‘Korona Stop LT’ Privacy Policy

Revised on 5 May 2021

The Privacy Policy specifies what data and for what purpose is collected when you use ‘Korona Stop LT’ App, and defines your rights under legal acts on the personal data protection applicable in the Republic of Lithuania.

We have developed our Privacy Policy in as clear format as possible, almost free from technical details to make it easily understandable for all users.

CONTENT

1. WHO DESIGNED THE APP?

'Korona Stop LT' (hereinafter – the App) has been designed on instruction of the Ministry of Health of the Republic of Lithuania (hereinafter – the MoH) and was commissioned by the National Public Health Centre under the Ministry of Health (hereinafter – the NPHC). In observance of legal acts on personal data protection, the MoH monitors compliance with the data processing rules and is the personal data controller, i.e. the MoH gives instructions on personal data processing. You may contact the Data Protection Officer of the MoH at the address: Vilniaus St. 33, LT-01506, Vilnius, Lithuania (addressing the letter to the Data Protection Officer of the MoH) or by email: duomenu.apsauga@sam.lt.

The data security of the App and the implementation of your rights (under the General Data Protection Regulation[1] (hereinafter – the GDPR) shall be ensured by the NPHC on behalf of the MoH. You may contact the Data Protection Officer of the NPHC at the address: Kalvarijų St. 153, LT-08221, Vilnius, Lithuania (addressing the letter to the Data Protection Officer of the NPHC) or by e-mail:

duomenu.apsauga@nvsc.lt.

2. USE OF THE APP IS VOLUNTARY

The installation and use of the App is voluntary. Data processing is carried out only with your consent by active actions of the installation and use of the App. In order to use the exposure logging function, you shall have to give your consent for the processing of your personal data in the App. To give your consent you shall activate the exposure logging function upon installation of the App.

By activating the exposure logging function you express your consent that your access, proximity, and, if relevant, health data (only the data on the potential risk to get infected with COVID-19 if it is identified by the App) is processed in this App, the App's Server System and The European Federation Gateway Service (EFGS). If you disagree, the App shall not use the information contained in your smartphone's 'Exposure log'. You can disable the exposure logging function at any time using the button provided in the App. In this case, you shall use the App's functionalities for informational purposes only.

Your consent is also required for data processing when you want to share the fact of becoming infected with Coronavirus (COVID-19) with other users of the App and European contract tracing apps that are connected to the EFGS. By choosing to report the infection with COVID-19, you give your consent to the processing of data on the fact of getting infected with Coronavirus (COVID-19).

3. WHAT IS THE LEGAL BASIS OF DATA PROCESSING?

The personal data processed by means of the App's tools shall be processed by the MoH on the basis of consent specified under Article 6(1)(a) and Article 9(2)(a) of the GDPR which you can withdraw at any time. For more information on the right to withdraw consent and the instructions of its implementation see paragraph 11.

4. TO WHOM IS THE APP INTENDED?

The App is intended for the Lithuanian residents from 16 years of age.

5. WHAT PERSONAL DATA ARE PROCESSED?

[1] Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

The App has been designed so as to use as little personal data as possible. This means that the App shall not collect data enabling the MoH or other users to identify you, your state of health or location.

The data processed by the App can be attributed to the following groups:

5.1. Access data

Your smartphone shall generate the access data when you use or turn on:

- Exposure logging function;
- Function of transmitting a notification on becoming infected with COVID-19.

The access data includes the following:

- IP address;
- Data transmission date and time of transmission (time stamp);
- Size of transmitted data (in bits);
- Successful data transmission–receipt stamp.

These data shall be processed for the technical infrastructure protection and maintenance purposes. The user shall not be identified. The App does not allow creating a user profile. At the time of data receipt from the App's server the IP address is encrypted and is not stored on the App's server and is not used further.

5.2. Proximity data, pseudonymised data of the infected person

If you enable the exposure logging function in your smartphone's operating system which allows tracking your presence in close proximity to other users of the App, your phone shall keep sending randomly generated keys (hereinafter – random IDs) by means of the Bluetooth Low Energy technology received by other smartphones which are nearby and the aforementioned function of which is enabled. Meanwhile, your smartphone shall receive the keys sent by them. In addition to random IDs, the following data shall be recorded and stored on your phone during the exposure logging:

- Date and time;
- Duration;
- Bluetooth signal strength;
- Encoded metadata (protocol version and transmission strength).

Your phone shall log the random IDs sent by your smartphone, incoming keys, and other proximity data (date, time, duration, signal strength and encrypted metadata) in the 'Exposure Log' and store for 14 days.

The exposure logging function in the settings of smartphones with Android operating system is designated as 'COVID-19 location notifications' and in smartphones running iOS operating system – as 'Exposure notifications'. This function is not a part of the App, but is integrated in smartphones, i.e. it is provided by Apple (iOS) or Google (Android) and is accordingly subject to the security policy provisions of these companies. The MoH has assessed the conformity of services provided by these companies with the privacy requirements, but has no possibility to control this and, therefore, shall not be responsible for data processed by operating systems in respect of enabling the exposure logging function on the smart device.

For more information on exposure logging functionality in Android operating system you can visit: https://support.google.com/android/answer/9888358?hl=en.

For more information on exposure logging functionality in iOS operating system is Android operating system see your smartphone's settings (Settings > *Exposure Notifications)*. Please note that this function is available only in iOS 13.5 release and its later versions.
When the exposure logging function is activated, the App shall process only the above referred data generated and stored by smart your phones as described above.

5.3. HEALTH DATA

The health data processed in the App include the fact of becoming infected with Coronavirus (COVID-19) and the information about the risk identified for you.
The health data shall be processed, if:

- you have voluntarily shared the fact of becoming infected with Cronavirus (COVID-19) in the App;
- the exposure logging function is used to determine the fact of being in close proximity to the infected person.

The App contains a link to a questionnaire on the NPHC website which you can fill out when you receive an increased exposure notification if you want an NPHC specialist to contact you and advise you on the need for self-isolation.

6. FUNCTIONS OF THE APP

6.1. EXPOSURE LOGGING FUNCTION

The App's main function is to log the presence of mobile App users close to each other. These data help assess your risk of infection and, on their basis, provide you with relevant information and recommendations for further action.

Having turned on the exposure logging function with the App running in the background mode, the App shall perform a random ID search on the server system several times a day for users who have shared the fact of getting infected with Coronavirus (COVID-19). These random IDs keys shall be transmitted by the App to the exposure logging function of the smartphone, with the help of which the codes shall be compared with the information stored in the 'Exposure Log' on your smartphone. If any overlapping data are found on your smartphone, the logged proximity data (date, duration, signal strength) shall be transmitted to the App.

The App shall analyse the 'Exposure Log' data and identify your personal risk of getting infected with Coronavirus (COVID-19). The research-based assessment algorithm shall determine how to interpret the proximity data (e.g., the risk of infection depends on the duration of being nearby and on the distance). Depending on the most relevant and recent scientific research, the MoH can update the settings of the assessment algorithm.

Your risk of infection with Coronavirus (COVID-19) shall be determined only on your smartphone, i.e. offline. The information on the identified risk shall not be transmitted to other users (including the MoH, the NPHC, Apple, Google and other parties).

6.2. FUNCTION OF NOTIFICATION ABOUT INFECTION WITH CORONAVIRUS (COVID-19)

For the purpose of performing its functions related to epidemiological diagnostics according to the procedure laid down by legal acts, the NPHC shall keep records on all cases of COVID-19 confirmed in Lithuania. These cases shall be processed in the Information System for Monitoring and Control of Communicable Diseases Likely to Spread and Pose Threat (hereinafter – ULSKIS), of which the App is a part.

If Coronavirus infection (COVID-19) has been confirmed for you, you shall be able to share this information anonymously in the App alerting other users this way. You can do this by entering the 10-digit case confirmation code (hereinafter – the diagnosis code) provided to you in the App. The diagnosis code shall be sent to you by SMS to the phone number provided by you to the NPHC staff during the interview. In order to use Coronavirus (COVID-19) Infection Notification function of the App, you shall have to inform the NPHC that you are using the App and want to receive the diagnosis code and specify the phone number to which this code should be sent by SMS. These data shall not be processed in the App and your phone number shall not be linked in any way to the data processed in the App.

If you use Coronavirus (COVID-19) Infection Notification function to alert other users, the App shall transmit random IDs generated and stored on your smartphone during the past 14 days to the App's server system. Firstly, this system shall check whether the diagnosis code is still valid and then shall add your random IDs to the list of random codes transmitted to the App's server system by other App users who have used Coronavirus (COVID-19) Infection Notification function. From that point on, your random IDs shall be received by other App users who also use the exposure logging function.

The diagnosis code must be used within 24 hours. If you don't use the diagnosis code issued to you within this time limit, you may be issued a temporary diagnosis code, which you can receive by calling +370 5 264 9676. The operator shall first ask you some questions to verify your personal identity. Such questions are necessary to prevent false reporting of infection and incorrect notification, as well as wrong determination of the risk status for other App's users. If the data provided are correct, you shall be asked to provide the phone number for sending to you the SMS with a temporary diagnosis code.

The diagnosis code shall be generated in the App's server system and sent to your specified phone number by SMS. After you enter the diagnosis code in the App, it will be sent back to the App's server system for validation. The App, in turn, shall receive from the server system a digital access key (tag) and shall store it. The App shall use the keys to request from the server system the information about the status of registered COVID-19 cases. This process shall be carried out without disclosing the content or other information which could allow the person's identification.

The diagnosis code is necessary in order to prevent the spread of false information on COVID-19 cases among users.

Please note that the App's users shall not be able to identify you when you use Coronavirus (COVID-19) Infection Notification function and, accordingly, you shall not be able to identify the persons who were in close proximity to you.

6.3. Use of the App solely for information purposes

If you use the App solely for informational purposes, i.e. do not use the functions described above and do not enter data, all data processed by the App shall remain only on your smartphone, the App shall not transmit any data to or receive them from other smart devices.

The websites linked with the App, e.g., http://koronastop.lrv.lt, shall open on your smartphone via your usual browser. Data presentation on the App shall depend on the type of the browser you use, its settings and the website's data processing principles.

7. What permissions and functions are needed for use of the App?

The App needs access to certain functions and interactions of your smartphone. For this purpose, you shall have to grant the App permissions that differ in various operating systems. For example, settings (permissions) may be grouped into the categories of settings (permissions), in which case you shall accept the use of the category. Please note that if you have not set the necessary permission in the App, you shall no longer be able to use one or all of the App's features.

7.1. TECHNICAL REQUIREMENTS (FOR ALL SMARTPHONES)

- Internet access

The exposure logging function requires internet access as it receives and transmits data about the fact of infection with Coronavirus (COVID-19), so the communication with the Application server system needs to be ensured.

- Bluetooth interface

Bluetooth connection has to be activated in order to receive random IDs from other smartphones and store them in the 'Exposure Log'.

- Background operation

When the App is used not actively, it shall operate in background mode and automatically search for random IDs for users who have shared the information about the fact of becoming infected with Coronavirus (COVID-19) and shall determine your risk level.

7.2. SMARTPHONES WITH ANDROID OPERATING SYSTEM

If you use a smartphone with Android operating system, you shall have to activate the following functions:

- Exposure logging

This function is necessary for the App's operation; if this function is not enabled the App shall not register that you were in close proximity to other users of the App and shall not notify you about the risk of infection with Coronavirus (COVID-19).

- Location

This function needs to be enabled in order for your smartphone to be able to locate Bluetooth signals from other devices. If the location function is not enabled, the App shall not be able to collect data from other App's users and shall not notify you about the risk of infection with Coronavirus (COVID-19). When this function is enabled, the GPS data about your physical location shall not be collected and stored.

- Receiving notifications

The function of receiving notifications is necessary if you want to receive in your App push notifications about the updated information on the risk of COVID-19. This notification function is already available in the operating system. If you do not want to receive the notifications, you can disable the function of receiving notifications through your phone's settings.

7.3. SMARTPHONES WITH IOS OPERATING SYSTEM

If your smartphone runs iOS operating system, the following features need to be enabled:

- Exposure logging

This function is necessary for operation of the App. If this function is not enabled the App shall not register that you were in close proximity to other users of the App and shall not notify you about the risk of infection with Coronavirus (COVID-19).

- Receiving notifications

The function of receiving notifications is necessary if you want to receive in your App push notifications about the updated information on the risk of COVID-19. This notification function is already available in the operating system. If you do not want to receive the notifications, you can disable the function of receiving notifications through your phone's settings.

8. When will the data be destroyed?

All data of the App shall be destroyed as soon as they become irrelevant for the performance of the App's functions.

8.1. Exposure logging function

- Random IDs of users who reported that they became infected with Coronavirus (COVID-19) shall be destroyed in the App immediately, and in the smartphone's exposure log – after 14 days.
- The MoH shall have no influence on the destruction of the proximity data in your phone (including your own random IDs) and the destruction of data in other smartphones, because this function is performed by Apple or Google. In this case, the destruction of data shall depend on the settings of Apple or Google. Currently, the data are destroyed after 14 days, but if Apple or Google function is used, you can delete manually the data in your phone settings.
- Once the level of infection risk is updated in the App, the previous data shall be deleted immediately; as a rule, this is done as soon as the App receives the list of new random IDs.

8.2. Function of notification about getting infected with Coronavirus (COVID-19)

- Random IDs of the user who has shared the fact of getting infected with Coronavirus (COVID-19) shall be stored in the App's server system for a maximum of 14 days and the older IDs shall be destroyed.
- The diagnosis code stored in the App shall be removed after notifying on becoming infected with Coronavirus (COVID-19).
- The diagnosis code stored in the server system shall be eliminated after 21 days.

9. Who will receive your data?

If you want to alert other users about becoming infected with Coronavirus (COVID-19), random IDs collected by you within the period of 14 days shall be sent to other users.

The MoH has tasked the NPHC with managing and the Information Society Development Committee – with overseeing the App's part of technical infrastructure (e.g., the server system). These two authorities shall process the data and act on behalf of the MoH (Article 28 of the GDPR).

The EFGS ensures the national contact tracing and warning applications interface and receives pseudonymised personal data of infected person (the infected person's keys, the country of origin of the keys, the related parties of the keys, and the information on confirmation of infection). These data shall be provided and received to ensure the interoperability of applications of such type between countries. The MoH acts as a joint

controller along with the other participating countries for the data processed in the EFGS. The responsibilities of the joint controller's are set in COMMISSION's IMPLEMENTING DECISION (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic Annex II (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1023&from=LT).

The list of the joint controller's is published here: https://ec.europa.eu/health/sites/health/files/ehealth/docs/gateway_jointcontrollers_en.pdf

The MoH may transfer to third parties the data collected in the process of using the App only when it has such legal obligation, e.g., when this is necessary for the purposes of criminal proceedings, in the event of the attack against the App's technical infrastructure. In other cases the data shall not be transmitted.

10. Are data transmitted to a third country?

The data stored in the App may be used only on servers of Lithuania and countries of the European Union or the European Economic Community.

11. Withdrawal of consent

You may withdraw at any time any consent given in the App's settings. Please note that the withdrawal of consent shall not affect the lawfulness of the data processing process carried out until the withdrawal.

To cancel the exposure logging function, you can disable the function in the App's settings or delete the App. If you want to use the exposure logging function again, you can turn it on or reinstall the App.

To withdraw consent to the processing of data on the fact of becoming infected with Coronavirus (COVID-19), you shall have to delete the App. In this case, all random IDs generated and stored on your smartphone shall be destroyed, and the App shall no longer be linked to your smartphone. If you want to report Coronavirus (COVID-19) infection again, you shall have to reinstall the App and to give consents again in order to access the default functions of the App.

You can also delete your random IDs from the 'Exposure Log' in the smartphone's settings. Please note that the App's user cannot delete the transferred random IDs contained in the random IDs list of the App's server system and other users' smartphones.

12. Other rights granted to you by provisions of data protection legal acts

If your data are processed by the MoH, you shall have the following rights:

- The rights established in Articles 15, 16, 17, 18, 20 and 21 of the GDPR. These rights of yours shall be implemented by the NPHC on behalf of the MoH;
- The right to contact the data protection officer of the MoH or NPHC and ask him questions (Article 38(4) of the GDPR);
- The right to lodge a complaint with a competent data protection authority. The competent supervisory authority shall be the State Data Protection Inspectorate, L. Sapiegos St. 17, LT-10312 Vilnius.

Requests of the App user to correct, delete, restrict management of personal data in the App, objections to management of the App data and to transferability of the data could not be carried out because there is no way to identify the user by pseudonymous personal data used in the App. For this reason, the App user cannot require to withdraw his (her) consent to manage his (her) pseudonymous personal data in the App.

Your rights shall be implemented by the NPHC on behalf of the MoH in accordance with the Description of procedure for implementing the data subject's rights in processing personal data in the registers and state information systems managed by the Ministry of Health of the Republic of Lithuania.

Updated on 5 May 2021