Furthermore, a User will have no obligation to notify the backend (thus to other Users) that she has been tested positive to COVID-19. Users can thus participate in the system "passively" (i.e. solely to be informed if they encounter an infected person, without disclosing to other Users if they themselves have tested positive for COVID-19).	**Acceptable subject to corrective measures:** - See recommendations in Section II.4. p. 21 above.
	6. Transparency and fairness of processing activities	The processing must be carried out in a way that is comprehensible to the data subject. The code of the DP^3T and its documentation is public and can be freely accessed and audited by anyone. The Consortium further published an explanatory comic in many languages in order to help individuals understand how the system works and which data will be processed. Nevertheless, the onus of providing sufficient and adequate information to individuals mainly rest on the entity that will act as controller in each implementing country. This information must be provided in a precise, transparent, comprehensible and easily accessible form in clear and simple language (Art. 12 para. 1 sentence 1 GDPR). More specifically, this includes information about the purposes of the processing, the measures used for those purposes, in particular the duration of the storage of personal data, data transmissions and their recipients, and how data subjects can effectively	**Acceptable subject to corrective measures:** - In each implementing country/region, the controller must be clearly defined. - Other stakeholders must also be referenced. - In each implementing country/region, the controller will be responsible for providing

		exercise their rights as data subjects vis-à-vis the controller, including through recourse to the competent data protection supervisory authority. This information must be provided in the User App privacy statement, but also through any other appropriate way. In order to ensure their fairness, accountability and, more broadly, their compliance with the law, algorithms must be auditable and should be regularly reviewed by independent experts.	all required Information to individuals. - Information must also be provided on the risks associated with the system, including that it might not work as anticipated, or that identification of infected users cannot be excluded. - A Steering Committee must be entrusted with the control and adaptation of algorithms on which the system relies.
Adequacy	7. Is the information processed/processing activities adequate to achieve the intended purposes?	**Yes.** The processing activities are adequate to achieving the purpose of contact tracing. It must be noted, however, that the usefulness of contact tracing systems, such as DP^3T, to limit the spread of COVID-19 will depend on the adoption of the system within a population and is currently debated. In a nutshell, the following factors could limit the adoption of the system: - participation is on a voluntary basis only; - not everyone has a smartphone or knows how to download or set up an application, in particular elderly people. It must be noted that any form of contact tracing is by itself not sufficient to tackle the spread of COVID-19 and that the system is designed as a complementary tool to traditional contact tracing techniques (notably interviews with COVID-19 positive persons) and other public health	**Acceptable**

		measures. Therefore, the use of DP^3T may only be adequate to achieve that purpose if it is used in combination with other measures (e.g. within a strategy based on testing, isolation, contact tracing, and quarantine (TICQ)), in addition to "traditional" measures (hygiene, social distancing and healthcare).	
	8. Is there alternative (less invasive means) of achieving the same purposes?	**No.** Contact tracing is normally done through interviews. But interviews alone provide an insufficient solution to limit the spread of COVID-19[68] and may be more intrusive than a privacy-preserving protocol like DP3T. Other forms of contact tracing using currently available technology are more invasive and present higher risks to privacy than the technology underpinning DP^3T.[69] As indicated above, the use of DP^3T is part of a global strategy to combat the COVD-19 epidemic, composed of several measures, none of which being an alternative to DP^3T.	**Acceptable**
	9. Which personal data could you not use without compromising the needs of the project (data minimisation)?	**None.** DP^3T has been designed to minimise data collection and processing:	**Acceptable**

[68] See Salathé/Cattoto, COVID-19 Response: What Data Is Necessary For Digital Proximity Tracing? (https://github.com/DP-3T/documents/blob/master/COVID19%20Response%20-%20What%20Data%20Is%20Necessary%20For%20Digital%20Proximity%20Tracing.pdf), p. 1f: "*Interviews can be problematic because i) they are slow, ii) they are difficult to scale because of resource requirements (e.g., required human effort), and iii) a "contact" in the case of a respiratory disease may be anyone who has been in close-range physical proximity (i.e. 2 metres) for some time (i.e. a few minutes). This can of course include strangers which one would never be able to recall in a traditional interview*."

[69] Scientists are currently considering fully decentralised architecture, which would not require any backend server. This technology is, however, not currently available (see Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V.: Data Protection Impact Assessment for the Corona App, Version 1.5 – 24.04.2020 (https://www.fiff.de/dsfa-corona), p. 6).

		- no entity, including the backend server, can track non-COVID-19 positive users based on broadcast ephemeral identifiers. - no entity beyond a user's device processes or stores any identifiable personal data about the user. It must be noted, however, that the alternative technical design of DP^3T ("unlinkable decentralised proximity tracing protocol") could potentially reduce the amount of data that are required for contact tracing. This is for instance the case of the variant design of DP^3T. Such alternative design would have increased the bandwidth required by the User App and has not been retained for deployment.[70]	
	10. How is function creep prevented?	As stated above, DP^3T is a decentralised system. This design mitigates the risk that the generation of identifiers and generation of contact graphs are misused by a central authority or contractor (e.g. a governmental entity or private company). In particular, in DP^3T, identifiers are not created by the backend but by the User App directly. Therefore, the backend cannot, at any point, link the past and future ephemeral identities of any user, infected or not, by decrypting back to their permanent identifier.[71] Furthermore, the system will organically dismantle itself after the end of the epidemic: infected patients will stop uploading their data to the central server, and people will stop using the User App.	**Acceptable**
Accurate and up to date	11. Are you able to amend information when necessary to ensure it is up to date?	No. There is no manual entry and therefore updates. Information about infected secret keys (SK) are removed at the end of the	**Acceptable**

[70] See above Section I.10. p. 10.
[71] This is different in PEPP-PT (see above Section I.2. pp 2 ff.).

		infectious window. Implementing a manual way to amend data is not necessary and could have detrimental effects (loss of integrity)	
	12. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	The system ensures that only data about COVID-19 positive persons are uploaded to the backend server by requiring an authorisation code that need to be provided by accredited healthcare providers.	**Acceptable**
Retention	13. What are the retention periods for the personal information and how will this be implemented?	Data which is stored on the backend server is automatically removed after 14 days. Data which is stored on each User's device is also automatically removed after 14 days.	**Acceptable**
	14. Are there any exceptional circumstances for retaining certain data for longer than the normal period?	**No.**	**Acceptable**
	15. How will information be fully anonymised or destroyed after it is no longer necessary?	Information (which can generally be considered as anonymous in the first place) are automatically erased by the system after 14 days.	**Acceptable**
Rights of the individual	16. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held? Or to delete it, rectify it or block it?	The DP^3T system has been designed so that only a User's device processes or stores any identifiable personal data about that User. No entities are involved in the processing of any identifiable User personal data. Accordingly, the DP^3T system is neutral from the point of view of individuals: in the absence of personal data being stored on the backend server or the device of other Users, individuals' rights pursuant to data protection laws are not restricted (nor are they enabled).	**Acceptable subject to corrective measures:** - In each implementing country/region, the controller of the project must inform the individuals about their rights and ensure that

		Users who want to stop participating in the system may at any time stop using their User App or delete it. All data are erased at the end of the retention period (14 days). It must be noted that due to the decentralised design of DP^3T, the backend server only has a limited control on the data. In particular, it cannot (i) identify the individuals to which the data stored on the backend server relates (thus cannot carry out requests for deletion) or (ii) access (nor delete) the data that is stored on the Users' devices. Providing the backend server with additional control over the data processed via the system would ultimately be detrimental to the individuals.	individuals clearly understand them. - Furthermore, the governments implementing the system are encouraged to enact laws or regulations that define the rights of the individual in the context of COVID-19 contact tracing system.[72]
Appropriate technical and organisational measures	17. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?	This aspect is country-specific. All processes will be described in a protocol and documentation.	**Acceptable subject to corrective measures:** - The required documentation must be implemented.
	18. What security measures will be applied to ensure the confidentiality, integrity and availability of the information at rest and in transit?	The system is designed to comply with state-of-the-art cryptographic techniques and security measures.[73] All transmissions are TLS/SLL encrypted. The data at rest is only a series of cryptographic codes.	**Acceptable**

[72] See for instance: Liliane EDWARDS *et al.*, Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates" available at https://osf.io/preprints/lawarxiv/yc6xu/.

[73] For a detailed description of security measures, see DP^3T's white paper and the Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems.

External Communications and International Transfers	19. Will individuals' personal information be disclosed to third parties, if so to whom, how and why?	**Only to the extent required.** The DP^3T system has been designed so that only a User's device processes or stores any identifiable personal data about that User. No entities are involved in the processing of any identifiable User personal data. The decentralised approach of DP^3T notably minimises the amount of personal data collected by any one entity, and heavily reduces the possibility of accessibility of any information, providing the guarantee that the backend server learns nothing about identifiable individuals or their health status. This promotes trust in the system, as concerns around function creep and lack of purpose limitation (such as the repurposing of the protocol by law enforcement or intelligence services in countries in which it is deployed) can be solidly rebutted mathematically. This itself may lead to wider uptake. **Project Owner (Consortium)** The Consortium members will not access any User personal data. **Users** Information that is stored on each User's device is described in Section II.2., pp. 13 ff. **Backend server** The backend server only stores information of infected Users if they decide to share their status. The information that is stored is - the authorisation code and User secret key (SK), and - a compact representation of the EphIDs it has broadcast during the infectious window. Accordingly, the backend server, will only observe anonymous identifiers of infected people without any proximity information. The backend server stores	**Acceptable**

		this identifier to send information to the User App. The backend does not store any other information (PII or otherwise) with this notification identifier. The backend server only stores the notification identifier of the User App. This identifier is only used to send data to the User App. When the User App uploads its secret key (SK) after having a User has been diagnosed, it does not supply this identifier to the backend. It must be noted that no computation is carried out on the backend server. The backend server transmits information about new infected EphIDs to Users' devices, which then compute infection risk locally, on the Users' device. This comes with the important benefit that the server cannot learn the social graph of infected Users, which is data that could easily be repurposed and misused in ways that individuals would not reasonably expect and may not wish. **Operating System Providers (Apple and Google)** The User App needs to regularly receive information pertaining to newly infected Users from the backend server, so that it can locally determine whether its User has been in physical proximity of an infected patient. Because apps running in the background are not guaranteed to be able to download information, the User App needs to register for a push notification service: Firebase Cloud Messaging (FCM) on Android and Apple Push Notification Service (APN) on iOS. The User App sends the notification identifier to the backend server. The Operating System Providers (Apple and Google) learn that the User installed the User App and has registered for the push notification service, but cannot see any data. Nevertheless, since they provide the operating system running on mobile devices, one has to trust them, since they could potentially learn information	

		related to the proximity tracing system (who is infected, who infected whom, social graphs, etc.).[74] **Healthcare professionals:** Healthcare professionals are not provided with any personal data by the DP^3T system. Their role within the system is limited to providing the Users diagnosed with COVID-19 with the authorisation code required for Users to share their EphIDs with the backend server. Of course, as part of their day-to-day activities, they process health data about their patients. This is, however, outside of the DP^3T system **Others** See above Section I.7.8. pp. 10 ff.	
	20. What measures do you take to ensure processors comply?	The main controller of the system will need to assess the need to obtain a standard data processor agreement with the Operating System providers, as with any public sector app using push notifications. The system contemplated here is unlikely to pose additional risks to the rights and freedoms of data subjects, as data subjects with smartphones will already be using these systems every day.	**Acceptable subject to corrective measures** - The controller in each country deploying the system, needs to clarify whether a data processing agreement needs to be entered into with Apple and Google.

[74] This is not specific to DP^3T, nor to any contact tracing system, but is common to all mobile apps.

	21. Will personal data be transferred to a country outside of Switzerland or the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data?	Not applicable.[75]	**Acceptable**

[75] The Consortium is working on a protocol to allow “roaming” and cross-border notifications, which if implemented would require a further assessment of this aspect.

VI. PRIVACY ISSUES IDENTIFIED AND RISK ANALYSIS

VI.1. Part I – Identify the Privacy And Related Risks

Ref No.	Privacy issue – element of the initiative that gives rise to the risk	(a) Risk to individuals	(b) Compliance risk	(c) Associated organisation/ corporate risk
PR1	***Unlawful access to data (loss of confidentiality)*** *Description: attackers may for instance create a non-official copy of the User App to gather information about the Users. Attackers could also access to in-transit information or information at rest on the backend server.*	*Disclosure of personal information.*	*Non-compliance with security requirements.*	*Loss of trust in the system.*
PR2	***Learning the identity of COVID-19 positive close contacts (identification)***[76] *Description: This risk is a consequence of the basic proximity tracing functionality. It relies on the single bit of information that any proximity tracing system must reveal – whether Users have been in close proximity to an infected person:* - *First, if a User has been in contact with only one person and receives a notification that she has been in contact with a COVID-19 positive person, this User will know who the infected person is.* - *A tech-savvy adversary can re-identify EphIDs from COVID-19 positive people that they have been physically close to in the past by actively modifying the app and collecting extra*	*Data about health of the individuals are disclosed to third parties.*	*Unauthorised disclosure of personal data.*	*The system relies on the principle that no personal data will be processed. Through re-identification, all information*

[76] This risk is described in detail in Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems, pp. 5 to 6.

	information about identities through additional means, such as a surveillance camera to record and identify the individuals. The information learned via the app is, in many cases, already expected to be known to this adversary (e.g., family, friends, neighbours, who will directly inform their close relations and friends). - *Furthermore, a tech-savvy attacker may also create multiple accounts and use them for a short time only (e.g., 15 minutes). If a notification arrives, the attacker examines the corresponding account. Since this account was only used during a fixed time window, the attacker now knows that she was in close proximity to an infected person during that period.*			*becomes personal data, which undermine the system.*
PR3	***Users not being notified that they have been exposed*** *Description: Multiple reasons can cause Users not being notified that they have been at risk. First of all, infected persons may decide not to participate in the system (the system being used on a voluntary basis) or may not use or deactivate their User App. Additionally, an attacker could use a Bluetooth jammer to disrupt communication between Users and therefore so that the close proximity events cannot be established.*	*At-risk individuals will not be informed.*	*None.*	*Loss of trust in the system.*
PR4	***Users being falsely notified that they have been exposed*** *Description: a malicious adversary places her proximity tracing device in a crowded area and hooks up a sensitive antenna and/or powerful transmitter to artificially increase the range of her Bluetooth contacts. As a result, other devices located beyond 2 metres can interact with the attacker's device and will perceive the attacker's device as "nearby". To complete the attack, the attacker must ensure that these interactions between her device and other devices are flagged as at-risk events:* *1. Is herself COVID-19 positive and brings her device to the hospital when she gets tested (requiring the attacker to be COVID-19 positive).* *2. Pays a symptomatic person to bring the attacker's device to the hospital instead of their own (or simply obtains the upload authorisation code from them).* *3. Hijacks/bribes the health authority that authorises COVID-19 positive individuals to trigger contact tracing.*	*Individuals will falsely fear to be infected;* unnecessary imposition of isolation or quarantine	*None.*	*Creating panics.* *Loss of trust in the system.*

	4. Hijacks/bribes the system server that sends information or directly notifies users of the system. Most systems we consider here use a backend server to check authorisations by health authorities and to relay information to users. As a result, the attacker can also collude with or bribe the backend server to help generate fake contact events. *To cause false notifications, the attacker may also actively relay the Bluetooth signals of people that the attacker believes will soon be diagnosed with SARS-CoV-2. For example, the attacker could observe and relay Bluetooth signals from people at a testing centre.*			
PR5	**Revealing usage of the User App and tracking Users' devices** *Description: The design of DP^3T uses Bluetooth Low Energy for proximity detection. Enabling Bluetooth, and transmitting EphIDs will reveal to any observer that the individual has enabled the User App. Furthermore, use of the system and therefore enabling Bluetooth brings some fundamental risks which could permit tracking the User devices:* - *Enabling Bluetooth can make the device trackable if the OS does not implement MAC address randomisation and disables advertisements;* - *bad synchronisation between MAC addresses randomisation and Bluetooth identifiers makes a device trackable as long as the attacker stays within range.*	*An attacker can know if an Individual uses the system (and may discriminate those not using the app).*	*None.*	*Loss of trust in the system (fear of surveillance).*
PR6	***Backend server identifying COVID-19 positive Users*** *Description: Any proximity tracing system in which COVID-19 positive individuals upload data directly from their phone to a central server, reveals to a system administrator or the central server which individuals have tested positive through their associated network identifiers. This attack is generic in the sense that all systems that use direct upload functionality are vulnerable to it.*	*Disclosure of personal information, including health data.*	*Unauthorised disclosure of personal data.*	*All information on the backend server becomes personal data, which undermine the system.*
PR7	***Gathering of information about Users through local phone access***	*Disclosure of personal information.*	*Non-compliance with*	*Loss of trust in the system.*

	Description: A law-enforcement adversary (LEA) or local attacker (e.g., an abusive spouse) can obtain access to a victim's phone, either legally by a subpoena or through direct coercion. This poses the following risks: - *Reveal social interactions (number of people somebody was with);* - *Recompute the risk score given the recorded observation, possibly using different parameters;* - *enabling **location tracing** of the victim given other observations, or confirm the location of the victim in the past.* *The use of a "master key" from which a device's daily keys are derived (as in the v1.0 Google/Apple design) would allow law enforcement to link an individual's identifiers for the entire lifetime of the application.*		*security requirements.* *Breach of purpose limitation.*	
PR8	***Gathering of significant number of EphIDs through relay attack*** *Description: A shortcoming in most decentralised proximity tracing systems based on BT handshakes between devices is that a malicious party who is willing to modify their app or deploy their own software is able to record a proximity event despite only being in contact for a short amount of time or from a long distance. In particular, an attacker could attempt to gather a significant number of EphIDs by deploying specialist equipment, either in high-traffic locations or in a vehicle that can cover a wide area ("wardriving"). The attacker can also deploy high gain, directional antennas to cover wide areas, further increasing the range and selectivity of the attack. The attacker can later see which of the recorded EphIDs correspond to COVID-19 positive individuals. If the attacker can use additional information (such as location, timing, video surveillance, etc.) the identities of exposed users could be inferred*	*Gathering of information about individuals.*	*Breach of purpose limitation.*	*System being repurposed (e.g. used to find hotspots or infected users' trajectories).*
PR9	**Reuse of the data for new purposes / function creep / mass surveillance** *Description: The system and information gather through it are reused by a central authority or contractor (e.g. a governmental entity or private company) for other purposes than information to Users of the possibility of exposure to COVID-19, for instance for mass surveillance, compliance with isolation obligations, etc.*	*Use of their data for unanticipated purpose*	*Breach of purpose limitation principle*	*Loss of trust in the system.*

PR10	**DP^3T system and technology does not function as anticipated** *Description: DP^3T system does not function as anticipated and does not provide the anticipated outcomes. This can be caused by an adoption of the system by too low a percentage of the population or the underlying technology not functioning as anticipated (too many false positives or false negatives).*	*At-risk individuals will not be informed; Individuals will falsely fear to be infected*	*None.*	*Loss of trust in the system (fear of surveillance).*
PR11	**Freedom restrictions when not using the User App** *Description: Even if the use of the tracing app is voluntary, it is possible that non-use makes one subject to special restrictions on freedom of movement and contact, if for example, the apps is used as access barriers to public and private buildings, universities, schools, means of transport, administrations, police stations, etc.*	*Restriction of the freedom of individuals*	*Will depend on the actual scenario*	*Societal impact (discrimination of portion of the population, etc.).*

VI.2. Part II – Identify the privacy solutions

Ref No.	Risk – taken from column (a), (b) and/or (c) in table 1.	Risk score [77]		Proposed solution(s) /mitigating action(s)	Result: is the risk accepted, eliminated, or reduced?
		Likelihood	Seriousness		
PR1	***Unlawful access of data*** *Disclosure of personal information* *Non-compliance with security requirements* *Loss of trust in the system.*	2	2	*The controllers, in collaboration with the public authorities, have to clearly and explicitly inform about the link to download the official national User App in order to mitigate the risk that individuals use a third-party app.* *Information in-transit and at-rest is encrypted, this limiting the seriousness of any breach of confidentiality.*	*This risk can be sufficiently mitigated.* *Its impact potential seriousness remains relatively low, since the system is designed to avoid transmission of sensitive data/personal data to the backend server.*
PR2	***Learning the identity of infected close contacts (identification)*** *Unauthorised disclosure of health data*	3	2	*Any proximity tracing system that notifies users that they are at risk enables a motivated attacker to identify the COVID-19 positive persons to whom she has been physically near.* *Possible mitigation actions would require the creation of multiple accounts to be onerous, which would have detrimental impacts (fewer*	*This risk cannot be eliminated.* *The risk is, however, acceptable provided that Users are clearly informed (for instance immediately prior to sharing information that they have been infected) of the risk of reidentification.*

[77] Likelihood and impact (seriousness) are ranked from 1 to 4: 1=Insignificant; 2=limited; 3=important; 4=maximum).

	Data in the system become personal data			*persons using the system, thus limiting its effectiveness and accuracy).* *Individuals must, however, be clearly informed of this risk.*	*It must be noted that epidemiologists currently expect that a large proportion of the population will at some point be infected by the virus (e.g. 50-75%). The seriousness of the impact that third party may identify through the system Users who have been infected can therefore be considered as limited.*
PR3	**Users not being notified that they have been exposed** *At-risk individuals will not be informed.* *Loss of trust in the system.*	3	2	*This risk is needed to ensure that contact tracing apps are voluntary. Designing the system under the assumption that a part of the population will not participate enables the core principle of giving everyone the freedom to decide individually if they want to participate in tracing. The assumption that not everyone will participate, ensures that the app is effective in the presence of incomplete data (e.g., people without phones).* *Individuals must, however, be clearly informed of this risk.*	*This risk cannot be eliminated.* *The risk is, however, acceptable provided that Users are clearly informed (for instance when installing the User App) of the risk that the app.*
PR4	**Users being falsely notified that they have been exposed** uncessary imposition of isolation or quarantine; *creating panics.* *Loss of trust in the system.*	2	2	*Some of these attack vectors can be mitigated to a certain degree, as described in Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems, pp. 7-8.*	*This risk can be to some extent mitigated but not eliminated.* *The overall risk associated with it is relatively low.*

PR5	**Revealing usage of the User App and tracking Users' devices** *Attackers can know if an Individual uses the system (and may discriminate those not using the app)* *Loss of trust in the system (fear of surveillance).*	4	2	*The risk of revealing usage of the User App is common to all Bluetooth contact tracing systems and cannot be technically addressed. Government must ensure legally that an individual cannot be discriminated unlawfully for using or not using the app (for instance an employer that would want to impose use of the User App to its employees, despite the system being voluntary in that country).* *Risks relating to the tracking of User devices can be addressed in modern smartphone operating systems, respectively are expected to be solved by the Apple/Google API proposal.*	*The consequences associated with the risk of revealing usage of the contact tracing system can be appropriately mitigated by lawmakers on a country-by-country basis.* *Risks relating to the tracking of Users' device can be eliminated technically.*
PR6	***Backend server can identify infected Users*** *Unauthorised disclosure of personal data* *Data in the system become personal data*	1	2	*The (network) identities of COVID-19 positive Users can be hidden by a simple proxy that relays the uploads from phones to the central server. For example, each local hospital could serve as a proxy for data uploads to avoid traffic analysis attacks. This approach suffices as we must trust the hospital with the privacy of patients.* *Furthermore, it is recommended specifying in national regulations that the traffic and upload information cannot be stored and processed by the backend server.*	*The risk of the backend server identifying Users can be eliminated.*
PR7	***Gathering of information about Users through local phone access***	2	4	*This risk is already to some extent mitigated by the design of DP^3T which minimises data collection and storage.*	*This attack requires access to the device and the technical knowledge to extract data from it.*

	Disclosure of personal information *Breach of purpose limitation*			*In order to minimise the data that can be accessed, a master key must not be used. Furthermore, the data must by locally stored in an encrypted form.*	*In most cases, any attacker with these abilities would be able to access the same or more information from devices (e.g. a hacker having access to other apps; or law agency having access to cell tower data/metadata). Therefore, despite its gravity, the likelihood of the risk remains mitigated.*
PR8	***Gathering of significant number of EphIDs through relay attack*** *Gathering of information about individuals* *System being repurposed (e.g. used to find hotspots or infected users' trajectories)*	2	1	*The attack's effectiveness can be reduced by requiring the attacker to be in proximity for a longer time. Systems using passive broadcasts could, for example, use secret-sharing of identifiers so that the attacker must listen or broadcast for a few minutes to be able to conduct the attack. Systems using active connections could instead require a minimum connection duration.*	*This risk is common to all proximity tracing systems proposed to date and cannot be eliminated, but mitigated.* *Its potential harmful impact is however limited, since EphIDs by themselves cannot serve to identify individuals. The risk can therefore be considered as acceptable.*
PR9	**Reuse of the data for new purposes / function creep / mass surveillance** *Use of their data for unanticipated purpose* *Breach of purpose limitation principle* *Loss of trust in the system.*	1	4	*The DP-3T protocol and the Google and Apple API are specifically designed to not allow function creep (which is enforced in the OS of the smart devices).* *DP^3T's design mitigates the risk that the generation of identifiers and generation of contact graphs are misused by a central authority or contractor (e.g. a governmental entity or private company). The backend cannot, at any point, link the past and future EphIDs of any user, COVID-19 positive or not, by decrypting back to their permanent identifier.*	*This risk is adequately mitigated from a technical point of view by the design of the system.* *Each government deploying the system is encouraged to enact regulations or laws which clearly stipulate how the system will be deployed, in accordance with the requirements set out by the EDPB (see above Section IV.. pp. 21 ff.)*

				Furthermore, the system will organically dismantle itself after the end of the epidemic: COVID-19 positive patients will stop uploading their data to the central server, and people will stop using the User App.	
PR10	**DP^3T system and technology does not function as anticipated** *At-risk individuals will not be informed; Individuals will falsely fear to be infected* *Loss of trust in the system (fear of surveillance).*	2	2	*In each country, a Steering Committee should be put in place to audit the functioning of the system and make the adjustments that are required.*	*It must be noted that a contact tracing system such as DP^3T, and the technology underpinning it, have never been used in the past. The success of such a project cannot be guaranteed. The risk of the system not providing the anticipated outputs cannot be excluded.*
PR11	**Freedom restrictions when not using the User App** *Restriction of the freedom of individuals* *Societal impact (discrimination of portion of the population, etc.).*	3	3	*The likelihood of this risk will depend on who the system is deployed on a national level. In order to mitigate this risk, it is recommended to enact laws that forbid public and private discrimination of users based on the use or not of the User App.*	*Government can enact laws to ensure that this risk is eliminated.*

VII. ANNEX – REQUIREMENTS SET OUT BY THE EDPB

Introduction

The table below lists the requirements set out by the EDPB in the "analysis guide" attached to its Guidelines 04/2020 and describes for each of them, whether the DP^3T protocol complies with the requirements.

The compliance with the EDPB's requirements is assessed using the following scale and colour code:

1	=	DP^3T protocol fully complies with the requirement.
2	=	DP^3T protocol can comply with the requirement if implemented on a country-basis as recommended by the Consortium.
3	=	Compliance with the requirement is possible but requires an adaptation to the DP^3T protocol.
4	=	DP^3T protocol cannot comply with this requirement.

Analysis

Ref.	*Requirements*	Assess-ment	Comments
GEN-1	*The application must be a complementary tool to traditional contact tracing techniques (notably interviews with infected persons), i.e. be part of a wider public health program. It must be used only up until the point manual contact tracing techniques can manage alone the amount of new infections.*	2	The DP^3T protocol is intended to be implemented in each country/region as part of a wider program to combatting COVID-19 (and not as an alternative).

GEN-2	*At the latest when "return to normal" is decided by the competent public authorities, a procedure must be put in place to stop the collection of identifiers (global deactivation of the application, instructions to uninstall the application, automatic uninstallation, etc.) and to activate the deletion of all collected data from all databases (mobile applications and servers).*	1	The system will organically dismantle itself after the end of the epidemic. COVID-19 positive Users will stop uploading their data to the backend server, and people will stop using the app. All data is automatically removed after 14 days.
GEN-3	*The source code of the application and of its backend must be open, and the technical specifications must be made public, so that any concerned party can audit the code, and where relevant - contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data.*	1	The DP^3T project is open-source. The source code and documentation of the system on the project's GitHub webpage.[78]
GEN-4	*The stages of deployment of the application must make it possible to progressively validate its effectiveness from a public health point of view. An evaluation protocol, specifying indicators allowing to measure the effectiveness of the application, must be defined upstream for this purpose.*	2	A Steering Committee must be set up in each country/region for this purpose.
PUR-1	*The application must pursue the sole purpose of contact tracing so that people potentially exposed to the SARS-Cov-2 virus can be alerted and taken care of. It must not be used for another purpose.*	1	See Section I.5. above.
PUR-2	*The application must not be diverted from its primary use for the purpose of monitoring compliance with quarantine or confinement measures and/or social distancing.*	1	DP^3T cannot be used for this purpose.
PUR-3	*The application must not be used to draw conclusions on the location of the users based on their interaction and/or any other means.*	1	DP^3T cannot be used for this purpose.

[78] https://github.com/DP-3T

FUNC-1	*The application must provide a functionality enabling users to be informed that they have been potentially exposed to the virus, this information being based on proximity to an infected user within a window of X days prior to the positive screening test (the X value being defined by the health authorities).*	1	
FUNC-2	*The application should provide recommendations to users identified as having being potentially exposed to the virus. It should relay instructions regarding the measures they should follow, and they should allow the user to request advises. In such cases, a human intervention would be mandatory.*	2	DP^3T enables each country to determine which information must be provided to Users who are notified of a potential risk of infection.
FUNC-3	*The algorithm measuring the risk of infection by taking into account factors of distance and time and thus determining when a contact has to be recorded in the contact tracing list, must be securely tunable to take into account the most recent knowledge on the spread of the virus.*	1	The algorithm is tunable. This should fall into the remit of the Steering Committee.
FUNC-4	*Users must be informed in case they have been exposed to the virus, or must regularly obtain information on whether they have been exposed to the virus, within the incubation period of the virus.*	1	
FUNC-5	*The application should be interoperable with other applications developed across EU Member States, so that users travelling across different Member States can be efficiently notified.*	3	This is currently not possible. The Consortium is, however, working on a technical solution to enable this functionality.
DATA-1	*The application must be able to broadcast and receive data via proximity communication technologies like Bluetooth Low Energy so that contact tracing can be carried out.*	1	
DATA-2	*This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application.*	1	
DATA-3	*The risk of collision between pseudo-random identifiers should be sufficiently low.*	1	

DATA-4	*Pseudo-random identifiers must be renewed regularly, at a frequency sufficient to limit the risk of re-identification, physical tracking or linkage of individuals, by anyone including central server operators, other application users or malicious third parties. These identifiers must be generated by the user's application, possibly based on a seed provided by the central server.*	1	
DATA-5	*According to the data minimisation principle, the application must not collect data other than what is strictly necessary for the purpose of contact tracing*	1	
DATA-6	*The application must not collect location data for the purpose of contact tracing. Location data can be processed for the sole purpose of allowing the application to interact with similar applications in other countries and should be limited in precision to what is strictly necessary for this sole purpose.*	1	The User App will not collect or store location data.
DATA-7	*The application should not collect health data in addition to those that are strictly necessary for the purposes of the app, except on an optional basis and for the sole purpose of assisting in the decision making process of informing the user.*		The User App will not collect or store health data.
DATA-8	*Users must be informed of all personal data that will be collected. This data should be collected only with the user authorisation.*	2	Information will have to be provided on country-by-country basis. The system is intended to be used on a voluntary basis.
TECH-1	*The application should [use] available technologies such as proximity communication technology (e.g. Bluetooth Low Energy) to detect users in the vicinity of the device running the application.*	1	The DP^3T protocol uses Bluetooth Low Energy technology.
TECH-2	*The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time.*	1	Storage is limited to 14 days.
TECH-3	*The application may rely on a central server to implement some of its functionalities.*	1	The DP^3T protocol is decentralised. The backend server exists only to enable people to use their own devices to trace

TECH-4	*The application must be based on an architecture relying as much as possible on users' devices.*	1	contacts. The server is not trusted with personally identifiable information at all (see Section I.3. pp. 2 ff.).
TECH-5	*At the initiative of users reported as infected by the virus and after confirmation of their status by an appropriately certified health professional, their contact history or their own identifiers should be transmitted to the central server.*	1	
SEC-1	*A mechanism must verify the status of users who report as SARS-CoV-2 positive in the application, for example by providing a single-use code linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, data must not be processed.*	1	The backend server is designed to only accept data from Users who have received an authorisation from a healthcare professional. How this authorisation will be granted and how the authorisation server will host the authentication keys will be specific to each country.
SEC-2	*The data sent to the central server must be transmitted over a secure channel. The use of notification services provided by OS platform providers should be carefully assessed, and should not lead to disclosing any data to third parties.*	1	Data is transmitted via an encrypted TLS connection.
SEC-3	*Requests must not be vulnerable to tampering by a malicious user.*	1	
SEC-4	*State-of-the-art cryptographic techniques must be implemented to secure exchanges between the application and the server and between applications and as a general rule to protect the information stored in the applications and on the server. Examples of techniques that can be used include for example: symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, homomorphic encryption, etc.*	1	
SEC-5	*The central server must not keep network connection identifiers (e.g., IP addresses) of any users including those who have been positively diagnosed and who transmitted their contacts history or their own identifiers.*	1	Network connection identifiers are not stored by the backend server.

SEC-6	*In order to avoid impersonation or the creation of fake users, the server must authenticate the application.*	1	
SEC-7	*The application must authenticate the central server.*	1	
SEC-8	*The server functionalities should be protected from replay attacks.*	1	
SEC-9	*The information transmitted by the central server must be signed in order to authenticate its origin and integrity.*	1	
SEC-10	*Access to all data stored in the central server and not publicly available must be restricted to authorised persons only.*	2	Access rights must be defined by the controller of the system in accordance with best practices and applicable laws.
SEC-11	*The device's permission manager at the operating system level must only request the permissions necessary to access and use when necessary the communication modules, to store the data in the terminal, and to exchange information with the central server.*	1	
PRIV-1	*Data exchanges must be respectful of the users' privacy (and notably respect the principle of data minimisation).*	1	
PRIV-2	*The application must not allow users to be directly identified when using the application.*	1	The DP^3T protocol is designed to limit the processing of personal data and mitigate the risks of identification. Such risks are described in detail in Section V. pp. 33 ff.
PRIV-3	*The application must not allow users' movements to be traced.*	1	Users' movements are not recorded.
PRIV-4	*The use of the application should not allow users to learn anything about other users (and notably whether they are virus carriers or not).*	1	Under normal operation, Users will not learn any information about any other identifiable User. Risks of identification are described in detail in Section V. pp. 33 ff.
PRIV-5	*Trust in the central server must be limited. The management of the central server must follow clearly defined governance rules and include all necessary measures to ensure its security. The localization of the central server should allow an effective supervision by the competent supervisory authority.*	1	The DP^3T has been designed in a decentralised manner to limit the trust required from the central server to the fullest extent possible.

PRIV-6	*A Data Protection Impact Assessment must be carried out and should be made public.*	1	
PRIV-7	*The application should only reveal to the user whether they have been exposed to the virus, and, if possible without revealing information about other users, the number of times and dates of exposure.*	1	Users only receive a notification that they have been potentially exposed.
PRIV-8	*The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements.*	1	The identity or movement of virus carriers is not shared and cannot be known under normal operations. Risks of identification are described in detail in Section V. pp. 33 ff.
PRIV-9	*The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement.*	1	Health authorities have no access to such information.
PRIV-10	*Requests made by the applications to the central server must not reveal anything about the virus carrier.*	2	The DP^3T protocol can be implemented in a manner ensuring that Users sending information to the backend server cannot be identified.[79]
PRIV-11	*Requests made by the applications to the central server must not reveal any unnecessary information about the user, except, possibly, and only when necessary, for their pseudonymous identifiers and their contact list.*	1	
PRIV-12	*Linkage attacks must not be possible.*	1	See Section V. pp. 33 ff. for an assessment of the risks.

[79] See Section V. pp. 33 ff., risk ref. "PR6" (Backend server can identify infected Users).

PRIV-13	*Users must be able to exercise their rights via the application.*	2	Users can at any time stop using the application or delete it. All their data will be erased after 14 days. In each country implementing the system, sufficient information must be provided to Users. Other rights of data subjects must be guaranteed by national authorities acting as controller (e.g. if applicable, ensure that individuals can obtain human intervention on the part of the controller, to express their point of view and to contest any automated decisions).[80]
PRIV-14	*Deletion of the application must result in the deletion of all locally collected data.*	1	
PRIV-15	*The application should only collect data transmitted by instances of the application or interoperable equivalent applications. No data relating to other applications and/or proximity communication devices shall be collected.*	1	
PRIV-16	*In order to avoid re-identification by the central server, proxy servers should be implemented. The purpose of these non-colluding servers is to mix the identifiers of several users (both those of virus carriers and those sent by requesters) before sharing them with the central server, so as to prevent the central server from knowing the identifiers (such as IP addresses) of users.*	2	This aspect is country-specific. DP^3T can be implemented in a manner that complies with this requirement.[81]
PRIV-17	*The application and the server must be carefully developed and configured in order not to collect any unnecessary data (e.g., no identifiers should be included in the server logs, etc.) and in order to avoid the use of any third party SDK collecting data for other purposes*	1	
CON-1	*The central server must collect the contact history of users reported as positive to COVID-19 as a result of voluntary action on their part.*		

[80] See Section IV.16. p. 27.
[81] See Section VI.2. pp. 38 ff. risk ref. "PR6".

CON-2	*The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus.*	n/a	Not applicable (these requirements only apply to systems in which COVID-19 positive Users send to a central server the history of proximity contacts they have obtained through scanning (instead or in addition to the list of its own identifiers), which is not the case of DP^3T.
CON-3	*Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person.*		
CON-4	*Except when the user detected as positive shares his contact history with the central server or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.*		
CON-5	*Any identifier included in the local history must be deleted after X days from its collection (the X value being defined by the health authorities).*		
CON-6	*Contact histories submitted by distinct users should not further be processed* *e.g. cross-correlated to build global proximity maps.*		
CON-7	*Data in server logs must be minimised and must comply with data protection requirements*		
ID-1	*The central server must collect the identifiers broadcast by the application of users reported as positive to COVID-19, as a result of voluntary action on their part.*	2	DP^3T is intended to be used on a voluntary basis. This is, however, specific to each implementing country.
ID-2	*The central server must not maintain nor circulate the contact history of users carrying the virus.*	1	
ID-3	*Identifiers stored on the central server must be deleted once they were distributed to the other applications.*	1	All identifiers stored on the central server are automatically deleted 14 days after having been uploaded.

ID-4	*Except when the user detected as positive shares his identifiers with the central server, no data must leave the user's equipment or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.*	1	In addition, EphIDs are shared between Users' devices as part of the normal operation of the system,
ID-5	*Data in server logs must be minimised and must comply with data protection requirements*	1	