COVID Alert Malta

Privacy Policy

Introduction

In this Privacy Policy the Superintendent of Public Health explains to what extent it will process personal data in connection with the use of the application “Covid Alert Malta” App (hereafter app).

The processing of personal data is governed by data protection legislation, including the General Data Protection Regulation¹ (EU) 2016/679 (GDPR) and Data Protection Act (Cap 586 in the Laws of Malta)². The legislation on data protection is applicable to data control, collecting, and processing of personal data.

“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.

Controller

The controller responsible for the data processing described herein is the:

Superintendent of Public Health.

Office of the Superintendence of Public Health

St Luke’s Hospital

OPD (Level 1), St. Luke’s Square

Pieta’ - Malta

PTA 1010

Telephone: +356 2595 3302 / +356 2595 3303

Fax: +356 2595 3304

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 and designed to maintain privacy through anonymisation and pseudonymisation. Data cannot be traced back by technical means to persons, locations or devices. What is collected is not location data, but merely encrypted data concerning proximity (contact) events. This is protected by technical means against misuse. The Superintendent of Public Health cannot draw any conclusions concerning app users. 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. 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. The notification contains the information that the user may potentially have been exposed to the coronavirus, the date on which this was last the case, and the behavioural recommendations of the Superintendent of Public Health. As a result of using the app, persons may thus potentially be identified.

The app system has two components:

1) An exposure notification data management system, comprising software installed by users on their mobile phones and a back end (EN backend).
2) An authorisation code management system, comprising a web-based front end and a back end.

Both back ends, as central servers, are under the control of the Superintendent of Public Health and are operated technically by the Malta Information Technology Agency (MITA). The code management front ends run on the devices of the health experts authorised to generate the authorisation codes.

The data stored locally on a user’s device consists of the following:

a) Rotating Proximity Identifiers (RPIs) that it broadcasts;
b) Coarse timestamps; and
c) The Temporary Exposure Keys (TEKs) used to generate the RPIs.

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

a) The authorisation code;
b) The date on which the first symptoms appeared, or – if the infected individual is asymptomatic – the date of testing (onset date);
c) The time at which this data is to be destroyed; and
d) The transmission risk level assigned by Health Authority to the case.
The EN back end contains a list with the following data:

- The secret keys (TEKs) of infected users which were current in the period during which infection of other persons is likely to have occurred (i.e., from onset date onwards up to max 14 days); and
- The date of each key.

After coming into proximity (2 metres or less) with another mobile phone on which the app is running, the app stores the following data:

- The Rotating Proximity Identifiers (RPIs) broadcast by the other device;
- Proximity (the Bluetooth low energy signal strength);
- Approximate time window; and
- The estimated duration of proximity.

**Purposes and Legal Basis**

The exclusive purposes of the app and the associated data processing are, in a privacy-preserving manner, to notify users of having potentially been in proximity of an infected person and to produce coronavirus-related statistics using data from the two back end systems.

**Data Transfer**

The EN back end data list is made available to the app in the retrieval process. Insofar as the Superintendent of Public Health engages third parties in Malta or abroad to provide this service, they undertake contractually to comply with the requirements of GDPR. The Superintendent of Public Health 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 be analysed by the Superintendent of Public Health. Aggregated data will be analysed by the Directorate for Health Information and Research.

The Superintendent of Public Health will periodically make available to the Directorate for Health Information and Research, in an aggregated and anonymised form, the data currently held in the two back end systems, for purposes of statistical analysis. MITA operates the entire software on behalf of the Superintendent of Public Health and provides the necessary technical support service. MITA 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.

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 devices and relevant technology. The operating system functions used via the interface must comply with the requirements of GDPR. The Superintendent of Public Health makes sure that these requirements are complied with, in particular by obtaining appropriate assurances.
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:

a) data in the proximity data management system on mobile phone: 14 days after capture
b) data in the proximity data management system back end: 14 days after upload

Data Security

To protect data against unauthorised access, loss, or misuse, the Superintendent of Public Health, 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.)

Rights of Data Subjects

Use of the app will occur on a voluntary basis. The storing of information in the smart phone of a user will happen with the user’s consent, which is obtained when the user agrees to this policy when downloading and using the app. Users will be able to withdraw their consent to use the system at any time by deleting the app or simply stopping using it, in which case no more data will be generated. Individuals who decide not to or cannot use the app will not suffer from any disadvantage.

Through innovative cryptographic methods and decentralised data processing, the system is designed to ensure that, as far as possible, no information relating to identified or identifiable persons (personal data) is present. For this reason, the Superintendent of Public Health cannot (i) identify the individuals to which the data stored on the backed server relates, thus cannot carry out request for deletion or (ii) access, nor delete, the data that is stored on the users’ devices. It is not possible for the Superintendent of Public Health, for example, to provide information on the proximity events logged for a specific person or to correct this data. The Superintendent of Public Health cannot inspect this data, as it is stored only on the mobile phones of the respective user.

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.

Amendments

The Superintendent of Public Health may amend this Privacy Policy at any time without prior notice.