




CH-3003 Bern, FDPIC-A-3F3C3401/1

To the Federal Office of Public Health



Your ref.:
Our ref.: FDPIC -A-3F3C3401/1
Case officer: 
Bern, 11 May 2020

Position statement according to Article 17a FADP re the pilot trial with the Swiss Proximity Tracing System (SPTS)

Dear Sir or Madam

The Federal Data Protection and Information Commissioner (FDPIC) has examined the documents provided by the Federal Office of Public Health (FOPH) in connection with the above matter and, in accordance with Article 17a of the Federal Act on Data Protection (FADP), and provides the following position statement:

The Commissioner regards the forthcoming pilot trial of the SPTS as permitted under the data protection law. Regulatory measures and recommendations may still be required during the pilot trial and following the transition to full operation as planned. The FDPIC comments on the following individual issues:

I. Swiss Proximity-Tracing-system (SPTS)

An international group of research scientists from various countries, including teams from the EPF Lausanne and the ETH Zurich, have developed a system known as 'Decentralised Privacy-Preserving Proximity Tracing' (DP-3T). The Swiss government wishes to make this technical aid available to the Swiss population as part of its strategy to combat the SARS-CoV-2 virus. When the associated mobile app is installed on a smartphone, it uses Bluetooth to decentrally and anonymously register when the phone 'encounters' other smartphones, i.e. is less than two metres away from them. The app identifies whether the smartphone has 'encountered' the smartphone of persons who are confirmed to be infected and warns users if they have been exposed to such persons for a certain duration.



Working with the EPFL and ETHZ, the FOPH plans to make a mobile app with the Swiss Proximity Tracing System (SPTS) available and to integrate the backend with servers in infrastructure operated by the Federal Office for Information Technology and Telecommunications (FOITT). As the federal authority responsible for operating this system, the FOPH must bear the responsibility of being the controller of a data file as per Article 3 letter i FADP (SR 235.1).

The Federal Council intends to introduce the mobile SPTS app from 13 May 2020 on the basis of a temporary ordinance (referred to below as the SPTS Ordinance), which is the subject matter of this position statement, and to test it until 30 June 2020. In the summer session in June 2020, Parliament is set to debate the dispatch announced by the Federal Council on an emergency amendment to the Epidemics Act (EpidA, SR 818.101).

II. Project and role of the Commissioner

The SPTS project involves the complex automated processing of large volumes of data from mobile phones and other smart devices used by the public, supplemented by notifications from and codes generated by medical professionals, who are bound to maintain confidentiality. Because these data sources relate to people and their health, the connection with persons and the sensitivity of the project in terms of data protection as a whole are obvious. Although the participants must not be identified, the SPTS still brings risks, in particular with re-identification, which must be countered with technical measures to protect the privacy and the informational self-determination over personal information of those concerned.

In their extraordinary session at the start of May 2020, the National Council and Council of States decided by comfortable majorities that the Federal Council's SPTS Ordinance should be replaced by a federal act in the June session of 2020. The discussions in the political institutions committees of both Councils and the Social Security and Health Committee of the Council of States, attended by the FDPIC, revealed that the introduction of the SPTS by the Federal Council before the enactment of the planned federal act would be based not on emergency or existing powers under the Epidemics Act (EpidA), but on the FADP. By conducting a pilot under Article 17a FADP, the conceptual and technical preliminary work can be tested over a short period in the expectation that the SPTS can come into operation at the end of June as an application that meets the practical requirements as well as its obligations with regard to fundamental rights, and which will be widely accepted by the general public based on the information they are given in advance.

In view of these clear political terms of reference, the Commissioner must review the statutory requirements of Article 17a FADP in conjunction with Article 27 of the Data Protection Ordinance in a way that takes account of the extraordinary limited timeframe necessitated by the pandemic.

Having been brought into the DP-3T project at an early stage as the independent supervisor for data protection and having informed the general public of his work in several interim reports published on his website, the FDPIC is now submitting his position statement on the pilot trial with the SPTS to the Federal Council pursuant to Article 17a paragraph 1 FADP. The position statement will be published in connection with the Federal Council decision on the SPTS Ordinance and will therefore also appear on the FDPIC website.

In accordance with the data protection principle of 'privacy by design', the EPFL contacted the FDPIC on 21 March 2020, which meant that the Commissioner's Corona Task Force was able to support the DP-3T project from the following day in accordance with Articles 27–29 and 31 FADP in all the essen-



tial phases, by supervising the project and offering legal advice and by providing its opinion on conformity with data protection requirements. This support was based on the documentation on Github¹ and on talking to people involved in the project at the EPFL and in the Federal Administration. On 2 April 2020, the FDPIC expressed its views in a first written outline assessment on main concerns related to data protection, in particular the anonymity of the personal data and the voluntary use of the app. A letter dated 23 April 2020 provided a legal data protection assessment of the technical structure of the backend, and on 1, 4 and 8 May 2020, the FDPIC expressed its views at office consultation procedures on the legal principles underlying the SPTS.

The political institutions committees of both councils and the Social Security and Health Committee of the Council of States held hearings with the Commissioner on 22 and 30 April, and on 5 and 7 May 2020 on the SPTS and other applications to combat the pandemic that his coronavirus task force is supervising.

III. Assessment of the application

1. Criteria

As the FDPIC made clear in his communication of 17 March 2020, that federal bodies that systematically gather data from a large number of personal sources such as smartphones and subject that data to automated processing are subject to the provisions of Article 4 FADP.

In the current context of combating the pandemic, the need for measures to be proportional and to have a clear purpose is particularly important; this demands that data processing related to the SPTS be limited in time and in the volume of data to the extent that is necessary to make a significant contribution to overcoming the current crisis.

Because of the aforementioned risks to privacy and informational self-determination over personal information related to the SPTS, automated processing that is unsuitable for achieving the expected minimum effect and that is therefore disproportionate cannot be permitted. Processing aimed at achieving additional objectives, such as the prevention of new epidemics, must also be excluded. In order to meet new objectives, new sector-specific legal principles that are sufficiently clear must be created through the standard legislative process. A clear purpose is necessary not least because if the SPTS is used successfully to combat the current pandemic, it is not inconceivable that authorities outside the healthcare sector might want to use proximity tracing for other purposes, such as maintaining national security or law enforcement.

The following assessment based on the criteria laid down by the FADP also follows the guidelines of the European Data Protection Board² and Council of Europe³ on combating pandemics.

2. Application design must be transparent and provide data protection by default

If the SPTS is to make an effective and direct contribution to the response to the current crisis and gradual easing of the public health-related restrictions on freedoms, the mobile app must be installed and activated by a significant proportion of the population that own smartphones equipped with Bluetooth technology. People must trust the app to process data in good faith as required by Article 4 paragraph 2 FADP: the operator must inform users fully and in easily understandable language about the

¹ <https://github.com/DP-3T/documents>, zugegriffen am 4. Mai 2020.

² https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_de (accessed on 9 May 2020).

³ <https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7> (accessed on 9 May 2020).



purpose of the SPTS and how it works, and it must be possible to activate the app's options in a user-friendly way. In addition, the operator must make it clear to everyone that the SPTS is designed to provide privacy by design.

2.1. Mode of operation

The way in which SPTS works, based on the principles of DP-3T, can roughly be described as follows:

Users download the mobile SPTS app from the Apple App Store or the Google Play Store and install it on their smartphones. On installation, a random initial private key is generated. The 'Messages' and Bluetooth functions are also required, which may require a confirmation.

The mobile SPTS app then begins to send via Bluetooth continuously changing random identifiers (Ephemeral IDs, EphIDs) that are based on the private key generated for that particular day, and receives EphIDs from other mobile SPTS apps in the immediate vicinity. The smartphone records its own private keys, which change each day, the EphIDs it receives, and the duration and approximate time of encounters with other phones running the app, storing them for 21 days in its own memory.

If a user tests positive for COVID-19, they can decide whether they wish send the date on which they may have been infected (as determined by a medical professional) to the server in encrypted form together with the private keys used by their app since that date. To do this, they need an authorisation code, which is also provided by a medical professional. This is necessary so that only cases of infection that have been medically confirmed can be reported via the SPTS. Once the backend server has been notified, the mobile app generates a new initial private key. This is generated randomly on a daily basis and does not allow any conclusions to be drawn as to any earlier private keys.

The mobile apps of all users retrieve the list stored on the backend server of the private keys of persons with confirmed infections and check whether the private keys they have received correspond to EphIDs they have recorded during any encounters. It is not possible to use the data sent (private key and starting date), whether on the backend server or on the smartphones, to identify persons who have been infected.

The data-protection-by-default approach of the SPTS is reflected in particular in the following design aspects:

- only the proximity between users is relevant, no location data is collected;
- there is no exchange of identifiers with smartphones that have not installed the mobile app;
- it is not possible to track people or devices based on the changing EphIDs;
- unless a person with a confirmed infection sends notification to the server, no data is uploaded to the server;
- only encounters of two metres or less are recorded and they only generate a message if they have lasted for at least 15 minutes on any day;
- data is only stored for as long as is useful to detect possible infections;
- the use of the system is limited to the duration of the pandemic;
- the system is based on a decentralised approach (see below).

A proximity tracing system needs infrastructure in the background. In order to process only as much data as is essential for tracing purposes (data minimisation), two approaches in particular currently come into consideration: the centralised and the decentralised models. The principles of the DP-3T provide for a decentralised system in which as much data as possible stays on the users' devices. Data on encounters is never stored on a central server. A server only exists in order to enable users to find out through their own devices whether they have had any relevant encounters. The server does not record any information that can be used to identify any persons, and does not disclose any identifiers. This means that centralised profiling is not possible. A decentralised approach also means that



the risks of the system being used for other purposes or of attacks on the server are reduced, which is why the FDPIC takes the view in his overall assessment that the decentralised model is preferable to a centralised approach.

As far as transparency is concerned, the DP-3T forming the basis for the SPTS is open-source. The documentation and the source code are available on the GitHub project website.⁴

2.2. Exposure notification solution von Apple and Google

On 10 April 2020, Apple and Google announced an 'exposure notification solution' for smartphones based on Bluetooth, with the aim of supporting contact tracing efforts. They claim that the available interface (API) will make using Bluetooth to constantly measure the distance between authorised mobile apps more secure, precise and efficient. The use of the API should in principle be restricted to one type of mobile app per country. According to their own information, Apple and Google will not receive any identifying information on users, locations or other devices near to the user. In addition, the project will not be commercialised. The two companies must be held to these claims. An update to the SPTS and the mobile app should be made to integrate the interfaces provided by Apple and Google for communication via Bluetooth when they become available.

2.3. Data protection declarations and conditions of use

The data protection declarations and conditions of use that the Commissioner has been given relate to the pilot trial. They are temporary in character and, apart from a few minor points that could be improved, appear to comply with data protection law. Individual changes may be made during the pilot.

2.4. Awaited mobile app test version

As no operable and testable SPTS mobile app is currently available, the FDPIC's assessment is based for the time being on the DP-3T concept, which is data protection compliant. As soon as testable visualised versions of the mobile app are available, the Commissioner will also be able to assess the conditions relating to data protection and usage as well as the user-friendliness of the SPTS mobile app intended for unrestricted operations and request any changes that may be needed.

2.5. Interim conclusion

Based on the foregoing, the FDPIC concludes that the backend in its current stage of development has data-protection-by-default architecture and meets the requirements for trustworthy and transparent data processing in terms of Article 4 FADP.

3. Risks and suitability of the measures taken

In line with the FDPIC's standing practice, federal bodies that systematically collect and process data from personal sources must conduct a data protection impact assessment that indicates the risks to the private domain and the measures that have been taken to counter such risks. The impact assessment must in particular consider the re-identification risks associated with anonymising personal data that the current app to combat the pandemic poses.

⁴ <https://github.com/DP-3T/> (accessed on 9 May 2020) and <https://github.com/admin-ch>.



During the DP-3T project, the FDPIC was provided with documents that correspond in essential respects to a risk impact assessment. On 1 May 2020, the FDPIC was also given a formal data protection impact assessment report, prepared by the EPFL and an external consulting company.⁵ This report identified the following risks in particular, proposing related measures:

- unlawful data access
- identification of contacts who test positive
- absence of any warning despite contact with an infected person
- false reports
- disclosure of app use and tracking of users' devices
- gathering of information on users based on local access to devices
- gathering of a significant number of EphIDs by relay attack
- data usage for other purposes / change of purpose / mass surveillance
- DP-3T system does not work as expected
- restrictions on freedom for those who do not use the app

Based on the foregoing, the FDPIC concludes that the application adequately explains the risks to privacy for app users and counters these risks with appropriate measures. For example, communications are encrypted and fake posts (noise) generated so that third parties are unable to identify persons who have been infected. For further details, reference is made to the technical assessment dated 23 April 2020 and to the abovementioned documentation.

4. Suitability

The SPTS is part of an overall strategy adopted by the Federal Council and the FOPH to respond to the present pandemic crisis and gradually relax the public health-related restrictions on freedoms.⁶ For the use of the SPTS to be assessed as proportionate under data protection law in view of the risks to privacy described above, the system must in principle be suitable to make an effective contribution to the overall strategy or to achieve a significant partial effect.

In the public debate over the SPTS, its suitability has been called into question on various occasions. For example, there are doubts as to whether a significant number of people will wish to install the app. Or there are fears that the project could fail because people will not be prepared to use the app to report that they have been infected. Critics have also suggested that many 'non-encounters' will be recorded in buildings, which will generate false alarms, or that the constant use of Bluetooth will use up a lot of battery power. In addition, people have pointed out that hardly any very elderly people, the group most at risk from the virus, use smartphones. Lastly, in view of the various approaches currently being taken by the pan-European consortium PEPP-PT,⁷ and of the withdrawal of the DP-3T Group from the consortium, the international compatibility of the SPTS according to the principles of DP-3T is in doubt.

In view of this criticism, it cannot be predicted with any certainty that the SPTS will have the effect hoped for. On the other hand, the Federal Council, the FOPH as the specialist office responsible and the EPFL regard it as likely that the SPTS will prove its worth and thus contribute to the further reduction and traceability of the life-threatening infections. In addition, representative surveys, such as that

⁵ https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf (accessed on 9 May 2020)

⁶ https://www.bag.admin.ch/dam/bag/de/dokumente/cc/kom/covid-19-faktenblatt-swiss-pt-app.pdf.download.pdf/BAG_Faktenblatt_Coronavirus_Swiss-PT-App.pdf (accessed on 9 May 2020).

⁷ <https://www.pepp-pt.org/> (accessed on 9 May 2020).



conducted by the Zurich University of Applied Sciences,⁸ seem to indicate that a majority of the population will decide not only to install the app, but also to use it to report an infection.

In view of the favourable prognoses from the FOPH as the specialist office, and of the comprehensive documentation provided by the EPFL and the scientific surveys, the FDPIC as supervisory authority for data protection must exercise caution in assessing the suitability of the SPTS, as he may not simply regard his discretion as superior to the prudent discretion of the specialist office responsible and there are no indications that the FOPH has not exercised its discretion prudently. In addition to the technical capabilities of the SPTS, user behaviour is also an important component of suitability. Although this behaviour may be influenced by the user-friendliness of the mobile app, which the FDPIC has yet to assess, and by the campaign to introduce the app promised by the FOPH, it is still hard to predict. Specific findings on acceptance will only become available after the evaluation of the pilot operations.

Based on the foregoing and according to the current level of knowledge, the Commissioner assesses the SPTS as suitable to make a partial contribution to preventing life-threatening infections. Accordingly, it is proven to be proportionate. In view of the doubts raised and the fact that, due to the lack of time, no explanatory report will be provided on the SPTS Ordinance, the FDPIC expects that the FOPH will justify suitability in the planned dispatch on the amendment of the Epidemics Act and in doing so respond to the criticism raised. If, during the pilot phase or full operations, it transpires that the application cannot fulfil the expectations made of it, the FDPIC reserves the right to recommend that the FOPH decide not to begin or continue full operations.

5. Statutory basis

Federal bodies that systematically gather and carry out automated processing of data from a large number of personal sources, such as mobile telephones, must have a statutory basis in terms of Article 17 paragraph 1 FADP for doing so in view of the associated risks to privacy and informational self-determination over personal information. This requirement applies even if using the application is voluntary.

According to its preamble, the temporary ordinance on the introduction of the SPTS provided by the Federal Council, which is the subject matter of this opinion from the FDPIC, takes Article 17a FADP as its basis. As a result, it provides an adequate statutory foundation for conducting the trials of the SPTS. In the summer session in June 2020, the Parliament should have the opportunity to debate the planned dispatch on an emergency amendment to the Epidemics Act (EpidA, SR 818.101). The FDPIC has already commented on the content of the SPTS Ordinance. His concerns were taken into account in the office consultation procedure.

The FOPH accordingly has an adequate statutory basis for the duration of the time-limited SPTS trials until 30 June 2020. The SPTS Ordinance and the trials based thereon are data protection compliant.

6. Permissibility of the SPTS trials

To assist us in preparing our opinion in accordance with Article 17a paragraph 1 FADP in conjunction with Article 27 paragraph 2 of the Data Protection Ordinance, the FOPH submitted the following documents to us in an email dated 7 May 2020 and in the course of the office consultation procedure on the SPTS Ordinance:

⁸ <https://www.zhaw.ch/de/ueber-uns/aktuell/news/detailansicht-news/event-news/viele-schweizer-fuerchten-ueberwachung-durch-contact-tracing-app/>, [zugegriffen am 04. Mai 2020](#).



- A. *General description of the pilot trial:* There are references to the aim, purpose and plan in the submission made to the Federal Council. These remarks must still be adapted to the requirements of the Hermes project management method.
- B. *Report that substantiates that the processing of sensitive personal data or personality profiles is required in order to fulfil statutory duties and that a test phase is essential before the Act formally comes into force (Art. 17a para. 1 let. c FADP):* The explanations given during the office consultation procedure on the SPTS Ordinance discuss the necessity of data processing using SPTS and of a test phase.
- C. *Description of the internal organisational structure and the data processing and control procedures (Art. 21 OFADP):* There are no regulations on processing. They must be submitted no later than two weeks before full operations begin.
- D. *Description of the security and data protection measures:* The FDPIC has received the risk impact assessment and further documents relating to the DP-3T concept that underlies the SPTS. However, the FOPH in an email dated 7 May 2020 only sent the FDPIC four documents on the risk analysis for the overall system⁹. The following information / documents have still to be provided:
- Latest risk assessment from the NCSC and implementation measures
 - Final version of the data flows for the pilot
 - Final system documentation (incl. connections to external systems) for the pilot
 - Protection requirements analysis
 - Proof of evaluation of risk analysis
 - Visualisation of the app
- E. *Draft of or concept for an ordinance that regulates the details of processing:* In the office consultation procedure on 8 May 2020, the draft of the SPTS Ordinance including a substantiated submission was given to the Federal Council.
- F. *Information relating to planning the various phases of the pilot trial:* There is no project management plan. Given the short duration of the urgently needed pilot trial, this plan is not needed.

In view of the urgency of the situation caused by the pandemic, it is understandable that the documents submitted to the FDPIC are incomplete. The introduction of the SPTS as a complementary measure for combating the pandemic should not be delayed because of this. The Commissioner expects, however, that the missing documents will be made available well before the start of full operations.

The first requirement for a pilot trial under Article 17a paragraph 1 letter a FADP is that the tasks that require automated processing are regulated in a formal enactment. The Federal Department of Home Affairs (FDHA) acknowledges this requirement in the submission to the Federal Council on the SPTS Ordinance, making reference to Article 31 paragraph 2 and Article 33 EpidA, which in particular provide that the responsible federal authorities, and therefore the FOPH, should support the cantonal authorities in informing persons that they may be infected with the disease.

⁹ Security Testplan Proximity Scanning, 14. April 2020, NCSC; Privacy Issue to be discussed v100, CSIRT-BIT/GovCERT-CH; Risk Assessment Proximity Tracing, 30 April 2020, CSIRT-BIT/GovCERT-CH; Checksums providing privacy in case a user mistypes its authentication code, 5 May 2020, NCSC.



The second requirement under Article 17a paragraph 1 letter b is that adequate measures must be taken to prevent breaches of privacy. Even though the Commissioner has not yet been able to verify all the relevant aspects of the SPTS, and in particular has not had access to a test version of the mobile app including visualisations, he regards the implementation of the SPTS based on current knowledge and the description of the planned trial to be adequate.

The final requirement for a pilot trial under Article 17a paragraph 1 letter c FADP is that in order to implement automated data processing in practice, there must be test phase before the enactment formally comes into force. In particular, this may apply when the effects and effectiveness must first be evaluated before necessary technical innovations or organisational or technical measures are introduced (Art. 17a para. 2 let. a. and b. FADP). In the submission to the Federal Council on the ordinance, the FDHA acknowledges these requirements, making reference to innovations that mean that testing before definitive introduction is essential. In view of the risks and complexity of the SPTS, the FDPIC agrees with this. As the FDHA admits, however, the planned pilot trial is rather short. The FDHA correctly states that the trial can nevertheless produce vital information relevant to the definitive introduction. This information relates in particular to operating the app, the technical infrastructure, the effectiveness of technical security measures and the use of the app by participants and specialists with access rights. In addition, the competent parliamentary committees expressly called for a brief pilot trial under Article 17a FADP to be conducted before the planned provisions in the EpidA come into force (see above Sec. II.). The conduct of a pilot trial is therefore essential.

7. Conclusion

The Commissioner regards the forthcoming trial of the SPTS by the FOPH as permissible under data protection law. The documents still missing must be submitted to the FDPIC in good time before the start of full operations. Regulatory measures and recommendations may still be required during the trial and following the transition to full operation as planned.

Yours faithfully

Adrian Lobsiger