Application “Stop COVID-19“

Data Protection Impact Assessment (*summary*)

Explanation

Since the SARS-CoV-2 virus began to spread across Europe and the world in early 2020, public and political debates have increasingly focused on a technological solution to the burning problem. Can the COVID-19 outbreak be curbed using an app on a smartphone?

Such a system would automatically record the user's contacts and thus be able, in a timely manner and anonymously, to inform those who were in epidemiologically relevant contact with a COVID-19 patient confirmed by the laboratory finding. Then exposed individuals could be effectively informed about the treatment of a potential early stage of infection.

In order to slow the spread of disease COVID-19 among the population in the Republic of Croatia, the Government of the Republic of Croatia and the Ministry of Health have developed an application **"Stop COVID19"** that informs users that they have been in contact with the person who was subsequently confirmed to be infected with disease COVID-19.

The app is based on a service jointly developed by Google and Apple and uses Bluetooth technology to exchange random keys between users' smart devices that are in an epidemiologically relevant close contact. These encrypted keys are changed several times during each hour, further guaranteeing the protection of users' privacy.

If one of the users subsequently receives a positive laboratory test for COVID-19, he may decide to share this information via the application using a one-time verification code. In this way, the application determines whether the user has been in contact with a COVID-19 positive person and, if so, specifies the date of the contact made and recommends the next steps. Downloading the app is voluntary, and the users can turn it off whenever they want. Information about keys will be exchanged through the European Federated Gateway Service (EFGS), and only if the user enables the setting for cross-border data exchange after installing the application. The installation and use of the application does not require user registration, any personal data is not recorded and none of the user's geolocation data be collected at any time.

Looking at the planned systems to prevent the spread of COVID-19 across Europe, these are extensive social experiments involving the digital recording of the behavior of individuals under state control. The effectiveness and implications of such applications cannot yet be predicted, and it can be assumed that various versions will be imported and evaluated.

The consequences for data protection, and therefore fundamental rights, will potentially affect individuals, but also society as a whole. For this reason, we consider it relevant to carry out a data protection impact assessment (DPIA).

In the whole process, we have included the Croatian Data Protection Supervisor, the Agency for the Protection of Personal Data (AZOP), with whom we will regularly consult in case of changes in the functionality of the application.

A summary of the data protection impact assessment was published on November 16, 2020. The Ministry reserves the right to modify and update this document.

Findings and assessment

The application "Stop COVID-19" is under the jurisdiction of the Ministry of Health of the Republic of Croatia, Ksaver 200a, 10000 Zagreb, Republic of Croatia, tel: 01 46 07 555. In accordance with data protection regulations, the Ministry is **the controller** and is responsible for processing data within the application. **The processor** is APIS IT d.o.o., Paljetkova 18, 10001 Zagreb. If necessary, you can contact the Ministry's data protection officer at the above address or by sending an e-mail to zastita.podataka@miz.hr.

The description of the processing being the subject of the assessment, the measures contributing to the rights of the application users and how any risks to the rights of the user are controlled, are contained in the answers to the questions in this assessment.

Is the application usage mandatory?

Installing and using the app is voluntary. Users decide independently whether to download the installation to their mobile device, how they will use it and when to remove the app from their mobile device. Users decide for themselves whether to enable the exchange of anonymous keys through the European Federated Gateway service. The legal basis for data processing is the performance of a task of public interest.

What types of data are processed and where?

Random keys of contacts and infected persons, one-time verification code and date of contact of the two users. Minors can also use the application, but the system does not check or determine this. The processing of pairing of random keys occurs exclusively on the user's mobile phone, the one-time verification code app communicates to the national background system with encrypted and protected channels.

Data processed using the Application is located on the user's mobile device, on the Application's servers in the Republic of Croatia or in another EU member state. Data is not transferred to third countries.

What is the scope of data processing?

For the app to be as efficient as it is, it is recommended to be installed by as much as possible share of the population. The geographical area covers the entire territory of Croatia, and once interoperability is established with EU Member States using the same Google/Apple services, key exchanges with servers in those countries will be achieved. The possibility of further processing for purposes unrelated to the management of the health crisis caused by the COVID-19 virus is excluded.The data will be used during an epidemic with the possibility of shutting down the app in case the health system is potentially burdened or at the end of epidemic.

What is the nature of the relationship between the data subject and the controller and the processor?

The controller and processor cannot find out who the users are because there is no list or register of the application users. The only information that the user voluntarily enters into the application is the verification code, generated by the competent

healthcare professional after a positive laboratory finding on the infection, to enable other users to be notified of the exposure to the infection. The user does not enter any other information and may remove the app from the device at any time. There is no practical possibility of intervention in data processing.

What is the maturity of technology?

The application involves applying brand new technology and ways to process data. The technology is in the early stages of application, but there is no particular concern as the same methods are used or are intended to be used by most EU members and other countries that choose to rely on Google/Apple exposure notification services. The European Commission, in cooperation with the World Health Organization, is preparing a common framework to assess the effectiveness of the use of these applications.

Is data processing proportionate to the legal basis?

The app is limited to the most necessary data and uses the Google/Apple service that is an integral part of the operating system (Android or iOS) on the mobile device, according to the publicly available documentation, description of the operation and architecture of the app, and the source programming code. Data processing is reduced to a strict minimum, and only necessary data are processed in accordance with the purpose (device identifiers, geolocation data, communication identifiers, etc. are not processed).

What data processing information does the data subject have?

Before installing an app or later in the app itself, the user has the option to read the Privacy Policy, Terms of Use, Accessibility Statement, and program components used. All information about the app is also available through the Government Official Website for timely and accurate information about the corona virus at koronavirus.hr.

What is the data security?

The processor ensures confidentiality, integrity and availability of data in accordance with standards and best practices (backups, limited powers on the production database, etc.), and irreconcilableness is ensured by the production and monitoring of log records. The system is also subject to vulnerability checks and no deficiencies have been identified. The processor has a valid ISO 27001 certificate. A security architecture defined at eHealth Network level is used to exchange data between the national system and the European Federated Gateway service.

How is the privacy of the user preserved?

At the design stage, the processor applied the principles of preserving privacy and initially set all features to preserve the privacy of users, thereby neutralizing these risks and minimizing them. All available and appropriate measures have been taken to prevent identification of the user of the application. Prior consultation with the Croatian Agency for the Protection of Personal Data was carried out in order to assess the compliance of the application with the General Data Protection Regulation, and compliance with guidelines and opinions of the European Data Protection Board on the use of location data and interoperability of contact tracing tools in the context of the COVID-19 outbreak.

How is compliance with obligations and the conduct of the processor ensured?
Decisions of the Government of the Republic of Croatia and the Minister of Health, the contractual obligation of the processor, implementation of all necessary procedures and protocols for data protection and compliance with legal regulations.

Is the health data being processed?

The health data is not being processed. The process consists in processing contact data on mobile devices that have an activated application, transferring that data to the server after a positive diagnosis and distributing it to all other mobile devices to determine the existence of possible contacts with affected persons. The application does not provide health advice or be tasked with replacing doctors or other medical staff in treating patients whether related to COVID-19 or any other disease and infection.

Is it possible to de-anonymize users?

Reference to a natural person is effectively and irreversibly separate from the processed data by a multidimensional approach, therefore preventing the possibility of re-identification of the app user. The application of legal, technical and organizational measures ensures the efficient and irreversible separation of data in practice resulting in non-identification data indicating disease exposure, which are stored on the server and distributed to other applications.