Privacy Policy
STOP COVID - ProteGO Safe

Most important information regarding your privacy

We have prepared this document to inform you how we process data in STOP COVID - ProteGO Safe, as well as what rights you are entitled to. Below you will find key information related to data processing occurring as part of our Application.

We have designed STOP COVID - ProteGO Safe in accordance with the Privacy by Default and Privacy by Design principles. This means that we apply the protection of your privacy by default and we have tried to limit the processing of information about you already at the stage of designing and creating the STOP COVID - ProteGO Safe application. We try not to obtain from you the information that would enable your identification (i.e. personal data), as we believe that effective pandemic prevention COVID-19 does not require the processing of personal data that identify the STOP COVID - ProteGO Safe Users.

The information processed by STOP COVID - ProteGO Safe does not allow your identification.

We will not have access to personal data that you enter into the STOP COVID - ProteGO Safe application. We will not take active steps to identify you. We will also not analyse how you use STOP COVID - ProteGO Safe.

Information entered into STOP COVID - ProteGO Safe related to the Triage (self-assessment of the risk of infection with COVID-19 - Triage Module) is analysed within STOP COVID - ProteGO Safe without leaving your device.

The functionality of analysing exposure to COVID-19 infection as a result of contact with other Application Users (Analytical Module) is voluntary. You have the option of analysing the potential exposure COVID-19 using Bluetooth technology for this purpose. If you decide to use this functionality, your Device will analyse the environment in which you are located in search of other Devices on which the Application is installed. If you encounter another Device on which the STOP COVID - ProteGO Safe Application is installed, information about this meeting will be saved in both Applications. Information about the meeting of two Devices with the Application installed remains on both of these Devices for no longer than 14 days, after which it will be deleted.

If your test COVID-19 will give positive result, a Contact Centre consultant will call you to inform you about the positive result of the test. Then the Contact Centre consultant will ask you if you have the STOP COVID - ProteGO Safe application installed. If this is the case, the Contact Centre consultant will offer you to notify other Users that they have stayed near the Device of a Person Tested Positive COVID-19 within the last 14 days, by providing you a PIN Code. The PIN Code confirms that your Device is a Device of a Person Tested Positive COVID-19. This confirmation is encrypted, and neither we nor other Users will be able to distinguish individual Devices and assign specific Users to them. After entering the PIN Code, the process of sending the encrypted Key to the STOP COVID - ProteGO Safe server, and then to the Devices of other Users, will be initiated in order to analyse the risk of COVID-19 infection. Entering the PIN Code to the Device is voluntary.

The Key sent from your Device to the STOP COVID - ProteGO Safe Server will not contain any data enabling identification or information about the Devices you have had contact with. It is up to you to decide whether you want to mark your Device as a Device of a Person Tested Positive, which will initiate the sending of an encrypted Key to the STOP COVID - ProteGO Safe Server, and then to other Application Users. Each Application, after receiving the Key, performs an automatic analysis of meetings by appropriate comparison of the received Key with the history of meetings of Devices with the installed Application from the last 14 days.

The analysis is performed independently on the Device of each User, it takes into account in particular the Users' distance (signal strength) and the time of staying in the vicinity of an infected person and as a result the status of the current risk group may be changed.

§1.
General provisions

1. This Privacy Policy sets out the rules for the collection, processing and protection of Users' Personal Data in connection with the use of the STOP COVID - ProteGO Safe application. Neither the Chief Sanitary Inspector (GIS) nor the Ministry of Digital Affairs (MC) identifies STOP COVID - ProteGO Safe Users.
2. The controller of User Data is the Chief Sanitary Inspector based in Warsaw, at ul. Targowa 65, 03–729 Warsaw.
3. By downloading STOP COVID - ProteGO Safe from the Play Store or the AppStore and installing it, the User gives the consent referred to in Article 173 paragraph 1 point2 of the Telecommunications Law; the Terms & Conditions and the Privacy Policy constitute the information referred to in Article 173 paragraph 1 point1 of the Telecommunications Law.
4. This document is prepared on the basis of the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data and the repeal of Directive 95/46/EC (General Regulation on Data Protection), the Act of 10 May 2018 on the protection of Personal Data (Journal of Laws of 2018, item 1000) and other generally applicable provisions.
5. The Data Controller has appointed a data protection officer. You can contact the data protection officer in all matters relating to the processing of personal data by the Data Controller and the exercise of rights related to the processing of such data. The Data Protection Officer is Renata Wągrodzka with whom you can contact via the e-mail address: iod@gis.gov.pl
6. If you have general questions regarding privacy, as well as questions regarding this Privacy Policy, please contact us at: protego@mc.gov.pl or iod@gis.gov.pl.
7. GIS ensures that it makes every effort to make the STOP COVID - ProteGO Safe Application ensure the highest standard of Users' privacy protection, and in particular ensures that it has taken all legal and technologically possible measures aimed at securing Users' privacy.
8. GIS declares that it uses technical and organisational measures to ensure the protection of Users' privacy, which are appropriate to the threats and categories of information protected, in particular, it uses encryption and protects information against disclosure to unauthorised persons, removal by an unauthorised person, processing in violation of the law as well as alteration, loss, damage or destruction.
9. In the event of consenting to Interoperability, the User should read the Appendix 1 to this Policy, which sets out the rights and obligations of the Joint Controllers and Users in connection to Interoperability. Annex 1 constitutes Annex 2 to the Commission 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.

§2.
Definitions

Whenever the Privacy Policy mentions:

1. **Analytical Module**- it is understood as the STOP COVID - ProteGO Safe functionality that enables saving, creating history and analysing the meeting of the User's Device with other Application Users' Devices. The Analytical Module is based on the Privacy-Preserving Contact Tracing API developed and made available by Google and Apple. The information generated by the Analytical Module along with the results of its work is stored locally on the Device for 14 days. Google and Apple in their documentation, which can be found here: exposurenotifications oraz exposurenotification ensure that they apply the highest security standards to protect Users' privacy.
2. **Contact Centre**- it is understood as the unit providing the test result by phone COVID-19, transmitting the PIN Code to the Application Users and providing information related to COVID-19.
3. **Current restrictions in poviats** - it is understood as the STOP COVID - ProteGO Safe functionality that allows you to display in the Application information about areas (poviats) covered by special safety rules introduced due to the pandemic COVID-19 based on the relevant and current ordinance on the establishment of certain restrictions, prohibitions and limitations in connection with the state of epidemic as well as the amending regulations;
4. **Device**- it is understood as an electronic device through which the User gains access to STOP COVID - ProteGO Safe (tablet, smartphone, etc.) with an active Bluetooth module, Android 5.0 or higher with access to the Google Play store or with an iOS system in a version not lower than 13.5 with access to the AppStore. The Analytical Module will work only on Devices with Android 6.0 supporting BLE technology or higher, or with an iOS version 13.5 or newer.
5. **Federation Gateway** - it is understood as a network gateway operated by the European Commission using a secure IT tool, which is used to receive, store and share a minimum set of Personal Data between European Union Member States backend servers for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications. The Federation Gateway enables Interoperability. Thanks to the Federation Gate, it is possible to send and receive Keys between the User and users of other national contact tracing and warning mobile applications, similar to STOP COVID - ProteGO Safe. Keys shipped are through the Federation Gate and the retention period for the Keys is 14 days;
6. **GDPR**- it is understood as the 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).
7. **GIS**- it is understood as the Chief Sanitary Inspector based in Warsaw, at ul. Targowa 65, 03–729 Warsaw. GIS is the controller of personal data within the meaning of the GDPR in relation to the personal data of STOP COVID - ProteGO Safe Users. GIS independently determines the purposes and methods of processing Personal Data within STOP COVID - ProteGO Safe.
8. **Health Diary Module**- it is understood as the STOP COVID - ProteGO Safe notepad-like functionality, enabling the User to record information about their health. Personal Data entered into the Health Diary Module are stored locally on the User's Device.

9. **Interoperability or Alerts in Europe** - it is understood as the STOP COVID - ProteGO Safe functionality that enables the exchange of Keys between the User and users of other contact tracing and warning mobile applications, similar to STOP COVID - ProteGO, which are supported by other Member States of the European Union and cooperate within the Federation Gateway. Thanks to Interoperability, Users can receive information about the potential exposure to infection in connection with the potential contact with users of other contact tracing and warning mobile applications, similar to STOP COVID - ProteGO Safe;
10. **Joint controllers** - it means health authorities responsible for controlling contact tracing and warning mobile applications similar to STOP COVID - ProteGO Safe that they use from the Federation Gateway. Details on the cooperation between the Joint Controllers are set out in Annex No. 1 in accordance with Annex No. 2 to the Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 in the field of cross-border data exchange between national mobile applications for to establish infectious contacts and alert in relation to fighting the COVID-19 pandemic. The list of Joint Controllers along with information about the processing of Personal Data by them of the User who has consented to Interoperability is available here: https://ec.europa.eu/health/ehealth/covid-19_en
11. **Key** - it is understood as a randomly generated, periodic and alphanumeric string of characters sent to the STOP COVID - ProteGO Safe Server, which contains encrypted Personal Data, initiating the process of analysis of exposure to infection COVID-19 as part of the Analytical Module. The Key is transferred to the STOP COVID - ProteGO Safe Server after the Person Tested Positive enters the PIN Code into the Application.
12. **MC**- it is understood as the Minister of Digital Affairs based in Warsaw, at Aleje Ujazdowskie 1/3, 00-583 Warsaw. Based on an agreement concluded with GIS, MC supports GIS in the development and maintenance of STOP COVID - ProteGO Safe.
13. **Person Tested Positive**- it is understood as a natural person with full legal capacity, who has been tested positive for the COVID-19. The Person Tested Positive does not have to be a User.
14. **Personal Data**- it is understood as any information relating to an identified or identifiable natural person within the meaning of Article 4 point 1 of the GDPR. The Processing of Personal Data in STOP COVID - ProteGO Safe shall be governed by Article 11 of the GDPR, as the purpose of processing does not require identification, therefore STOP COVID - ProteGO Safe Users are not identified.
15. **Processing**- it is understood as an operation or a set of operations, which are performed on personal data or sets of personal data in an automated or non-automated manner, such as collecting, recording, organizing, structuring, storing, adapting or modifying, downloading, browsing, using, disclosing through sending, distributing or sharing in any other way, alignment or combination, restriction, erasure or destruction.
16. **PUSH notification** - it is understood as a text message sent by the STOP COVID - ProteGO Safe Server, which will be displayed on the screen of the User's Device, regardless of whether the Application is turned on or not. The content of PUSH notifications will be directly related to the development of the SARS-CoV-2 virus pandemic or the Application itself and will be determined each time by the Chief Sanitary Inspector (GIS) or the Ministry of Digital Affairs (MC).

17. **STOP COVID - ProteGO Safe or Application**- it is understood as the STOP COVID - ProteGO Safe application, which includes the Analytical Module, the Triage Module and the Health Diary Module, and also supports the prophylaxis and prevention of infection, transmits important information related to the pandemic COVID-19 and reminds about safe behaviours and daily hygiene habits.
18. **STOP COVID - ProteGO Safe Server**- it is understood as the cloud infrastructure maintained by the National Cloud Operator, used to transmit the Key to Users' Devices. Keys are stored on the STOP COVID - ProteGO Safe Server in an encrypted form for 14 (fourteen) days.
19. **Terms & Conditions**- it is understood as the document that specifies the terms of use of STOP COVID - ProteGO Safe, as well as the rights and obligations of GIS, MC and Users.
20. **Test PIN code** - it is understood as a randomly generated alphanumeric password active for half an hour from the moment of generation, which is provided to the User by the Contact Centre consultant. The Test PIN code is provided to the User who has a high risk of exposure to infection COVID-19 generated by the Analytical Module and high risk of exposure to infection COVID-19 confirmed by the Triage Module;
21. **Triage Module**- it is understood as the STOP COVID - ProteGO Safe functionality that allows the User to perform a self-assessment of the risk of exposure to infection COVID-19, based on the WHO questionnaire. Personal Data entered into the Triage Module are stored locally on the User's Device.
22. **User**- it is understood as a person with full legal capacity who, after accepting the Terms & Conditions and the Privacy Policy, uses STOP COVID - ProteGO Safe.
23. **WHO** - it is understood as the World Health Organization.

§3.
General rules

1. The Processing of Personal Data in STOP COVID - ProteGO Safe shall be governed by Article 11 of the GDPR, as the purpose of processing does not require User identification. When designing the STOP COVID-ProteGO Safe technical security measures, GIS and MC exercised due diligence to prevent identification of Users. However, due to the fact that the User's Personal Data is processed locally as part of the Application, despite the lack of access to it by GIS as the data controller, the Regulation still applies.
2. Personal Data is processed solely for the purpose of supporting the public in preventing the spread of the pandemic COVID-19: acting in the broadly understood public interest, the controller, by distributing and ensuring the operability of the STOP COVID - ProteGO Safe application, supports the rapid exchange of information between natural persons within a specific community, acting for the prevention of public health and counteracting the spread of SARS CoV-2 virus and disease COVID-19, through the exchange of encrypted information on infected persons and software enabling the analysis of meetings and contacts, as well as through algorithms enabling the assessment of the risk of infection.
3. Personal Data is processed on the basis of **Article 6, paragraph 1, letter e, of the GDPR** in connection with a task carried out in the public interest consisting in preventing, counteracting and combating COVID-19 resulting from Article 1, 2, 3, 6

and 8a paragraph 1, 4 and 5 of the Act of 14 March 1985 on the State Sanitary Inspection (Journal of Laws of 2019, item 59).

4. Personal Data regarding the User's health is also processed on the basis of **Article 9, paragraph 2, letter i of the GDPR** in connection with the public task of preventing, counteracting and combating COVID-19 resulting from Article 1, 2, 3, 6 and 8a paragraph 1, 4 and 5 of the Act of 14 March 1985 on the State Sanitary Inspection (Journal of Laws of 2019, item 59), because processing is necessary for reasons related to the public interest in the field of public health, such as protection against serious cross-border health threats under the law of the Member State.
5. STOP COVID - ProteGO Safe processes Personal Data that does not require identification as provided for in Article 11 of the GDPR. Neither GIS nor MC are able to identify the data subject (User). GIS adheres to the following Personal Data Processing principles:
    1) it implements appropriate technical and organizational measures so that the processing of data about the Application Users takes place in an encypted manner without their identification in accordance with the provisions on Personal Data protection and to be able to demonstrate it;
    2) it supervises the security of Personal Data throughout the entire period of their possession in a manner ensuring, in particular, protection against unauthorised access, damage, destruction or loss;
    3) it keeps confidential information about the User through the use of encryption;
    4) it maintains the confidentiality of Personal Data;
    5) it provides data subjects with the possibility to make use of their rights under the law.
6. GIS may process the following Personal Data:
    1) Data related to the use of the server that provides messages to the Users:
        a. **UID**– random designation of the User that prevents identification,
        b. Average time of using the Application by Users (statistical data that cannot be linked to individual Users).
    2) Statistical data from application stores, i.e. GooglePlay Store and Apple AppStore, which cannot be associated with individual Users (statistical data):
        a. Information about the installation, last use and removal of the Application;
        b. Location where the User was while installing the Application (city or country specification);
        c. User Device Models;
    3) Data stored only locally on Devices, regardless of the Device's operating system. The following data are not transferred outside the User's Device, in particular they are not processed by GIS or MC:
        a. User ID,
        b. History of entries in the Health Diary,
        c. History of entries in the Triage Module,
        d. Temporary_exposure_keys_upload_status - information whether the transfer of information as part of the Analytical Module was successful or not,
        e. information about whether the Application is launched for the first time,

f. information about the Internet connection,
g. information whether the User has given their consent to push notifications in the Application,
h. information on whether the User has granted the Application an authorisation necessary for the operation of the Analytical Module,
i. information on whether the device's Bluetooth module is turned on,
j. Information about the status, activation and operation of the Analytical Module,
k. Information about the Application status (whether it is running in the foreground or in the background),
l. Information deleted after 14 days:
    I. history of the Analytical Module analysis results from the last 14 days,
    II. period of contact of Users' Devices, values in the range of 5-30 minutes,
    III. date of contact of the Users' Devices.

4) Data transferred to other Devices via the STOP COVID - ProteGO Safe Server:
    a. Key - contains key information, rollingPeriod, rollingStartNumber, and transmissionRisk (exact information can be found here)
    b. region of the Application's operation (Poland);
    c. information that the Key is related to the STOP COVID - ProteGO Safe application;
    d. confirmation that the PIN Code is correct.
5) A cookie containing the User's UID, transferred to Cloudflare Inc. in order to prevent DDOS attacks and ensure the highest standards of user security. The cookie file referred to in this point does not enable profiling or monitoring of the User's behaviour on various websites (cross-site tracking). More information regarding the security of this solution is available here: https://support.cloudflare.com/.
6) Information disclosed indirectly by the User to the Chief Sanitary Inspector in connection with the verification of the correctness of the Test PIN Code:
    a. status of high risk of exposure to infection COVID-19 generated by the Analytical Module;
    b. status of a person with high risk of exposure to infection COVID-19 generated by the Triage Module;
7) The data exchanged and processed through the Federation Gate as part of Interoperability includes the following information:
    a. Keys provided by STOP COVID - ProteGO Safe and other national contact tracing and warning mobile applications similar to STOP COVID - ProteGO Safe, up to 14 days prior to the date of upload of the Keys;
    b. key log data in accordance with the technical specification protocol used in the country of origin of the Keys
    c. verification of the infection;
    d. countries of interest to the User and the country of origin of the Keys.

7. Providing Personal Data referred to in paragraph 5 point 3 of this section is voluntary, but may condition the use of all the STOP COVID - ProteGO Safe functionalities.

8. STOP COVID - ProteGO Safe enables sending and receiving Keys between STOP COVID - ProteGO Safe Users and users of other national contact tracing and warning mobile applications similar to STOP COVID - ProteGO Safe, which use the Federation Gateway. Interoperability (Alerts in Europe) is voluntary and its use is based on the User's consent expressed pursuant to Art. 9 paragraph 1 lit. a GDPR. Interoperability is provided through the Federation Gateway. In order to use Interoperability effectively, you must give your consent. The consent expressed by the User applies to sending and receiving Keys for all mobile applications similar to STOP COVID - ProteGO Safe. The consent may be withdrawn at any time, without affecting the sent and received Keys that were sent or received before the consent was withdrawn. After giving consent, the Keys are sent to national contact tracing and warning mobile applications similar to STOP COVID - ProteGO Safe. The history of devices on which an application similar to STOP COVID - ProteGO Safe is installed, will be stored at the Federation Gateway for 14 days.
9. Recipients of Personal Data from STOP COVID - ProteGO Safe:
    1) to the extent specified in §3 paragraph 4 point1, 2 and 4 may include entities that cooperate with GIS for the purpose of the development and maintenance of STOP COVID - ProteGO Safe:
        a. MC responsible for supervising the development and maintenance of STOP COVID - ProteGO Safe, i.e. the Minister of Digital Affairs based in Warsaw, at ul. Królewska 27, 00-060 Warsaw, e-mail: mc@mc.gov.pl;
        b. the entity responsible for the maintenance of the STOP COVID - ProteGO Safe application, as well as the performance of development and developer works on STOP COVID - ProteGO Safe commissioned by MC: TYTANI24 Spółka z ograniczoną odpowiedzialnością with its registered office in Wrocław, at ul. Ząbkowicka 55, 50-511 Wrocław (office address: ul.Kościerzyńska32A, Wrocław, 51-410), entered into the Register of Entrepreneurs of the National Court Register kept by the District Court in Wrocław, 6th Commercial Division of the National Court Register, under the number KRS 0000725465, REGON 369879064, NIP 8992843182, share capital paid in full in the amount of PLN 20,000;
    2) to the extent specified in §3 paragraph 4 point 1, 2 and 4 may include Operator Chmury Krajowej Sp. z o. o. as an entity providing infrastructure enabling downloading and updating STOP COVID - ProteGO Safe and maintaining the STOP COVID - ProteGO Safe Server. This entity also maintains the Google Firebase service that enables sending push notifications to Users - https://firebase.google.com;
    3) to the extent specified in §3 paragraph 4 point 5 may include: Cloudflare Inc. 101 Townsend St, San Francisco, CA 94107, USA in the scope of providing the service of preventing DDOS attacks and ensuring the highest standards of Users' security.
    4) to the extent specified in §3 paragraph 4 point 7 may include Joint Controllers and European Commission acting as processor.
10. STOP COVID - ProteGO Safe will only be active during the pandemic period COVID-19 and may be deactivated in accordance with the decision of the GIS. After stopping

the use of STOP COVID - ProteGO Safe, all Personal Data will be deleted along with the Application.

11. The User's Personal Data in the form of an anonymous UID address may be transferred outside the European Economic Area as regards the use of the service provided by Cloudflare in order to prevent DDOS attacks and ensure the highest standards of Users' security. Such transfer will also take place only in an exceptional situation, in particular when the User uses the Application outside the European Economic Area on basis of standard contractual clauses.
12. The processed Personal Data are not made available to the Recipients of Personal Data in a form that would allow the identification of the data subject.
13. The data referred to in §3 para. 6 point 6, related to the verification of the Test PIN Code are not disclosed to the Chief Sanitary Inspector directly, but only Users who have a double high-risk status indicated by both the Triage Module and the Analytical Module may verify the correctness of the Test PIN Code.
14. No decisions as part of STOP COVID - ProteGO Safe are made in an automated manner within the meaning of Article 22 of the GDPR. This means that the fact of using the Application does not result in issuing any decisions in relation to the User that could have a legal effect or similarly significantly affect the User.

§4.
Users' rights

1. The Processing of Personal Data in STOP COVID - ProteGO Safe shall be governed by Article 11 of the GDPR
2. Data subjects are entitled to:
    1. the right to access Personal Data based on Article 15 of the GDPR;
    2. the right to rectify Personal Data based on Article 16 of the GDPR;
    3. the right to delete Personal Data based on Article 17 of the GDPR;
    4. the right to request the Controller to limit the Processing of Personal Data based on Article 18 of the GDPR, subject to the cases referred to in Article 18 paragraph 2 of the GDPR;
    5. the right to object to the Processing of Personal Data based on Article 21 of the GDPR.
3. Exercising the rights referred to in paragraph 1 is possible by using the appropriate STOP COVID - ProteGO Safe functionalities.
4. STOP COVID - ProteGO Safe enables the User to exercise the right to delete Personal Data at any time:
    1. In order to delete Personal Data from the Triage Module, the Health Diary Module and other data entered by the User, select on the main screen of STOP COVID - ProteGO Safe the following: More, then My Data, then Manage Data, then Erase Data. After the User's confirmation, all data entered by the User will be irretrievably deleted.
    2. In order to delete Personal Data from the Analytical Module, the User has to:
        a. for devices with iOS version 13.5 or 13.6, select the following: System Settings> Privacy> Health> COVID-19 Exposure Logging> Delete Exposure Log;

b. for Devices with iOS version 14, select the following: System Settings> Exposure Notifications -> Delete Exposure Log;
c. for devices with Android system, select the following: Settings> Google> Notifications about the risk of exposure to COVID-19> Delete random identifiers; after the User's confirmation, all data related to the Analytical Module will be irretrievably deleted.

5. For any questions and requests related to Users' rights, please contact us at: protego@mc.gov.pl.
6. The User has the right to lodge a complaint with the President of the Personal Data Protection Office if they consider that the Processing of their Personal Data violates the provisions of the GDPR or generally applicable provisions. The complaint can be sent in writing to the following address: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2,00-193 Warszawa or electronically via the ePUAP portal.
7. The User has the right to withdraw consent to the operation of the Analytical Module at any time, but the withdrawal of consent will not affect the lawfulness of the actions performed prior to its withdrawal. To withdraw consent related to the Analytical Module:
    1. for Devices with iOS version 13.5 or 13.6, select the following: System Settings> Privacy> Health> COVID-19 Exposure Logging -> Disable Exposure Logging;
    2. for Devices with iOS version 14, select System Settings > Exposure Notifications > Disable Exposure Logging;
    3. for Devices with Android system, select the following: Settings -> Google -> Notifications about the risk of exposure to COVID-19 -> Disable Notifications about the risk of exposure; after the User's confirmation, the Analytical Module will cease to operate.
8. The User has the right to withdraw consent to being sent PUSH Notifications at any time, but the withdrawal of consent will not affect the lawfulness of actions performed prior to its withdrawal. Withdrawal of consent to being sent PUSH notifications doesn't affect notifications about high risk of exposure to infection COVID-19 generated by the Application's Analytical Module. In order to withdraw consent to being sent PUSH notifications:
    1. for devices with iOS, select the following: Settings -> ProteGO Safe Notifications -> Disable Notifications
    2. for Devices with Android system, select the following: Settings -> Applications -> Manage applications -> ProteGO Safe -> Disable Notifications; after the User's approval of the decision, PUSH notifications will no longer be sent.
9. The User has the right to withdraw the consent expressed pursuant to Article 173 paragraph 1 of the Telecommunications Law at any time, but the withdrawal of consent will not affect the lawfulness of actions performed before its withdrawal. To withdraw consent, the User has to remove STOP COVID - ProteGO Safe from the Device.

§5.
Final provisions

1. STOP COVID - ProteGO Safe may contain links to other websites. Such websites operate independently of GIS and are not supervised by it in any way. These websites sites may have their own privacy policies, which we recommend that the User should familiarise with.

2. GIS reserves the right to amend the Privacy Policy by publishing a new Privacy Policy on the STOP COVID - ProteGO Safe website.
3. When the SARS-CoV-2 virus pandemic or the pandemic threat ends, the STOP COVID - ProteGO Safe Application will be deactivated.

RESPONSIBILITIES OF THE PARTICIPATING MEMBER STATES AS JOINT CONTROLLERS FOR THE FEDERATION GATEWAY FOR CROSS-BORDER PROCESSING BETWEEN NATIONAL CONTACT TRACING AND WARNING MOBILE APPLICATIONS

SECTION 1

Subsection 1

Division of responsibilities

(1) The joint controllers shall process personal data through the federation gateway in accordance with the technical specifications stipulated by the eHealth Network ([1]).

(2) Each controller shall be responsible for the processing of personal data in the federation gateway in accordance with the General Data Protection Regulation and Directive 2002/58/EC.

(3) Each controller shall set up a contact point with a functional mailbox that will serve for the communication between the joint controllers and between the joint controllers and the processor.

(4) A temporary subgroup set up by the eHealth network in accordance with Article 5(4) shall be tasked to examine any issues arising from the interoperability of national contact tracing and warning mobile applications and from the joint controllership of related processing of personal data and to facilitate coordinated instructions to the Commission as a processor. Amongst other issues, the controllers may, in the framework of the temporary subgroup, work towards a common approach on the retention of data in their national backend servers, taking into account the retention period set forth in the federation gateway.

(5) Instructions to the processor shall be sent by any of the joint controllers' contact point, in agreement with the other joint controllers in the subgroup referred to above.

(6) Only persons authorised by the designated national authorities or official bodies may access personal data of users exchanged in the federation gateway.

(7) Each designated national authority or official body shall cease to be joint controller from the date of withdrawal of its participation in the federation gateway. It shall however remain responsible for processing in the federation gateway that occurred prior to its withdrawal.

Subsection 2

Responsibilities and roles for handling requests of and informing data subjects

(1) Each controller shall provide the users of its national contact tracing and warning mobile application ("the data subjects") with information about the processing of their personal data in the federation gateway for the purposes of cross-border interoperability of the national contact tracing and warning mobile applications, in accordance with Articles 13 and 14 of the General Data Protection Regulation.

(2) Each controller shall act as the contact point for the users of its national contact tracing and warning mobile application and shall handle the requests relating to the exercise of the rights of data subjects in accordance with the General Data Protection Regulation, submitted by those users or their representatives. Each controller shall designate a specific contact point dedicated to requests received from data subjects. If a joint controller receives a request from a data subject, which does not fall under its responsibility, it shall promptly forward it to the responsible joint controller. If requested, the joint controllers shall assist each other in handling data subjects' requests and shall reply to each other without undue delay and at the latest within 15 days from receiving a request for assistance.

(3)Each controller shall make available to the data subjects the content of this Annex including the arrangements laid down in points 1 and 2.

SECTION 2

Management of security incidents, including personal data breaches

(1)The joint controllers shall assist each other in the identification and handling of any security incidents, including personal data breaches, linked to the processing in the federation gateway.

(2)In particular, the joint controllers shall notify each other of the following:

a)any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing processing in the federation gateway;

b)any security incidents that are linked to the processing operation in the federation gateway;

c)any personal data breach, the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

d)any breach of the technical and/or organisational safeguards of the processing operation in the federation gateway.

(3)The joint controllers shall communicate any personal data breaches with regard to the processing operation in the federation gateway to the Commission, to the competent supervisory authorities and, where required so, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679 or following notification by the Commission.

SECTION 3

Data Protection Impact Assessment

If a controller, in order to comply with its obligations specified in Articles 35 and 36 of the General Data Protection Regulation needs information from another controller, it shall send a specific request to the functional mailbox referred to in Subsection 1(3) of Section 1. The latter shall use its best efforts to provide such information.