POLITYKA PRYWATNOŚCI
STOP COVID - ProteGO Safe

Najistotniejsze informacje dotyczące Twojej prywatności

Przygotowaliśmy ten dokument, aby poinformować Cię jak przetwarzamy dane w STOP COVID - ProteGO Safe, a także jakie prawa Ci przysługują. Poniżej znajdziesz kluczowe informacje związane z przetwarzaniem danych w ramach naszej Aplikacji.
Zaprojektowaliśmy STOP COVID - 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 STOP COVID - 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 STOP COVID - ProteGO Safe.

Informacje przetwarzane przez STOP COVID - ProteGO Safe nie umożliwiają Twojej identyfikacji.

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

Informacje wprowadzone do STOP COVID - ProteGO Safe związane z Triażem (samooceną ryzyka zarażenia COVID-19 - Moduł Triażu) są analizowane w ramach STOP COVID - 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 STOP COVID - 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 STOP COVID - 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 jest zaszyfrowane, 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 zaszyfrowanego Klucza na serwer STOP COVID - ProteGO Safe, a następnie do Urządzeń innych Użytkowników w celu analizy ryzyka zarażenia COVID-19. Wprowadzenie Kodu PIN do Urządzenia jest dobrowolne.

Klucz wysłany z Twojego Urządzenia na Serwer STOP COVID - 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 zaszyfrowanego Klucza na Serwer STOP COVID - ProteGO Safe, a następnie do innych Użytkowników Aplikacji. Każda z Aplikacji, po otrzymaniu Klucza dokonuje automatycznej

analizy spotkań poprzez odpowiednie porównanie otrzymanego Klucza 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 STOP COVID - ProteGO Safe. GIS ani MC nie identyfikują Użytkowników STOP COVID - ProteGO Safe.
2. Administratorem Danych Użytkowników jest Główny Inspektor Sanitarny z siedzibą w Warszawie, ul. Targowa 65, 03–729 Warszawa.
3. Poprzez pobranie STOP COVID - 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 STOP COVID - 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.
9. W przypadku wyrażenia zgody na Interoperacyjność Użytkownik powinien zapoznać się z treścią Załącznika nr 1 do niniejszej Polityki, która określa prawa i obowiązki Współadministratorów i Użytkowników w związku z tą funkcjonalnością. Załącznik nr 1 stanowi Załącznik nr 2 do Decyzji Wykonawczej Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniającej decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19.

§2.
Definicje

Ilekroć w Polityce Prywatności mowa o:

1) **Aktualnych obostrzeniach w powiatach** – rozumie się przez to funkcjonalność STOP COVID - ProteGO Safe umożliwiającą wyświetlanie w Aplikacji informacji o obszarach (powiatach) objętych szczególnymi zasadami bezpieczeństwa wprowadzonymi ze względu na pandemię COVID-19 na podstawie z odpowiedniego i aktualnego rozporządzenia w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii oraz rozporządzeń zmieniających;
2) **Bramie Federacyjnej** – rozumie się przez to bramę sieciową obsługiwaną przez Komisję Europejską za pomocą bezpiecznego narzędzia IT, która służy do odbierania, przechowywania i udostępniania minimalnego zbioru Danych Osobowych między serwerami wewnętrznymi państw członkowskich Unii Europejskiej w celu zapewnienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania. Brama Federacyjna umożliwia Interoperacyjność. Dzięki Bramie Federacyjnej możliwe jest wysyłanie oraz odbieranie Kluczy pomiędzy Użytkownikiem a użytkownikami innych aplikacji mobilnych, podobnych do STOP COVID – ProteGO Safe. Klucze wysyłane są za pośrednictwem Bramy Federacyjnej, a okres przechowywania Kluczy wynosi 14 dni;
3) **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;
4) **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 STOP COVID - ProteGO Safe zastosowanie znajduje art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji, zatem Użytkownicy STOP COVID - ProteGO Safe nie są identyfikowani;
5) **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 STOP COVID - ProteGO Safe. GIS samodzielnie ustala cele i sposoby przetwarzania Danych Osobowych w ramach STOP COVID - ProteGO Safe;
6) **Interoperacyjności lub Ostrzeganiu w Europie** – rozumie się przez to funkcjonalność STOP COVID - ProteGO Safe umożliwiającą wymianę Kluczy pomiędzy Użytkownikiem a użytkownikami innych aplikacji mobilnych, podobnych do STOP COVID – ProteGO, które są wspierane przez inne państwa członkowskie Unii Europejskiej i współpracują w ramach Bramy Federacyjnej. Dzięki Interoperacyjności Użytkownicy mogą otrzymać informację o potencjalnym narażeniu na zakażenie w związku z potencjalnym kontaktem z użytkownikami innych aplikacji mobilnych, podobnej do STOP COVID – ProteGO Safe;
7) **Kluczu** - rozumie się przez to generowany losowo, okresowy i alfanumeryczny ciąg znaków przekazywany na Serwer STOP COVID - ProteGO Safe, który zawiera zaszyfrowane Dane Osobowe, inicjujący proces analizy narażenia na zarażenie COVID-19 w ramach Modułu Analitycznego. Klucz jest przekazywany na Serwer STOP COVID - ProteGO Safe po wpisaniu do Aplikacji Kodu PIN przez Użytkownika będącego Osobą Chorą;
8) **Kodzie PIN Testu** – rozumie się przez to generowane losowo i aktywne przez pół godziny od momentu wygenerowania alfanumeryczne hasło, które jest przekazywane Użytkownikowi przez konsultanta Centrum Kontaktu. Kod PIN Testu przekazywany jest Użytkownikowi, który ma status wysokiego ryzyka narażenia na zakażenie COVID-19 wygenerowany przez Moduł Analityczny oraz wysokie ryzyko narażenia na zakażenie COVID-19 potwierdzone przez Moduł Triażu;
9) **MC** - rozumie się przez to Ministra Cyfryzacji z siedzibą w Warszawie, Aleje Ujazdowskie 1/3, 00-583, Warszawa. MC w oparciu o porozumienie zawarte z GIS, wspiera GIS w rozwoju i utrzymaniu STOP COVID - ProteGO Safe;
10) **Module Analitycznym** - rozumie się przez to funkcjonalność STOP COVID - 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 prywatność Użytkowników;

11) **Module Dziennik Zdrowia** - rozumie się przez to funkcjonalność STOP COVID - 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;
12) **Module Triażu** - rozumie się przez to funkcjonalność STOP COVID - 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;
13) **Osobie Chorej -** 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;
14) **Powiadomieniu PUSH** – rozumie się przez to wiadomość tekstową wysyłaną przez Serwer STOP COVID - ProteGO Safe, która wyświetli się na ekranie Urządzenia Użytkownika niezależnie od tego czy Aplikacja jest włączona. Treść powiadomień PUSH będzie bezpośrednio związana z rozwojem pandemii wirusa SARS-CoV-2 lub Aplikacją i każdorazowo ustalana przez GIS lub MC.
15) **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;
16) **Regulaminie** – rozumie się przez to dokument, który określa warunki korzystania z STOP COVID - ProteGO Safe, a także prawa i obowiązki GIS, MC oraz Użytkowników;
17) **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);
18) **Serwerze STOP COVID - ProteGO Safe -** rozumie się przez to infrastrukturę chmurową utrzymywaną przez Operatora Chmury Krajowej służącą do przekazania Klucza do Urządzeń Użytkowników. Klucze są przechowywane na Serwerze STOP COVID - ProteGO Safe w postaci zaszyfrowanej przez 14 (czternaście) dni;
19) **STOP COVID - ProteGO Safe lub Aplikacji** – rozumie się przez to aplikację STOP COVID - 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;
20) **Urządzeniu** – rozumie się przez to elektroniczne urządzenie za pośrednictwem, którego Użytkownik uzyskuje dostęp do STOP COVID - 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;

21) **Użytkowniku** – rozumie się przez to osobę posiadającą pełną zdolność do czynności prawnych, która po zaakceptowaniu Regulaminu i Polityki Prywatności korzysta z STOP COVID - ProteGO Safe;
22) **WHO** - rozumie się przez to Światową Organizację Zdrowia (World Health Organisation);
23) **Współadministratorach** - rozumie się przez to organy ochrony zdrowia odpowiedzialne za administrowanie aplikacji podobnych do STOP COVID - ProteGO Safe, które korzystają z Bramy Federacyjnej. Szczegóły dotyczące współpracy między Współadministratorami określa Załącznik nr 1 zgodnie z Załącznikiem nr 2 do Decyzji Wykonawczej Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniającej decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19. Lista Współadministratorów wraz z informacjami o przetwarzaniu przez nich Danych Osobowych Użytkownika, który wyraził zgodę na Interoperacyjność, znajduje się tutaj: https://ec.europa.eu/health/ehealth/covid-19_pl

§3.
Ogólne zasady

1. Do Przetwarzania Danych Osobowych w STOP COVID - ProteGO Safe zastosowanie znajduje art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji Użytkownika. GIS oraz MC projektując zabezpieczenia techniczne STOP COVID - 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 STOP COVID - 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 zaszyfrowanych 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. STOP COVID - 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 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 STOP COVID - ProteGO Safe:
      a) Klucz - zawiera rollingPeriod, rollingStartNumber oraz transmissionRisk (dokładne informacje tutaj)
      b) region działania Aplikacji (Polska);
      c) informacja, że Klucz jest związany z aplikacją STOP COVID - 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.

6) Informacje ujawniane GIS pośrednio przez Użytkownika w związku z weryfikacją prawidłowości Kodu PIN Testu:
   a) status wysokiego ryzyka narażenia na zakażenie COVID-19 wygenerowany przez Moduł Analityczny;
   b) status wysokiego ryzyka narażenia na zakażenie COVID-19 wygenerowany przez Moduł Triażu;
7) Dane wymieniane oraz przetwarzane za pośrednictwem Bramy Federacyjnej w ramach Interoperacyjności obejmują następujące informacje:
   a) Klucze przekazane przez STOP COVID - ProteGO Safe oraz inne aplikacje, podobne do STOP COVID - ProteGO Safe, w okresie do 14 dni poprzedzających datę przesłania Kluczy;
   b) dane dziennika dotyczące Kluczy zgodnie z protokołem specyfikacji technicznych stosowanym w państwie pochodzenia Kluczy;
   c) weryfikację zakażenia;
   d) państwa będące przedmiotem zainteresowania Użytkownika oraz państwo pochodzenia Kluczy.

7. Podanie Danych Osobowych, o których mowa w ust. 5 pkt. 3 niniejszego paragrafu, jest dobrowolne, lecz może warunkować korzystanie z pełnych funkcjonalności STOP COVID - ProteGO Safe.
8. STOP COVID - ProteGO Safe umożliwia przesyłanie i odbieranie Kluczy pomiędzy Użytkownikami STOP COVID – ProteGO Safe oraz użytkownikami aplikacji podobnych do STOP COVID – ProteGO Safe, które korzystają z Bramy Federacyjnej. Interoperacyjność (Ostrzeganie w Europie) ma charakter dobrowolny i korzystanie z niej jest oparte o zgodę Użytkownika wyrażoną na podstawie **art. 9 ust. 1 lit. a RODO**. Interoperacyjność jest świadczona za pośrednictwem Bramy Federacyjnej. W celu skutecznego korzystania z Interoperacyjności należy wyrazić odpowiednią zgodę w Aplikacji. Zgoda wyrażona przez Użytkownika dotyczy wysyłania i odbierania Kluczy w stosunku do wszystkich aplikacji mobilnych, podobnych do STOP COVID – ProteGO Safe. Zgodę można w każdej chwili wycofać, bez wpływu na wysłane i odebrane Klucze, które zostały wysłane lub odebrane przed cofnięciem zgody. Po wyrażeniu zgody Klucze wysyłane są do aplikacji podobnych do STOP COVID - ProteGO Safe. Historia spotykanych urządzeń, na których jest zainstalowana aplikacja podobna do STOP COVID - ProteGO Safe, będzie przechowywana w Bramie Federacyjnej przez 14 dni.
9. Odbiorcami Danych Osobowych z STOP COVID - 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 STOP COVID - ProteGO Safe:
      a) MC odpowiedzialny za nadzór nad rozwojem i utrzymaniem STOP COVID - ProteGO Safe tj. Minister Cyfryzacji z siedzibą w Warszawie, Aleje Ujazdowskie 1/3, 00-583, Warszawa, e-mail: ad@kprm.gov.pl;
      b) podmiot odpowiedzialny za utrzymanie aplikacji STOP COVID - ProteGO Safe, a także wykonywanie zleconych przez MC prac rozwojowych i deweloperskich nad STOP COVID - 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 STOP COVID - ProteGO Safe oraz utrzymujący Serwer STOP COVID - 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. 6 mogą być Współadministratorzy oraz Komisja Europejska działająca w charakterze podmiotu przetwarzającego;
4) 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.

10. STOP COVID - ProteGO Safe będzie aktywne jedynie przez okres pandemii COVID-19 i może zostać dezaktywowana zgodnie z decyzją GIS. Po zaprzestaniu korzystania z STOP COVID - ProteGO Safe wszystkie Dane Osobowe zostaną usunięte wraz z Aplikacją.
11. Dane Osobowe dotyczące Użytkownika w postaci zaszyfrowanego 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. Dane są przekazywane w oparciu o standardowe klauzule umowne. Takie przekazanie nastąpi także jedynie w sytuacji wyjątkowej, w szczególności wtedy, gdy Użytkownik będzie korzystał z Aplikacji poza terenem Europejskiego Obszaru Gospodarczego.
12. Przetwarzane Dane Osobowe nie są udostępniane Odbiorcom Danych Osobowych w formie, która pozwalałaby na identyfikację osoby, której dane dotyczą.
13. Dane, o których mowa w §3 ust. 6 pkt. 6, związane z weryfikacją Kodu PIN Testu nie są ujawniane GIS bezpośrednio, ale jedynie Użytkownicy, którzy mają podwójny status wysokiego ryzyka wskazany zarówno przez Moduł Triażu, jak i Moduł Analityczny mogą zweryfikować poprawność Kodu PIN Testu.
14. W ramach STOP COVID - 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 STOP COVID - 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 STOP COVID - ProteGO Safe.
4. STOP COVID - 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

STOP COVID - 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 STOP COVID - 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 na wysyłanie Powiadomień PUSH w dowolnym momencie, przy czym wycofanie zgody nie wpłynie na zgodność z prawem działań dokonanych przed jej wycofaniem. Wycofanie zgody na wysyłanie Powiadomień PUSH nie wpływa na powiadomienia o wysokim ryzyku narażenia na zakażenie COVID-19 generowane przez Moduł Analityczny Aplikacji. Aby wycofać zgodę na wysyłanie Powiadomień PUSH należy:
   1) dla Urządzeń z systemem iOS wybrać kolejno: Ustawienia -> ProteGO Safe powiadomienia -> Wyłącz powiadomienia
   2) dla Urządzeń z systemem Android wybrać kolejno: Ustawienia -> Aplikacje -> Zarządzaj aplikacjami -> ProteGO Safe -> Wyłącz Powiadomienia;
   po zatwierdzeniu przez Użytkownika decyzji Powiadomienia PUSH nie będą wysyłane.
9. 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 STOP COVID - ProteGO Safe z Urządzenia.

§5.
Postanowienia końcowe

1. W STOP COVID - 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 STOP COVID - ProteGO Safe.
3. Po zakończeniu okresu pandemii lub zagrożenia pandemicznego związanego z wirusem SARS-CoV-2 Aplikacja STOP COVID - ProteGO Safe zostanie zdezaktywowana.

Załącznik nr 1 – Postanowienia dotyczące Współadministrowania. Załącznik nr 2 do Decyzji Wykonawczej Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniającej decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19.

Postanowienia dotyczące Współadministrowania. Załącznik nr 2 do Decyzji Wykonawczej Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniającej decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19.

Obowiązki uczestniczących Państw Członkowskich jako Współadministratorów na potrzeby Bramy Federacyjnej do celów transgranicznego przetwarzania między aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania

Sekcja 1

Podsekcja 1

Podział obowiązków

1. Współadministratorzy przetwarzają dane osobowe za pośrednictwem bramy federacyjnej zgodnie ze specyfikacjami technicznymi określonymi przez sieć e-zdrowie ([1]).
2. Każdy administrator odpowiada za przetwarzanie danych osobowych za pośrednictwem bramy federacyjnej zgodnie z ogólnym rozporządzeniem o ochronie danych i dyrektywą 2002/58/WE.
3. Każdy administrator ustanawia punkt kontaktowy posiadający funkcyjną skrzynkę pocztową, która będzie służyć do komunikacji między współadministratorami oraz między współadministratorami a podmiotem przetwarzającym.
4. Tymczasowa podgrupa utworzona przez sieć e-zdrowie zgodnie z art. 5 ust. 4 ma za zadanie analizowanie wszelkich kwestii wynikających z interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania oraz ze współadministrowania powiązanym przetwarzaniem danych osobowych, a także ułatwianie wydawania skoordynowanych instrukcji dla Komisji jako podmiotu przetwarzającego. W ramach tymczasowej podgrupy administratorzy mogą prowadzić prace mające na celu m.in. wypracowanie wspólnego podejścia do przechowywania danych na ich krajowych serwerach wewnętrznych, z uwzględnieniem okresu przechowywania danych określonego w ramach bramy federacyjnej.
5. Instrukcje dla podmiotu przetwarzającego są wysyłane przez punkt kontaktowy któregokolwiek z współadministratorów w porozumieniu z pozostałymi współadministratorami wchodzącymi w skład wspomnianej powyżej podgrupy.
6. Wyłącznie osoby uprawnione przez wyznaczone organy krajowe lub organy urzędowe mogą mieć dostęp do danych osobowych użytkowników, które to dane są przekazywane za pośrednictwem bramy federacyjnej.
7. Każdy wyznaczony organ krajowy lub organ urzędowy przestaje być Współadministratorem od dnia wycofania swojego udziału w bramie federacyjnej. Pozostaje on jednak odpowiedzialny za przetwarzanie za pośrednictwem bramy federacyjnej, które miało miejsce przed jego wycofaniem się.

Podsekcja 2

Obowiązki i role w zakresie rozpatrywania wniosków osób, których dane dotyczą, oraz w zakresie informowania takich osób

1. Każdy Współadministrator przekazuje użytkownikom swojej krajowej aplikacji mobilnej służącej do ustalania kontaktów zakaźnych i ostrzegania (»osoby, których dane dotyczą«) informacje na temat przetwarzania ich danych osobowych za pośrednictwem bramy federacyjnej do celów transgranicznej interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania zgodnie z art. 13 i 14 ogólnego rozporządzenia o ochronie danych.
2. Każdy Współadministrator pełni rolę punktu kontaktowego dla użytkowników jego krajowej aplikacji mobilnej służącej do ustalania kontaktów zakaźnych i ostrzegania oraz rozpatruje składane przez tych użytkowników lub ich przedstawicieli wnioski związane z wykonywaniem praw osób, których dane dotyczą, zgodnie z ogólnym rozporządzeniem o ochronie danych. Każdy administrator wyznacza specjalny punkt kontaktowy zajmujący się rozpatrywaniem wniosków otrzymanych od osób, których dane dotyczą. Jeżeli Współadministrator otrzyma od osoby, której dane dotyczą, wniosek, który nie wchodzi w zakres jego odpowiedzialności, niezwłocznie przekazuje go odpowiedzialnemu Współadministratorowi. Jeżeli zostaną o to poproszeni, Współadministratorzy pomagają sobie nawzajem w rozpatrywaniu wniosków osób, których dane dotyczą, i udzielają sobie nawzajem odpowiedzi bez zbędnej zwłoki, przy czym nie później niż w terminie 15 dni od otrzymania prośby o udzielenie pomocy.
3. Każdy Współadministrator udostępnia osobom, których dane dotyczą, treść niniejszego załącznika, w tym ustalenia określone w pkt 1 i 2.

SEKCJA 2

Zarządzanie cyberincydentami, w tym naruszeniami ochrony danych osobowych

1. Współadministratorzy pomagają sobie nawzajem w identyfikacji cyberincydentów i reagowaniu na cyberincydenty, w tym w przypadku naruszeń ochrony danych osobowych, w związku z przetwarzaniem za pośrednictwem bramy federacyjnej.
2. Współadministratorzy w szczególności powiadamiają się nawzajem o kwestiach takich, jak:
   a) wszelkie potencjalne lub faktyczne ryzyko dla dostępności, poufności lub integralności danych osobowych przetwarzanych za pośrednictwem bramy federacyjnej;
   b) wszelkie cyberincydenty związane z operacją przetwarzania za pośrednictwem bramy federacyjnej;
   c) każde naruszenie ochrony danych osobowych, prawdopodobne konsekwencje naruszenia ochrony danych osobowych oraz ocena ryzyka naruszenia praw i wolności osób fizycznych, a także wszelkie środki wdrożone w celu przeciwdziałania naruszaniu ochrony danych osobowych i łagodzenia ryzyka naruszenia praw i wolności osób fizycznych;
   d) każde naruszenie technicznych lub organizacyjnych zabezpieczeń dotyczących operacji przetwarzania za pośrednictwem Bramy Federacyjnej.
3. Współadministratorzy powiadamiają o wszelkich naruszeniach ochrony danych osobowych odnoszących się do operacji przetwarzania za pośrednictwem bramy federacyjnej Komisję, właściwe organy nadzorcze i, jeśli jest to wymagane, osoby, których dane dotyczą, zgodnie z art. 33 i 34 rozporządzenia (UE) 2016/679 lub po otrzymaniu powiadomienia ze strony Komisji.

SEKCJA 3

Ocena skutków dla ochrony danych

Jeżeli w celu wypełnienia obowiązków określonych w art. 35 i 36 ogólnego rozporządzenia o ochronie danych Współadministrator potrzebuje informacji od innego administratora, wysyła specjalny wniosek na adres funkcjonalnej skrzynki pocztowej, o której mowa w sekcji 1 podsekcja 1 pkt 3. Współadministrator, który otrzymał taki wniosek, dokłada wszelkich starań, aby takie informacje przekazać.