Privacy notice

Application #OstaniZdrav

This privacy notice explains what data is collected when you use the #OstaniZdrav App, how that data is used, and your rights under data protection law.

1. Who has provided you with #OstaniZdrav App?

The #OstaniZdrav application ("App") was prepared by the National Institute of Public Health ("NIJZ") and the Ministry of Public Administration ("MJU"), whereas the NIJZ is responsible for the content of the application and the MJU for its technical part. According to the General Data Protection Regulation (GDPR), MJU and NIJZ play the role of a joint controllers within the framework of the #OstaniZdrav application.

E-mail address of the data protection officer:
- with the NIJZ: vop@nijz.si
- with the MJU: dpo.mju@gov.si.

In the event of confirmed SARS-CoV-2 coronavirus infection, and if you enable exposure logging, you warn also users of other mobile App in Member States of European Union (which are integrated into the daily exchange system via a central server (EU Federation Gateway Service - EFGS) managed by the European Commission). In this case, the participating European Union Member States, represented by the designated national authorities or official bodies determine together the purpose and means of processing of personal data through the federation gateway and are therefore joint controllers. National Joint Controllers and their privacy policies are available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/gateway_jointcontrollers_en.pdf.

2. Is using the App voluntary?

The use of the #OstaniZdrav App is completely voluntary.

3. Are personal data processed for the operation of the App?

Randomly assigned daily keys and transmit codes are processed for the operation of the App, which have, legally speaking, the status of pseudonymized personal data. For more information, see below.

If you decide to use the App, you must press the "Enable exposure logging" button, when you log in the App for the first time. Without your agreement, the App cannot access the functionality of exposure logging on your smartphone.

Special agreement is required for processing of data carried out for the purpose of informing other users of the App that you are infected with SARS-CoV-2.

You can disable the functionality of exposure logging at any time in the App, which means that the application cannot work at that time.

4. On what legal basis is your data processed?

Your data is processed on the legal basis of the Act on Temporary Measures for Mitigation and Elimination of Consequences of COVID-19 (Official Gazette of the Republic of Slovenia, No. 152/20), supplemented with the Act on Intervention Measures to mitigate the consequences of the second wave of the COVID-19 epidemic (Official Gazette of Republic of Slovenia, no. 175/20), which stipulates that the installation and use of the App is voluntary.

Stated Act on Temporary Measures for Mitigation and Elimination of Consequences of COVID-19 determines purpose of establishing and operating the App, its design details and its interoperability with the central system (EFGS) provided by the European Commission (Article 46 – 54).

You can stop using the App at any time. More information about the cancellation can be found in Section5.

The application does not log your exposure if you:

- disable the exposure logging;
- turn off Bluetooth system;
- in the case of Android systems, turn off location that does not in itself have the functionality related to the App (i.e. it does not have access to location data) but the phone is technically designed to require it to be switched on for the operation of Bluetooth;
- have your phone turned off;
- remove the App from your phone.

The transmission of the confirmed SARS-CoV-2 infection to the infected code server through the transmission of daily keys shall be provided only after the entry of a specific intervention code and after additional specific agreement within the App. The data thus transmitted shall be deleted from the server of the infected code within 14 days of transmission.

5. Stop using the App

You have the right to stop using the App at any time with effect for the future. Please note that this will not affect the lawfulness of the processing before you stopped using the App.

You can disable the exposure logging feature using the toggle switch in the App or delete the App. If you decide to use the exposure logging feature again, you can toggle the feature back on or reinstall the App. The NIJZ and MJU do not have access to random proximity identifiers that were transmitted via Bluetooth to another user, but the App is designed in such a way that they are erased after 14 days.

The transmission of the confirmed SARS-CoV-2 infection to the infected code server through the transmission of temporary exposure keys shall be provided only after the entry of a specific code and after additional specific agreement within the App. The agreement is valid for a single transfer of infected codes to the infected code server. The data thus transmitted shall be deleted from the server of the infected code within 14 days of the transmission.

6. Who is the App intended for?

The App is intended for persons residing in the Republic of Slovenia who are at least 16 years old.

7. What personal data is processed?

The App is designed to process as little personal data as possible, at the same time, these data are processed dispersed on different devices. This means, that the App does not collect any data that would allow the NIJZ and MJU or other users to obtain data of your encounters or of your possible infection, as well as infer your identity, health status or location. The encounters dealt with in the App are the detections of the phone of an individual user that another user's phone is located in detectable vicinity.

In addition, the App deliberately refrains from using tools to analyze how you use the App. As part of the functioning of the App:

- The random temporary exposure keys ("daily key") created by the App is processed when the individual installs it on the phone. The daily key changes daily and is kept exclusively on this individual's phone for 14 days, then it is automatically deleted. Only if an individual enters a specific verification code into the App and explicitly gives his agreement, is the daily key temporarily transferred to a special server ("infected key server") located on the infrastructure of the Ministry of Public Administration. Only the daily key is transmitted from the to the server of infected keys in case of explicit agreement of the individual, without any other information from the phone,
- Every 15 minutes, based on the daily key, the App creates a transmit code that is stored on an individual's phone through completion and encryption, and this same transmit code is transferred to another user's phone when an encounter is detected. When downloading, another user's phone creates a set of metadata that shows the time of encounter and decibels, from which the App calculates the distance of the encounter and assesses the degree of risk of infection.
- An individual with confirmed infection with SARS-CoV-2 is contacted over the phone by the NIJZ which provides them with the confirmation code ("teleTAN"). This allows the individual to confirm that they are infected within one hour through the App. After confirmation, the verification key is converted into proof by using the registration token, which then provides information on the daily keys to the infected key server. Daily keys of the users diagnosed with SARS-CoV-2 infection are stored in the infected key server for 14 days, then they are automatically deleted. Once a day the App retrieves from the infected key server information on the infected keys and calculates the data in such a way that it complies and encrypts the individual daily key and compares is with the transmitting code of

its encounters (i.e. the users of the App that were in detectable vicinity of Bluetooth area of the user's phone). Only when a match is established, can the App open a set of metadata and assesses the risk of infection.

Additional highlights:

The logging of encounters on a user's phone from the second indent is therefore carried out only from the moment the exposure logging is confirmed in the App. Previous logging of exposure is not possible as there is no technical solution to do so. In case of receival of information about infectiousness of an individual daily key, the possibility to check this contact information is therefore limited to the time when the App was operating on each phone.

The database of infected persons kept by NIJZ under Annex 1 of the Healthcare Databases Act are in no way technically related to the #OstaniZdrav App and the NIJZ runs it independently of the #OstaniZdrav App. The database does not contain any data from the #OstaniZdrav App.

The list of users of the #OstaniZdrav App does not exist.

The data processed in the #OstaniZdrav App can therefore be divided into:

a. Technical access data

Technical access data is generated when you use or enable the following features

- Exposure Logging
- Notifying other users of your infection.

Each time the App exchanges data with the back-end system, access data are monitored. This is necessary so that the App can retrieve the correct data or transfer the data from the phone to the server. Access data are processed to maintain and protect the technical data of the operation of the App to maintain and protect the technical data of the App and the back-end system. You will not be identified as an App user from this information, not will a user profile be created.

The IP number assigned by your operator from which your mobile device accesses the back-end system is stored according to the rules for storing access logs. This data is stored on the back-end system server for up to 6 months in a backup copies for up to 12 months, after which is deleted. Further processing of the IP number is not possible without a court order. It is not possible to identify an individual by the data controller on the basis of these records.

The following data is also processed:

- Date and time of access (time stamp);
- Transmitted data volume (or packet length);
- Notification of successful access.

This technical access data is only processed to secure and maintain the technical infrastructure. You are not identified personally as a user of the App and it is not possible to create a user profile.

b. Contact data
If you enable exposure logging in your smartphone's operating system, which records encounters (with other users, then your smartphone will continuously send out transmit codes, complied and encrypted values of daily key which are changed every 15 minutes (RPI) via Bluetooth Low Energy, which other smartphones in your vicinity can receive if exposure logging is also enabled on them. Your smartphone, in turn, also receives the transmits codes of the other smartphones. In addition to the transmit codes received from other smartphones, your smartphone's exposure logging functionality logs and stores the following contact data:

- Date and time of the contact
- Duration of the contact
- Bluetooth signal strength of the contact
- Encrypted metadata (protocol version and transmission strength).

Your own transmit codes and those received from other smartphones as well as the other contact data (date and time of the encounter, duration of the encounter, signal strength of the encounter) are recorded by your smartphone in exposure log and stored there for 14 days.

The functionality used to record encounters with other users is called "COVID-19 Exposure Notifications of persons diagnosed with SARS-CoV-2" on Android smartphones and "COVID-19 Exposure Logging" on iPhones. Please note that this exposure logging functionality is not part of the App, but an integral part of your smartphone's operating system. This means that the exposure logging functionality is provided to you by Apple (iPhones) or Google (Android smartphones) and is subject to these companies' respective privacy policies. The NIJZ and MJU are not responsible or has no influence on data processing performed by the operating system in connection with exposure logging.

More information about the exposure logging functionality on Android smartphones is available in settings under "Google" > "COVID-19 Exposure Notifications" and at https://support.google.com/android/answer/9888358?hl=en. Please note that the exposure logging functionality is only available if the version of Android is 6 or higher.
More information about Apple's exposure logging functionality can be found in your iPhone's settings under "Privacy" > "Health" > "COVID-19 Exposure Logging". Please note that the exposure logging functionality is only available if iOS version 13.5 or higher is installed on your iPhone.

The App will only process the contact data generated and stored by your smartphone if the App's exposure logging feature is enabled.

c. Data on random daily keys of an individual that wishes to share information of their infection

If you want to share with other users of the application or users of the other mobile App of the Member States of the European Union the information that the result of the SARS-CoV-2 test has been positive, this will be done in a way that:

- to agree to provide information, you use the confirmation code (teleTAN), which is provided by the epidemiologic service and is valid for three hours;
- By using the registration token, which is changed to another number, you provide information on your random daily keys for the last 14 days to the infected key server.

8. App features

a. Exposure Logging
The App's core functionality is exposure logging with other devices and assess the risk of infection with SARS-CoV-2. In addition to the risk-based assessment, the application shall also show advice pre-prepared by the NIJZ for each risk status. They are text generically prepared in the application and tied to the displayed status.

If you enable the exposure logging feature, then once a day, while the App runs in the background (or when you tap on "Update"), it will retrieve from the infected keys server a list of transmit codes from users who have tested positive and shared their own transmit codes. The retrieval is carried out in a way that the App calls the server which then provides the codes as an automated response. The App shares these transmit codes with your smartphone's exposure logging functionality, which then compares them with the transmit codes stored in your smartphone's exposure log. If your smartphone's exposure logging functionality detects a match, it transfers the contact data (date, duration, signal strength) to the App, but not the transmit codes of the encounter in question.

In the event of a contact, the App analyses the contact data provided by the exposure logging functionality in order to assess your individual risk of infection. The evaluation algorithm which determines how the contact data is interpreted (for example, how the duration of a contact influences the risk of infection) is based on current scientific findings. To account for new findings as and when they arise, the NIJZ and MJU can update the evaluation algorithm by adjusting its settings. The settings for the evaluation algorithm are sent to the App together with the list of daily keys of infected users.

The assessment of your risk of infection is only carried out locally on your smartphone. Once identified, the risk of infection is also only stored in the App and is not passed on to any other recipients (including the NIJZ, MJU, Apple, Google and other third parties).

b. Notifying other App users or users of the other mobile App of the Member States of the European Union that you are infected
If you use the feature for notifying and warn other App users or users of the other mobile App of the Member States of the European Union that you were infected with SARS-CoV-2, you can only do so after receiving confirmation of infection from the NIJZ and receiving a TeleTAN number.

The epidemiological service uses the entry portal to create a TeleTAN number with special access to the server system and provides the users with the TeleTAN number. When you enter the TeleTAN number in the App, it sends it back to the application server system for comparison and verification. The App receives a token from the server system, i.e. a digital access key stored in the application. With the token, the App requires a TAN number from the server system. The teleTAN number can only be used once.

Informing other App users or users of other mobile App of the Member States of the European Union that SARS-CoV-2 infection has been confirmed in is carried out between mobile App in the Member States of the European Union and which are through controlled procedure included in the system for exchange of daily keys managed by the European Commission.

The server in the Republic of Slovenia and the European Central Server (EFGS) exchange data on assigned daily keys of mobile App users who were positive for SARS-CoV-2 infection with other comparable voluntary App for notification of contacts with infected persons within the European Union. The European Central Server (EFGS) is an integral part of the digital infrastructure of the eHealth network set up between the Member States of the European Union. The exchange of daily keys of users of mobile App that have been positive for SARS-CoV-2 infection is carried out between mobile App, operating in the Member States of the European Union and are through controlled procedure included in the daily key exchange system, managed by the European Commission. Only Member States of the European Union that meet the relevant data protection criteria can participate in such cross-border data exchange. More detailed information on such cooperation between Member States, as well as other technical details can be found in the European Commission Decision, i.e. Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of information between national contact tracing and alert applications in relation to the fight against the COVID-19 pandemic - https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj.

For the purpose of operating the mobile App and other mobile App of the Member States of the European Union, randomly assigned daily keys, that are transmitted from server in the Republic of Slovenia, are stored on the European Central Server (EFGS).

The European Commission, as the provider of technical and organizational solutions for the cross-border exchange of data, is considers a controller within the meaning of the provisions of the General Data Protection Regulation and is committed to data protection as set in the contract or relevant legal acts. The above-mentioned European Commission Decision lays down rules on the processing carried out by the European Commission as a processor.

c. Using the App only for information purposes
TAs long as you use the App for information purposes only, i.e. do not use any of the App features mentioned above and do not enter any data, then processing only takes place locally on your smartphone and no personal data is generated. Websites linked in the app, such as https://gov.si/en/ostanizdrav, will open in your smartphone’s standard browser. The data processed here depends on the browser used, your browser settings, and the data processing practices of the website you are visiting.

9. What permissions and features does the App require?

The App requires access to a number of your smartphone's features and interfaces. For this purpose, you need to grant the App certain permissions. Permissions are programmed differently by different manufacturers. For example, individual permissions may be combined into permission categories, where you can only agree to the permission category as a whole. Please note that if the App is denied access, you will not be able to use any or all of the App's features.

a. Technical requirements (all smartphones)

- Internet

The App requires an internet connection for the exposure logging feature, and so that it can receive and transmit test results, so that it can communicate with the App's server system.

- Bluetooth

Your smartphone's Bluetooth interface must be enabled for your smartphone to log transmit codes from other smartphones and store them in the device's exposure log.

- Background operation

The App runs in the background (i.e. when you are not actively using the App) in order to be able to automatically assess your risk. If you deny the App permission to run in the background in your smartphone's operating system, then the App will not function properly.

b. Android smartphones

If you are using an Android device, the following system features must also be enabled:

- COVID-19 Exposure Notifications

The App's exposure logging feature requires this functionality. Otherwise, no exposure log with the transmit codes of your contacts will be available. The functionality must be enabled within the App to allow the App to access the exposure log.

- Location

Your smartphone's location service must be enabled for your device to search for Bluetooth signals from other smartphones. Please note that no location data is collected in this process.

- Notification

The user is notified locally of the assessed risk of infection. The necessary notification function is already enabled in the operating system.

c. iPhone (Apple iOS) smartphones

- COVID-19 Exposure Logging

The App's exposure logging feature requires this functionality, otherwise no exposure log with the transmit codes of your contacts will be available. The functionality must be enabled within the App to allow the App to access the exposure log.

- Notifications

The user is notified locally of the assessed risk of infection. Notifications must be enabled.

10. When will data be deleted?

All data stored in the App is deleted as soon as it is no longer needed for the App features:

a. Exposure logging

- The list of transmit codes of users will be automatically deleted from your smartphone’s exposure log after 14 days.
- The NIJZ in MJU have no way of influencing the deletion of contact data in your smartphone’s exposure log (including your own transmit codes) and contact data on other smartphones, as this functionality is provided by Apple or Google. In this case, the deletion depends on what Apple or Google has determined. Currently, the data is automatically deleted after 14 days. It may also be possible, using the functionality provided by Apple and Google, to manually delete data in your device’s system settings.
- The risk status displayed in the App will be deleted as soon as a new risk status has been assessed. A new risk status is usually determined after the App has received a new list of transmit codes.

b. Notifying other App users or users of the other mobile App of the Member States of the European Union of your infection

- Your smartphone’s own transmit codes which are shared in the App will be deleted from the server system in Republic of Slovenia after 14 days, from the European Central Server (EFGS) in accordance with the rules of the operator.
- The complied value of TAN stored on the server system will be deleted after 21 days.
- The TAN stored in the App will be deleted after the test result has been shared.
- The TeleTAN stored in the App will be deleted after the test result has been shared.
- The TeleTAN stored on the server system will be deleted after 21 days.
- The TeleTAN received by the epidemiological service will be deleted there immediately after it has been passed on to you by telephone.
- The token stored on the server system will be deleted after 21 days.
- The registration token stored in the App will be deleted after the information of infection has been shared.

11. Who will receive your data?

If you wish to notify other users of App or users of the other mobile App of the Member States of the European Union of your infection, your transmit codes from the last 14 days will be passed on to the infected keys server and the to the App on other users’ smartphones.

12. Is data transferred to a third country?

If you enable exposure logging for warning other users of mobile App, it can create communication between Apps regardless where you are – for example, vacation abroad, business trip. Otherwise, the data created during the use of the App is processed on servers in the Republic of Slovenia and the European Central Server (EFGS) provided by European Commission for the purpose of connecting back-end systems of Member States European Union and are subject to strict rules of the General Data Protection Regulation.

13. Your other rights under the Personal Data Protection Act and General Data Protection Regulation

Since the use of the #OstaniZdrav App is a processing that does not require the identification of an individual, certain rights of an individual under Article 11 of the General Data Protection Regulation are not guaranteed. However, since it is not necessary for the purposes of the App and is not intended to do so, the NIJZ and MJU are not obliged to collect additional data (in accordance with the second paragraph of Article 11 of the General Data Protection Regulation). In addition, this would run counter to the stated objective, which aims at minimizing the amount of data processed for the application. More specifically:

- Information relating to the processing of personal data – general information on the processing of data can be obtained from the NIJZ and MJU websites, and information linked to an individual will not be provided due to the absence of an appropriate personal identifier;
- Right to rectification – the right to rectification will not be possible, as both the individual and the controller will not know which information relates to it at all and, as a result, will not be able to identify the error;
- Right to deletion – deletion of personal data will only be possible from the application installation, under which the individual will be able to delete all data generated in the context of the operation of the application;
- The right to restriction of processing and the right to object – the right to limit processing will be exercised by the individual if he proves that he is the holder of a specific randomly determined daily key for which the data on infection are to be protected. Due to the functioning of the application in such a way that the individual contact information is only local on a mobile phone, the right to limit processing because this processing does not require identification will not be possible In this part. The right to object may not be exercised otherwise than in the part in which the data are processed locally, by deleting them.
- E-mail address of the data protection officer:
  - with the NIJZ: vop@nijz.si
  - with the MJU: dpo.mju@gov.si.
- Information on the existence of automated decision-making, including profiling: the NIJZ and MJU shall not carry out profiling or automated decision-making based on profiling with personal data.
- Information on the right to lodge a complaint with the supervisory authority: You can submit your complaint to the Information Commissioner, Dunajska cesta 22, 1000 Ljubljana, e-mail address: gp.ip@ip-rs.si, website: www.ip-rs.si.

This shall also apply to the European Commission providing the European Central Server (EFGS) and to the competent national authorities of official bodies of the Member States, which have been acceded to cross-border exchange of information under condition, if you enable exposure logging. Any claims relating to exercise of the rights of individuals in accordance with the General Data Protection Regulation relating to another Member States or the European Commission may be forward directly to the controller in the Republic of Slovenia; however, you can also contact the Member State's controller or the European Commission (contact details of the Commission's Data Protection Officer – so-called DPO: data-protection-officer@ec.europa.eu)

14. Statistics

For the purpose of statistics, data on the number of issued teleTAN codes and the number of used teleTAN codes are periodically published from the verification server. The data is retrieved from the stored condensed values on the verification server. The data are published on the gov.si website, and the entire statistics on the OPSI portal. Data on the number of downloads of the application from Google play and Apple store are also published on the gov.si website, and the entire statistics on the OPSI portal.

Last change: 3 February 2021