POLITYKA PRYWATNOŚCI
ProteGO Safe

Najistotniejsze informacje dotyczące Twojej prywatności

Przygotowaliśmy ten dokument, aby poinformować Cię jak przetwarzamy dane w ProteGO Safe, a także jakie prawa Ci przysługują. Poniżej znajdziesz kluczowe informacje związane z przetwarzaniem danych w ramach naszej Aplikacji.
Zaprojektowaliśmy ProteGO Safe zgodnie z zasadami Privacy by Default oraz Privacy by Design. Oznacza to, że domyślnie stosujemy ochronę Twojej prywatności i staraliśmy się ograniczyć przetwarzanie informacji o Tobie już na etapie projektowania i tworzenia aplikacji ProteGO Safe. Staramy się nie pozyskiwać od Ciebie informacji, które umożliwią Twoją identyfikację (tj. danych osobowych), gdyż wierzymy, że skuteczne zapobieganie pandemii COVID-19 nie wymaga przetwarzania danych osobowych, które identyfikują Użytkowników ProteGO Safe.

Informacje przetwarzane przez ProteGO Safe nie umożliwiają Twojej identyfikacji.

Nie będziemy mieli dostępu do danych osobowych, które wprowadzisz do aplikacji ProteGO Safe. Nie będziemy podejmowali aktywnych działań, aby Cię zidentyfikować. Nie będziemy także analizowali w jaki sposób korzystasz z ProteGO Safe.

Informacje wprowadzone do ProteGO Safe związane z Triażem (samooceną ryzyka zarażenia COVID-19 - Moduł Triażu) są analizowane w ramach ProteGO Safe bez opuszczania Twojego urządzenia.

Funkcjonalność analizowania narażenia na zarażenie COVID-19 w związku z kontaktem z innymi Użytkownikami Aplikacji (Moduł Analityczny) jest dobrowolna. Masz możliwość analizowania potencjalnego narażenia na zarażenie COVID-19 wykorzystując do tego celu technologię Bluetooth. Jeśli zdecydujesz się na korzystanie z tej funkcjonalności Twoje Urządzenie będzie analizowało otoczenie, w którym się znajdujesz, w poszukiwaniu innych Urządzeń na których zainstalowana jest Aplikacja. W przypadku spotkania innego Urządzenia, na którym zainstalowana jest Aplikacja ProteGO Safe w obu Aplikacjach zapisze się informacja o tym spotkaniu. Informacja o spotkaniu dwóch Urządzeń z zainstalowaną Aplikacją pozostaje na obu tych Urządzeniach nie dłużej niż przez 14 dni, po czym informacje te zostaną usunięte.

Jeśli Twój test na COVID-19 będzie miał wynik pozytywny zadzwoni do Ciebie konsultant Centrum Kontaktu, który poinformuje o pozytywnym wyniku testu. Następnie konsultant Centrum Kontaktu zapyta Cię, czy masz zainstalowaną aplikację ProteGO Safe. Jeśli tak będzie, konsultant Centrum Kontaktu zaproponuje Ci powiadomienie innych Użytkowników o tym, że przebywali w pobliżu Urządzenia Osoby Chorej na COVID-19 w ciągu ostatnich 14 dni, poprzez podyktowanie Ci Kodu PIN. Kod PIN ma na celu potwierdzenie, że Twoje Urządzenie, to Urządzenie Osoby Chorej na COVID-19. Potwierdzenie to ma charakter anonimowy, ani my, ani inni Użytkownicy nie będziemy w stanie rozróżnić poszczególnych Urządzeń i przypisać do nich konkretnych Użytkowników. Po wprowadzeniu kodu PIN zostanie zainicjowany proces przesłania anonimowego Klucza Diagnostycznego na serwer ProteGO Safe, a następnie do Urządzeń innych Użytkowników w celu analizy ryzyka zarażenia COVID-19. Wprowadzenie Kodu PIN do Urządzenia jest dobrowolne.

Klucz Diagnostyczny wysłany z Twojego Urządzenia na Serwer ProteGO Safe nie będzie zawierał danych umożliwiających identyfikację ani informacji o Urządzeniach, z którymi miałeś styczność. Ty będziesz decydować o tym, czy chcesz oznaczyć swoje Urządzenie jako Urządzenie Osoby Chorej, co zainicjuje wysłanie anonimowego Klucza Diagnostycznego na Serwer ProteGO Safe, a następnie do innych Użytkowników Aplikacji. Każda z Aplikacji, po otrzymaniu Klucza Diagnostycznego dokonuje automatycznej analizy spotkań poprzez odpowiednie porównanie otrzymanego Klucza

Diagnostycznego z historią spotkań Urządzeń z zainstalowaną Aplikacją z ostatnich 14 dni. Analiza wykonywana jest niezależnie na Urządzeniu każdego Użytkownika, brana jest w niej pod uwagę w szczególności odległość Użytkowników (siła sygnału) oraz czas przebywania w pobliżu osoby zakażonej i w jej wyniku może zostać zmieniony status aktualnej grupy ryzyka.

§1.
Postanowienia ogólne

1. Niniejsza Polityka Prywatności określa zasady zbierania, przetwarzania i ochrony Danych Osobowych Użytkowników w związku z korzystaniem z aplikacji ProteGO Safe. GIS ani MC nie identyfikują Użytkowników ProteGO Safe.
2. Administratorem Danych Użytkowników jest Główny Inspektor Sanitarny z siedzibą w Warszawie, ul. Targowa 65, 03–729 Warszawa.
3. Poprzez pobranie ProteGO Safe ze sklepu Play lub AppStore oraz zainstalowanie Użytkownik wyraża zgodę, o której mowa w art. 173 ust. 1 pkt. 2 Prawa Telekomunikacyjnego, a Regulamin oraz Polityka Prywatności stanowią informację, o której mowa w art. 173 ust. 1 pkt. 1 Prawa Telekomunikacyjnego.
4. Niniejszy dokument jest przygotowany w oparciu o przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem Danych Osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), ustawy z dnia 10 maja 2018 r. o ochronie Danych Osobowych (Dz.U. z 2018 r. poz. 1000) oraz innych przepisów powszechnie obowiązujących.
5. Administrator Danych powołał inspektora ochrony danych. Z inspektorem ochrony danych można kontaktować się we wszystkich sprawach dotyczących przetwarzania danych osobowych przez Administratora Danych oraz korzystania z praw związanych z przetwarzaniem tych danych. Inspektorem Ochrony Danych jest Renata Wągrodzka z którą możesz skontaktować się za pośrednictwem adresu e-mail: iod@gis.gov.pl.
6. W razie ogólnych pytań dotyczących prywatności, a także pytań dotyczących niniejszej Polityki Prywatności zachęcamy do kontaktu pod adresem: protego@mc.gov.pl lub iod@gis.gov.pl.
7. GIS zapewnia, iż dokłada wszelkich starań, by Aplikacja Protego Safe zapewniała najwyższy standard ochrony prywatności Użytkowników, a w szczególności zapewnia, iż podjął wszelkie przewidziane prawem i możliwe technologicznie środki zmierzające do zabezpieczenia prywatności Użytkowników.
8. GIS oświadcza, iż stosuje środki techniczne i organizacyjne zapewniające ochronę Danych Osobowych Użytkowników odpowiednią do zagrożeń oraz kategorii Danych Osobowych objętych ochroną, a w szczególności stosuje szyfrowanie oraz zabezpiecza Dane Osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§2.
Definicje

Ilekroć w Polityce Prywatności mowa o:

1) **Centrum Kontaktu** - rozumie się przez to jednostkę powiadamiającą telefonicznie o wyniku testu na COVID-19, przekazującą Kod PIN Użytkownikom Aplikacji i udzielająca informacji związanych z COVID-19.
2) **Danych Osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej w rozumieniu art. 4 pkt 1 RODO. Do Przetwarzania Danych Osobowych w ProteGO Safe zastosowanie znajduje art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji, zatem Użytkownicy ProteGO Safe nie są identyfikowani.
3) **GIS** – rozumie się przez to Głównego Inspektora Sanitarnego z siedzibą w Warszawie, ul. Targowa 65, 03–729 Warszawa. GIS jest administratorem danych osobowych w rozumieniu

RODO względem danych osobowych Użytkowników ProteGO Safe. GIS samodzielnie ustala cele i sposoby przetwarzania Danych Osobowych w ramach ProteGO Safe.

4) **Kluczu Diagnostycznym** - rozumie się przez to generowany losowo, okresowy i alfanumeryczny ciąg znaków przekazywany na Serwer ProteGO Safe, który zawiera zanonimizowane Dane Osobowe, inicjujący proces analizy narażenia na zarażenie COVID-19 w ramach Modułu Analitycznego. Klucz Diagnostyczny jest przekazywany na Serwer ProteGO Safe po wpisaniu do Aplikacji Kodu PIN przez Użytkownika będącego Osobą Chorą.
5) **MC** - rozumie się przez to Ministra Cyfryzacji z siedzibą w Warszawie, ul. Królewska 27, 00–060 Warszawa. MC w oparciu o porozumienie zawarte z GIS, wspiera GIS w rozwoju i utrzymaniu ProteGO Safe.
6) **Module Analitycznym** - rozumie się przez to funkcjonalność ProteGO Safe umożliwiająca zapisywanie, tworzenie historii oraz analizowanie spotkania Urządzenia Użytkownika z innymi Urządzeniami Użytkowników Aplikacji. Moduł Analityczny jest oparty o Privacy-Preserving Contact Tracing API wytworzone oraz udostępnione przez Google oraz Apple. Informacje generowane przez Moduł Analityczny wraz z wynikami jego pracy są przechowywane lokalnie na Urządzeniu przez 14 dni. Google oraz Apple w swojej dokumentacji, którą można odnaleźć tutaj: https://www.google.com/covid19/exposurenotifications/ oraz https://developer.apple.com/documentation/exposurenotification zapewniają, że stosują najwyższe standardy bezpieczeństwa, aby chronić anonimowość Użytkowników.
7) **Module Dziennik Zdrowia** - rozumie się przez to funkcjonalność ProteGO Safe o charakterze notatnika umożliwiającą Użytkownikowi odnotowywanie informacji o swoim stanie zdrowia. Dane Osobowe wprowadzane do Modułu Dziennik Zdrowia są przechowywane lokalnie na Urządzeniu Użytkownika.
8) **Module Triażu** - rozumie się przez to funkcjonalność ProteGO Safe umożliwiająca wykonanie przez Użytkownika samooceny ryzyka narażenia na zakażenie COVID-19, stworzona na podstawie kwestionariusza WHO. Dane Osobowe wprowadzane do Modułu Triażu są przechowywane lokalnie na Urządzeniu Użytkownika.
9) **Osoba Chora** - rozumie się przez to osobę fizyczną, posiadającą pełną zdolność do czynności prawnych, która uzyskała pozytywny wynik testu na COVID-19. Osoba Chora nie musi być Użytkownikiem.
10) **ProteGO Safe lub Aplikacji** – rozumie się przez to aplikację ProteGO Safe, która zawiera Moduł Analityczny, Moduł Triażu oraz Moduł Dziennik Zdrowia, a także wspiera w profilaktyce i zapobieganiu zarażeniem, przekazuje istotne informacje związane z pandemią COVID-19 oraz przypomina o bezpiecznych zachowaniach i nawykach codziennej higieny.
11) **Przetwarzaniu** – rozumie się przez to operację lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
12) **Regulaminie** – rozumie się przez to dokument, który określa warunki korzystania z ProteGO Safe, a także prawa i obowiązki GIS, MC oraz Użytkowników.
13) **RODO** – rozumie się przez to Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem Danych Osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
14) **Serwerze ProteGO Safe -** rozumie się przez to infrastrukturę chmurową utrzymywaną przez Operatora Chmury Krajowej służącą do przekazania Klucza Diagnostycznego do Urządzeń Użytkowników. Klucze Diagnostyczne są przechowywane na Serwerze ProteGO Safe w postaci zaszyfrowanej przez 14 (czternaście) dni.
15) **Urządzeniu** – rozumie się przez to elektroniczne urządzenie za pośrednictwem, którego Użytkownik uzyskuje dostęp do ProteGO Safe (tablet, smartphone itp.) z aktywnym modułem

Bluetooth, systemem Android 5.0 lub wyższym z dostępem do sklepu Google Play albo z systemem iOS w wersji nie niższej niż 13.5 z dostępem do sklepu AppStore. Moduł Analityczny będzie działał jedynie w Urządzeniach z systemem Android 6.0 wspierających technologię BLE lub wyższym albo z systemem iOS w wersji nie niższej niż 13.5.

16) **Użytkowniku** – rozumie się przez to osobę posiadającą pełną zdolność do czynności prawnych, która po zaakceptowaniu Regulaminu i Polityki Prywatności korzysta z ProteGO Safe.
17) **WHO** - rozumie się przez to Światową Organizację Zdrowia (World Health Organisation).

§3.
Ogólne zasady

1. Do Przetwarzania Danych Osobowych w ProteGO Safe zastosowanie znajduje art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji Użytkownika. GIS oraz MC projektując zabezpieczenia techniczne ProteGO Safe dochowali należytej staranności, aby uniemożliwić identyfikację Użytkowników. Niemniej z uwagi na fakt, że lokalnie w ramach Aplikacji przetwarzane są Dane Osobowe Użytkownika, pomimo braku dostępu do nich ze strony GIS jako administratora danych, Rozporządzenie w dalszym ciągu znajduje zastosowanie.
2. Dane Osobowe Przetwarzane są wyłącznie w celu wsparcia społeczeństwa w przeciwdziałaniu rozprzestrzeniania się pandemii COVID-19: działając w szeroko rozumianym interesie publicznym, administrator poprzez dystrybucję i zapewnienie operacyjności aplikacji ProteGO Safe wspiera szybką wymianę informacji pomiędzy osobami fizycznymi w ramach określonej społeczności, działając na rzecz profilaktyki zdrowia publicznego i przeciwdziałania rozprzestrzenianiu się wirusa SARS CoV-2 oraz choroby COVID-19, poprzez wymianę zanonimizowanych informacji dotyczących osób zakażonych oraz oprogramowanie umożliwiające analizę spotkań i kontaktów, jak również poprzez algorytmy umożliwiające ocenę ryzyka zarażenia.
3. Dane Osobowe Przetwarzane są na podstawie **art. 6 ust. 1 lit. e RODO** w zw. z zadaniem realizowanym w interesie publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej (Dz.U. z 2019 r. poz. 59).
4. Dane Osobowe dotyczące stanu zdrowia Użytkownika są przetwarzane także na podstawie **art. 9 ust. 2 lit. i RODO** w zw. z zadaniem publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej (Dz.U. z 2019 r. poz. 59), gdyż przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi na podstawie prawa państwa członkowskiego.
5. ProteGO Safe przetwarza Dane Osobowe niewymagające identyfikacji jak stanowi art. 11 RODO. GIS ani MC nie są w stanie zidentyfikować osoby, której dane dotyczą (Użytkownika). GIS przestrzega następujących zasad Przetwarzania Danych Osobowych:
    1) wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych o Użytkownikach Aplikacji odbywało się w sposób anonimowy bez ich identyfikacji zgodnie z przepisami o ochronie Danych Osobowych i aby móc to wykazać;
    2) wykonuje nadzór nad bezpieczeństwem Danych Osobowych przez cały okres ich posiadania w sposób zapewniający w szczególności ochronę przed dostępem osób nieuprawnionych, uszkodzeniem, zniszczeniem lub utratą;
    3) zachowuje poufność informacji dotyczących Użytkownika poprzez zastosowanie szyfrowania;
    4) zachowuje poufność Danych Osobowych;
    5) zapewnia osobom, których dane dotyczą, realizację ich praw wynikających z przepisów prawa.
6. GIS może przetwarzać następujące Dane Osobowe:

1) Dane związane z wykorzystywaniem serwera zapewniającego przekazywanie Użytkownikom komunikatów:
   a) UID – losowe oznaczenie Użytkownika uniemożliwiające identyfikację,
   b) Średni czas korzystania z Aplikacji przez Użytkowników (dane statystyczne, których nie można powiązać z poszczególnymi Użytkownikami).
2) Dane statystyczne pochodzące ze sklepów z aplikacjami tj. Google Play Store oraz Apple AppStore, których nie można powiązać z poszczególnymi Użytkownikami (dane statystyczne):
   a) Informacja o instalacji, ostatnim korzystaniu i usunięciu Aplikacji;
   b) Lokalizacja, w której znajdował się Użytkownik podczas instalacji Aplikacji (określenie miasta lub kraju);
   c) Modele Urządzeń Użytkowników;
3) Dane przechowywane wyłącznie lokalnie na Urządzeniach, niezależnie od systemu operacyjnego Urządzenia. Dane te nie są przekazywane poza Urządzenie Użytkownika, w szczególności nie Przetwarza ich GIS ani MC:
   a) ID Użytkownika,
   b) Historia wpisów do Dziennika Zdrowia,
   c) Historia wpisów do Modułu Triażu,
   d) Temporarary_exposure_keys_upload_status - informacja czy przesłanie informacji w ramach Modułu Analitycznego zakończyło się pomyślnie czy też z błędem,
   e) informacja o tym, czy Aplikacja jest uruchamiana pierwszy raz,
   f) Informacja o połączeniu Internetowym,
   g) informacja o tym, czy Użytkownik udzielił zgodę na powiadomienia push w Aplikacji,
   h) informacja o tym, czy Użytkownik przydzielił Aplikacji uprawnienie konieczne dla funkcjonowania Modułu Analitycznego,
   i) informacja o tym, czy moduł Bluetooth urządzenia jest włączony,
   j) Informacja o stanie, włączeniu i aktywności Modułu Analitycznego,
   k) Informacja o stanie Aplikacji (czy jest włączona na pierwszym planie, czy w tle),
   l) Informacje usuwane po 14 dniach:
      i) historia wyników analiz Modułu Analitycznego z ostatnich 14 dni,
      ii) okres kontaktu Urządzeń Użytkowników, wartości w zakresie 5-30 minut,
      iii) data kontaktu Urządzeń Użytkowników.
4) Dane przekazywane do innych Urządzeń za pośrednictwem Serwera ProteGO Safe:
   a) Klucz Diagnostyczny - zawiera informacje o kluczu, rollingPeriod, rollingStartNumber oraz transmissionRisk (dokładne informacje tutaj)
   b) region działania Aplikacji (Polska);
   c) informacja, że Klucz Diagnostyczny jest związany z aplikacją ProteGO Safe;
   d) potwierdzenie, że Kod PIN jest poprawny.
5) Plik cookies zawierający UID Użytkownika przekazywany do Cloudflare Inc. w celu zapobiegania atakom DDOS oraz zapewnienia najwyższych standardów bezpieczeństwa Użytkowników. Plik cookies, o którym mowa w niniejszym punkcie nie umożliwia profilowania, ani monitorowania zachowań Użytkownika na różnych witrynach (cross-site tracking). Więcej informacji dotyczących bezpieczeństwa tego rozwiązania jest dostępne tutaj: https://support.cloudflare.com/hc/en-us/articles/200170156-Understanding-the-Cloudflare-Cookies#12345682.

7. Podanie Danych Osobowych, o których mowa w ust. 5 pkt. 3 niniejszego paragrafu, jest dobrowolne, lecz może warunkować korzystanie z pełnych funkcjonalności ProteGO Safe.
8. Odbiorcami Danych Osobowych z ProteGO Safe:
   1) w zakresie określonym w §3 ust. 4 pkt. 1, 2 i 4 mogą być podmioty, które współpracują z GIS w celu rozwoju i utrzymania ProteGO Safe:

a) MC odpowiedzialny za nadzór nad rozwojem i utrzymaniem ProteGO Safe tj. Minister Cyfryzacji z siedzibą w Warszawie, ul. Królewska 27, 00–060 Warszawa, e-mail: mc@mc.gov.pl;
b) podmiot odpowiedzialny za utrzymanie aplikacji ProteGO Safe, a także wykonywanie zleconych przez MC prac rozwojowych i deweloperskich nad ProteGO Safe: TYTANI24 Spółka z ograniczoną odpowiedzialnością z siedzibą we Wrocławiu, ul. Ząbkowicka 55, 50 – 511 Wrocław (adres biura: ul. Kościerzyńska 32A, Wrocław, 51 – 410), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000725465, REGON 369879064, NIP 8992843182, o kapitale zakładowym opłaconym w całości w wysokości 20 000,00 zł;

2) w zakresie określonym w §3 ust. 4 pkt. 1, 2 i 4 może być Operator Chmury Krajowej Sp. z o.o. jako podmiot dostarczający infrastrukturę umożliwiającą pobieranie i aktualizowanie ProteGO Safe oraz utrzymujący Serwer ProteGO Safe. Podmiot ten świadczy także utrzymanie usługi Google Firebase umożliwiającej przekazywanie Użytkownikom powiadomień push - https://firebase.google.com/support/privacy;
3) w zakresie określonym w §3 ust. 4 pkt. 5 może być: Cloudflare Inc. 101 Townsend St, San Francisco, CA 94107, USA w zakresie dostarczania usługi zapobiegania atakom DDOS oraz zapewnienia najwyższych standardów bezpieczeństwa Użytkowników.

9. ProteGO Safe będzie aktywne jedynie przez okres pandemii COVID-19 i może zostać dezaktywowana zgodnie z decyzją GIS. Po zaprzestaniu korzystania z ProteGO Safe wszystkie Dane Osobowe zostaną usunięte wraz z Aplikacją.
10. Dane Osobowe dotyczące Użytkownika w postaci anonimowego adresu UID mogą być przekazywane poza Europejski Obszar Gospodarczy w zakresie korzystania z usługi świadczonej przez Cloudflare w celu zapobiegania atakom DDOS oraz zapewnienia najwyższych standardów bezpieczeństwa Użytkowników. Cloudflare Inc pozostaje podmiotem certyfikowanym w ramach programu certyfikacji Privacy Shield, funkcjonującego w oparciu o decyzję wykonawczą Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. ws. Tarczy Prywatności. Takie przekazanie nastąpi także jedynie w sytuacji wyjątkowej, w szczególności wtedy, gdy Użytkownik będzie korzystał z Aplikacji poza terenem Europejskiego Obszaru Gospodarczego.
11. Przetwarzane Dane Osobowe nie są udostępniane Odbiorcom Danych Osobowych w formie, która pozwalałaby na identyfikację osoby, której dane dotyczą.
12. W ramach ProteGO Safe nie są podejmowane decyzje w sposób zautomatyzowany w rozumieniu art. 22 RODO. Oznacza to, że okoliczność korzystania z Aplikacji nie powoduje wydawania w stosunku do Użytkownika jakichkolwiek decyzji, które mogłyby mieć charakter skutku prawnego lub w podobny sposób istotnie wpływać na Użytkownika.

§ 4.
Prawa Użytkowników

1. Do Przetwarzania Danych Osobowych w ProteGO Safe zastosowanie znajduje art. 11 RODO
2. Osobom, których dane dotyczą, przysługuje:
   1) na podstawie art. 15 RODO prawo dostępu do Danych Osobowych;
   2) na podstawie art. 16 RODO prawo do sprostowania Danych Osobowych;
   3) na podstawie art. 17 RODO prawo do usunięcia Danych Osobowych;
   4) na podstawie art. 18 RODO prawo żądania od Administratora ograniczenia Przetwarzania Danych Osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
   5) na podstawie art. 21 RODO prawo sprzeciwu wobec Przetwarzania Danych Osobowych.
3. W celu realizacji praw wskazanych w ust. 1, należy skorzystać z odpowiednich funkcjonalności ProteGO Safe.

4. ProteGO Safe umożliwia Użytkownikowi w dowolnym czasie realizację prawa do usunięcia Danych Osobowych:
    1) Aby usunąć Dane Osobowe z Modułu Triażu, Modułu Dziennik Zdrowia oraz innych Danych Osobowych wprowadzonych przez Użytkownika należy na ekranie głównym ProteGO Safe wybrać kolejno: Więcej, następnie Moje dane, następnie Zarządzaj danymi, a następnie Wymaż dane. Po zatwierdzeniu przez Użytkownika decyzji wszystkie Dane Osobowe wprowadzone przez Użytkownika do ProteGO Safe zostaną bezpowrotnie usunięte.
    2) Aby usunąć Dane Osobowe z Modułu Analitycznego należy odpowiednio:
        a. dla Urządzeń z systemem iOS w wersji 13.5 lub 13.6 wybrać kolejno: Ustawienia Systemowe > Prywatność > Zdrowie > Rejestrowanie Narażenia na COVID-19 -> Usuń dziennik narażeń;
        b. dla Urządzeń z systemem iOS w wersji 14 wybrać kolejno: Ustawienia Systemowe > Powiadomienia o narażeniu -> Usuń dziennik narażeń;
        c. dla Urządzeń z systemem Android wybrać kolejno: Ustawienia -> Google -> Powiadomienia o ryzyku ekspozycji na COVID-19 -> Usuń losowe identyfikatory;
        po zatwierdzeniu przez Użytkownika decyzji wszystkie dane związane z Modułem Analitycznym zostaną bezpowrotnie usunięte.
5. W sprawie jakichkolwiek pytań i wniosków związanych z prawami Użytkowników należy kontaktować się pod adresem: protego@mc.gov.pl.
6. Użytkownik, ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli uzna, że Przetwarzanie jego Danych Osobowych narusza przepisy RODO lub powszechnie obowiązujące przepisy. Skargę można wysłać pisemnie na adres: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa lub elektroniczne za pośrednictwem portalu ePUAP.
7. Użytkownik ma prawo do wycofania zgody na działanie Modułu Analitycznego w dowolnym momencie, przy czym wycofanie zgody nie wpłynie na zgodność z prawem działań dokonanych przed jej wycofaniem. Aby wycofać zgodę związaną z Modułem Analitycznym należy:
    1) dla Urządzeń z systemem iOS w wersji 13.5 lub 13.6 wybrać kolejno: Ustawienia Systemowe > Prywatność > Zdrowie > Rejestrowanie Narażenia na COVID-19 -> Wyłącz Rejestrowanie narażenia;
    2) dla Urządzeń z systemem iOS w wersji 14 wybrać kolejno Ustawienia Systemowe > Powiadomienia o narażeniu -> Wyłącz Rejestrowanie narażenia;
    3) dla Urządzeń z systemem Android wybrać kolejno: Ustawienia -> Google -> Powiadomienia o ryzyku ekspozycji na COVID-19 -> Wyłącz Powiadomienia o ryzyku ekspozycji;
    po zatwierdzeniu przez Użytkownika decyzji Moduł Analityczny przestanie działać.
8. Użytkownik ma prawo do wycofania zgody wyrażonej na podstawie art. 173 ust. 1 ustawy Prawo telekomunikacyjne w dowolnym momencie, przy czym wycofanie zgody nie wpłynie na zgodność z prawem działań dokonanych przed jej wycofaniem. Aby wycofać zgodę należy usunąć ProteGO Safe z Urządzenia.

§5.
Postanowienia końcowe

1. W ProteGO Safe mogą pojawiać się linki do innych stron internetowych. Takie strony internetowe działają niezależnie od GIS i nie są w żaden sposób przez niego nadzorowane. Strony te mogą posiadać własne polityki prywatności oraz regulaminy, z którymi zalecamy się zapoznać.
2. GIS zastrzega sobie prawo zmiany Polityki Prywatności poprzez opublikowanie nowej Polityki Prywatności na stronie ProteGO Safe.
3. Po zakończeniu okresu pandemii lub zagrożenia pandemicznego związanego z wirusem SARS-CoV-2 Aplikacja ProteGO Safe zostanie zdezaktywowana.