Data Protection Statement of the Federal Office of Public Health FOPH in connection with the use of the "SwissCovid app"

Version: 1 July 2021

In this Data Protection Statement, the Federal Office of Public Health (FOPH) explains to what extent it will process personal data in connection with the use of the application "SwissCovid app" (hereafter app) in Switzerland. This account is not exhaustive; specific matters may be governed by other data protection statements, similar documents, terms and conditions of use, or applications.

The processing of personal data is governed by data protection legislation. The federal legislation on data protection is applicable to the processing of personal data. In addition, the Data Protection Statement is in line with the Epidemics Act of 28 September 2012 (EpG; CC 818.101), the Ordinance of 24 June 2020 on the Proximity Tracing System for the Coronavirus SARS-CoV-2 (VPTS; CC 818.101.25), the Federal Act on the Statutory Principles for Federal Council Ordinances on Combating the COVID-19 Epidemic of 25 September 2020 (COVID-19 Act; CC 818.102) and the Ordinance of 30 June 2021 on a system for notification of possible infection with the Coronavirus Sars-CoV-2 at events (VBV; CC 818.102.4).

"Personal data" means all information relating to an identified or identifiable person. "Processing" means any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data.

1 Controller

The controller responsible for the data processing described herein is the

Federal Office of Public Health FOPH
3003 Bern
Switzerland
Tel. +41 58 462 69 98
recht(at)bag.admin.ch

2 Collection and processing of personal data

The entire app system is designed to ensure that the app user is not identifiable. The processing of personal data is kept to a minimum. Data cannot be traced back by technical means to persons, locations or devices. What is collected via proximity tracing in the event of contacts is not location data, but merely encrypted data concerning proximity (contact) events. For the warning system only encrypted data about events and threats of infection at these events are collected. This data is protected by technical means against misuse. The FOPH cannot draw any conclusions concerning app users or decrypt the data. The app protects users' data in such a way that it cannot, at a distance, be connected to specific persons. Connection to a specific person cannot, however, be ruled out altogether. In particular with the proximity tracing system, there is a certain likelihood that, when someone is notified of a possible exposure, their recollection of social contacts over recent days may allow them to deduce the identity of the infected individual. As a result of using the app, persons may thus potentially be identified. The

notification on the basis of a close contact with a user who has tested negative also contains the behavioural recommendations of the FOPH, the information that the user may potentially have been exposed to the coronavirus, the dates on which this was the case and it draws attention to a guide (web form) as well as the Infoline offering free advice operated by the FOPH. If the user leaves the app in order to complete the guide, the dates named in the app on which an infection may have taken place are automatically transferred to the guide. Notifications on the basis of the check-in function cover the above-mentioned points, although here no guide or infoline is offered; the primary content of the notification is the recommendation to have a test.

The app system has three components:

- a proximity data management system, comprising software installed by users on their mobile phones and a back end (PM back end);
- a system for the management of codes for the activation of notifications (code management system), comprising a web-based front end and a back end;
- a system for the management of events, comprising software installed by users on their mobile phones and a back end (event back end).

The three back ends, as central servers, are under the direct control of the FOPH and are operated technically by the Federal Office of Information Technology, Systems and Telecommunication (FOITT). The code management front ends run on the devices of the experts authorised to generate the activation code (Covid code).

The following data is stored on the mobile phone:

- the identification codes (random ID) received from other mobile phones on which the app is running;
- the signal strength;
- the date and the estimated duration of proximity;
- the event identification codes with the relevant date, duration of attendance and designation of the event.

In the event of an infection being confirmed in a user, the following data is recorded in the code management system:

- the activation code (Covid code);
- the date on which the first symptoms appeared, or – if the infected user is asymptomatic – the date of testing;
- the time at which this data is to be destroyed.

The PM back end contains a list with the following data:

- the private keys of infected users which were current in the period during which other users were potentially exposed to the coronavirus;
- the date of each key.

The event back end contains a list with the following data:

- the event identification codes for the infected participants that were current at the time infection by other people at an event was possible;
- the date of each event identification code;
- the encrypted relevant period for the infected participant for each event identification code.

The proximity tracing system can also be connected to corresponding foreign systems if adequate protection of privacy is assured in the country in question (by means of corresponding legislation or sufficient guarantees, in particular in the form of an agreement). Foreign systems are considered to be "corresponding" if they are designed according to the following principles of the app system:

- During the processing of data, all appropriate technical and organisational measures must be taken in order to prevent instances in which the participating individuals can be identified;
- To the greatest extent possible, the data is processed on decentralised components installed by the participating individuals on their mobile phones. In particular, data on a participating individual's mobile phone about other people may only be processed and stored on this mobile phone;
- Only data required to determine the distance and time at which proximity occurred and to issue notifications is obtained or otherwise processed, not location data;
- The data is destroyed as soon as it is no longer required for the notification.

At present, there is a connection with the Corona-Warn-App used in Germany. During the connection, the PM back end and the foreign system are linked to a connection system that allows for the mutual transmission of the private keys of infected users. The app system then transmits the app's private key to the connection system and saves the private keys of the connected foreign apps on the PM back end.

3 Purposes and legal basis

The app system operated by the FOPH and the connection system are based on the EpG, the VPTS, the COVID-19 Act and the VWV. The exclusive purposes of the app and the associated data processing are, in a privacy-preserving manner, to notify users potentially exposed to the coronavirus and to produce coronavirus-related statistics using data from the three back end systems.

The connection system serves to ensure that such a notification is also possible between connected national apps. This means that users of the app can also be notified if they have been in proximity to an infected user of a foreign app (e.g. cross-border commuters and tourists in Switzerland or contacts abroad). Conversely, users of a connected foreign app can also be notified if they have been in proximity to infected users of the app.

4 Data transfer

The list of data in the PM and event back end systems is made available to the app (or front end) in the retrieval process. Insofar as the FOPH engages third parties in Switzerland or abroad to provide this service, they undertake contractually to comply with the requirements of Article 60*a* EpG, the VPTS, Article 3 paragraph 7 letter a COVID-19 Act and the VWV, with the exception of the provisions concerning the source code specified in Article 60*a* paragraph 5 letter e EpG and Article 15 VWV. The FOPH monitors compliance with the legal requirements. The third parties engaged are not permitted to use non-core data arising in the execution of this task for their own purposes. This data will only be analysed by the FOPH or the FOITT (cf. Section 8).

The list with the private keys of the infected users of the PM back end is also regularly transmitted to the connection system for a cross-border notification. The connected foreign systems (currently: the German Corona-Warn-App) then download these private keys and make them available to their apps for retrieval (see *Section 2*).

The FOPH will periodically make available to the Federal Statistical Office (FSO), in an anonymised form, the data currently held in the three back end systems, for purposes of statistical analysis. The data of the connection system can be disclosed to the FSO and the responsible foreign body for statistical purposes in a completely anonymised form. The FOITT operates the entire software on behalf of the

FOPH and provides the necessary technical support service. The FOITT has access to data only insofar as this is necessary for the purposes described and the activities of the employees concerned. They are bound by confidentiality in the management of the data.

For the proximity tracing system the app uses an interface to the operating system of the user's mobile phone, which entails the processing of data by Apple or Google. The operating system functions used via the interface must comply with the requirements of Article 60*a* EpG and the VPTS, with the exception of the provisions concerning the source code specified in Article 60*a* paragraph 5 letter e EpG. The FOPH makes sure that these requirements are complied with, in particular by obtaining appropriate assurances.

5 Retention period

The data will be destroyed as soon as it is no longer required for the notification of users. Specifically, it will be destroyed as follows:

- data in the proximity data management system (both on mobile phones and in the PM back end): 14 days after capture;
- data in the event management system (both on mobile phones and in the event back end): 14 days after their collection;
- data in the code management system: 24 hours after capture;
- the data of the connection system: not later than 14 days after its transmission to the connection system.

6 Data security

To protect data against unauthorised access, loss, or misuse, the FOPH, in close collaboration with its internal and external hosting providers and other IT service providers, takes appropriate security measures of a technical (e.g. encryption, pseudonymisation, logging, access controls and restrictions, data backup, IT and network security solutions, etc.) and organisational nature (e.g. staff directives, confidentiality agreements, inspections, etc.) in accordance with the requirements of the Federal Administration and Swiss data protection legislation.

7 Rights of data subjects

With regard to your data, you have the right to information, rectification, erasure or disclosure. You also have the right to restrict or object to data processing. In addition, you have the right to withdraw your consent, without this affecting the lawfulness of processing based on consent before its withdrawal. These rights are applicable insofar as personal data is present. This is, however, prevented to the greatest possible extent by the "privacy by design" principle underlying the app system, which – through innovative cryptographic methods and decentralised data processing – is designed to ensure that, as far as possible, no information relating to identified or identifiable persons (personal data) is present. For this reason, it is not possible for the FOPH, for example, to provide information on the proximity events logged for a specific person or to correct this data. The FOPH cannot inspect this data, as it is stored only on the mobile phones.

The exercise of your rights requires that you provide clear evidence of your identity (e.g. a copy of identity documents). To assert your rights, you can contact the FOPH at the address given in Section 1.

In the event of infringements of data protection legislation, you can contact the competent data protection supervisory authority or take legal action in accordance with the data protection legislation.

8 Other information

PM back end, event back end and code management system access events are logged for the purposes specified in Articles 57*l*–57*o* of the Government and Administration Organisation Act of 21 March 1997 (RVOG; SR 172.010). The access events may be statistically analysed. The provisions applicable are Articles 57*i*–57*q* RVOG and the Ordinance of 22 February 2012 on the Processing of Personal Data Linked to the Use of the Electronic Infrastructure of Federal Bodies (SR 172.010.442).

Log data will be destroyed as follows:

- Log data from the third parties engaged by the FOPH: 7 days after capture;
- Otherwise, the destruction of log data is governed by Article 4 paragraph 1 letter b of the Ordinance of 22 February 2012 on the Processing of Personal Data Linked to the Use of the Electronic Infrastructure of Federal Bodies (SR 172.010.442).

9 Amendments

The FOPH may amend this Data Protection Statement at any time without prior notice. The current published version, or the version valid for the period in question, is applicable. This Data Protection Statement has been issued in several languages. In the event of discrepancies, the German version shall prevail. In the event of an update, the app user will be informed of the amendment in an appropriate manner.

* * * * *