MINISTER CYFRYZACJI

Mateusz Morawiecki

BM-WOP.072.237.2020

Warszawa, dnia 22 października 2020 r.

Szanowna Pani
Elżbieta Witek
Marszałek Sejmu RP

Dot. pisma z 29 września br. Posła na Sejm RP Pani Gabrieli Lenartowicz oraz Pana Dariusza Jońskiego w sprawie aplikacji ProteGO Safe (Interpelacja nr 11404).

Szanowna Pani Marszałek,

Minister Cyfryzacji, realizując rozwiązanie mające na celu zmniejszenie ryzyka zakażenia wirusem SARS-CoV-2 wykorzystujące możliwości urządzeń mobilnych, od początku uwzględniał skuteczność działania oraz ochronę prywatności użytkowników. Nigdy celem rozwiązania, ani zamiarem resortu nie było zbieranie danych o użytkownikach, ich lokalizacji, kontaktach czy stanie zdrowia. Nie to jest celem aplikacji STOP-COVID (dawniej ProteGO – Safe).

Podstawowym zadaniem STOP-COVID jest powiadamianie użytkowników o ryzyku spotkania osoby zakażonej. Dla realizacji tego celu wymagane jest, aby urządzenia użytkowników mogły zebrać informacje o wzajemnym „kontakcie". Informacje te muszą być wystarczające do identyfikacji tzw. bliskiego kontaktu zgodnie z definicją GIS/ WHO. Dane potrzebne do oceny takiego zdarzenia to czas „widoczności" pomiędzy urządzeniami oraz szacowana odległość. Oba te parametry są możliwe do oszacowania z wykorzystaniem technologii Bluetooth Low Energy (BLE). Od początku prace nad wspominanym systemem koncentrowały się wokół tej technologii. Po wielu dyskusjach zarówno ze społecznością programistów, jak i zespołem ekspertów, zdecydowano się na wykorzystanie API przygotowanego przez Google oraz Apple (Exposure Notification - EN). To podejście pozwalało na objęcie rozwiązaniem najszerszego zbioru urządzeń dostępnych na rynku. Co więcej, standardy w zakresie prywatności, jakie narzuca proces weryfikacji aplikacji przed publikacją w sklepach Apple i Google, dają dodatkową pewność wysokiej ochrony prywatności użytkownika. Dane, jakie są tu przesyłane, to zmieniane co 15 minut jednorazowe klucze. Mechanizm zabezpieczeń wykorzystywany w tym procesie opisuje dokumentacja API Google i Apple[1].

[1] https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf , https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf?1

W efekcie rozwiązanie przyjęte przez resort, używające wspominanego powyżej API, zbiera i przetwarza lokalnie na urządzeniu użytkownika jedynie dane wymagane do oceny ryzyka bliskiego kontaktu z osobą zakażoną. Pozostałe dane, w tym samoocena zdrowia są w pełni dobrowolne, a ich niepodanie w żaden sposób nie ogranicza działania funkcjonalności oceny ryzyka kontaktu z osobą zakażoną. Co więcej, te dane również nie opuszczają urządzenia użytkownika. Wszystkie dane wykorzystywane przez aplikację są dodatkowo szyfrowane lokalnie na urządzeniu. Finalnie powiadomienie o zakażeniu nie jest przekazywane przez resort, infrastrukturę serwerową czy w sposób automatyczny przez aplikację. Informacja ta jest przekazywana przez aplikację na wyraźne życzenie, w pełni dobrowolnie przez użytkownika. Informacja ta jako wrażliwa, a dodatkowo wpływająca na innych użytkowników, może być wysłana jedynie po wprowadzeniu przez użytkownika sześcioznakowego kodu PIN. Informacja o zakażeniu jest przesyłana w postaci zaszyfrowanego klucza (Exposure Key) możliwego do użycia jedynie na urządzeniach użytkowników. Do przesyłania klucza jest wykorzystywana infrastruktura serwerowa.
Zespół zajmujący się projektem i realizacją aplikacji STOP-COVID uwzględnił w pracach:

- głosy płynące od społeczności programistów (wątki dyskusji na Gitlab[2]),
- wymagania Google i Apple[3],
- wymagania i zalecenia wskazane przez Unię Europejską w postaci eHealth Newtork Toolbox[4],
- wymagania w zakresie interoperacyjności w ramach Unii Europejskiej[5].

Zdając sobie sprawę z istotności zagadnienia prywatności danych użytkownika oraz obaw użytkowników, zlecono przeprowadzenie trzech, niezależnych audytów bezpieczeństwa oraz zgodności aplikacji STOP-COVID ze standardami ochrony danych oraz zgodności z Toolbox UE.

Wyniki audytów potwierdziły prawidłowość działania i zgodność z powyższymi standardami. Raporty z audytów są publicznie dostępne pod adresami:

- https://www.gov.pl/web/protegosafe/dokumenty - sekcja Materiały,
- https://github.com/ProteGO-Safe/specs/tree/master/audits .

Dodatkowymi aspektami zwiększającymi pewność, iż aplikacja nie realizuje żadnych ukrytych działań, są:

---

[2] https://github.com/ProteGO-Safe/specs/issues
[3] https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf , https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf, https://www.google.com/covid19/exposurenotifications/
[4] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf, https://ec.europa.eu/health/ehealth/covid-19_en, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_669
[5] https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf

- publicznie dostępny kod rozwiązania umieszczony w ogólnie dostępnym repozytorium - https://github.com/ProteGO-Safe,
- udział w pracach nad interoperacyjnością w ramach UE oraz udział polskiej aplikacji w testach EFGS (European Federation Gateway Service).

Wszystkie te działania dają szansę na zwiększenie poziomu zaufania do rozwiązania, a w efekcie zwiększenia liczby użytkowników STOP-COVID.

Poniżej przedstawiam odpowiedzi na pytania szczegółowe:

Ad 1) W jaki sposób wykorzystywane są dane zebrane przez ProteGO Safe?

Dane nie są wykorzystywane, ponieważ nie są zbierane poza urządzeniami użytkowników. Wszystkie dane zbierane przez aplikację są gromadzone i przetwarzane lokalnie na urządzeniach użytkowników. Dane te zgodnie ze specyfikacją API Google/ Apple są wykorzystywane do oceny ryzyka kontaktu z osobą zakażoną. Ocena ryzyka jest wykonywana przez moduł dostarczany przez Google/ Apple zgodnie z algorytmem opisanym w specyfikacji opublikowanej przez Google/ Apple[6].

Dodatkowo, jeśli użytkownik zdecyduje się na wypełnienie testu samodiagnostycznego i prowadzenie dziennika zdrowia, lokalnie na urządzeniu są zbierane i przetwarzane dane z ankiety samooceny. Na podstawia ankiety aplikacja dokonuje oceny ryzyka zachorowania użytkownika. Dane te nie są przesyłane poza urządzenie użytkownika. Co do zasady żadne dane związane z aplikacją STOP-COVID (z wyjątkiem kluczy przekazywanych przez Bluetooth oraz Exposure Keys przekazywanych dobrowolnie przez zakażonego użytkownika) nie opuszczają urządzenia użytkownika. Co więcej, dane niepotrzebne do oceny ryzyka (starsze niż 14 dni) są usuwane z urządzenia.

Ad 2) Kto ma dostęp do danych zebranych przez aplikację?

Dane są przechowywane lokalnie na urządzeniu użytkownika, dane wykorzystywane przez aplikację są szyfrowane. Jedyną osobą, która ma dostęp do tych danych, jest użytkownik aplikacji. Dodatkowo, jak każde urządzenie podłączające się do sieci, urządzenie ma przydzielony adres IP przez dostawcę połączenia sieciowego. Nie jest to jednak dana przydzielana i zbierana przez administrację, co więcej, nie jest to adres stały urządzenia oraz nie jest powiązany z danymi identyfikującymi urządzenie.

Ad 3) Czy aplikacja ProteGO Safe śledzi lokalizację użytkowników?

Aplikacja STOP-COVID (ProteGO Safe) nie śledzi i nie zapisuje lokalizacji urządzenia czy dalej użytkownika. Co więcej, gdyby tak się działo, aplikacja - jako korzystająca z API Google/ Apple -

[6] https://developers.google.com/android/exposure-notifications/meaningful-exposures

nie przeszłaby audytu przed publikacją w sklepach Google i Apple. Zatem nie byłaby w ogóle dostępna dla użytkowników.

Ad 4) Jakiego rodzaju dane są przetwarzane przez aplikację?

Aplikacja zbiera na potrzeby oceny ryzyka kontaktu z osobą zakażoną dane wymagane przez Moduł Analityczny, czyli API Google/ Apple[7]. Są to klucze wymieniane przez Bluetooth oraz Exposure Keys rozgłaszane dobrowolnie przez osoby zakażone. Dodatkowo, jeśli użytkownik zdecyduje się na wypełnienie testu samodiagnostycznego i prowadzenie dziennika zdrowia (Moduł Triażu) lokalnie na urządzeniu są zbierane i przetwarzane dane z ankiety samooceny zdrowia. Co ważne, wszystkie te dane są przechowywane jedynie na urządzeniu użytkownika.

Ad 5) Jakie uprawnienia posiada aplikacja ProteGO Safe?

Aplikacja zależnie od systemu operacyjnego (Android, iOS) wymaga włączenia modułu Bluetooth w urządzeniu użytkownika, a także odpowiednio dla urządzeń z systemem operacyjnym Android: włączenia systemowej opcji rejestrowania narażenia na COVID-19 oraz udzielenia zgody na lokalizację (w zakresie modułu Bluetooth, STOP COVID - ProteGO Safe nie wykorzystuje danych GPS), a dla urządzeń z systemem operacyjnym iOS: zaznaczenia opcji Rejestrowanie narażenia na COVID-19. W przypadku urządzeń z systemem Android korzystanie z modułu Bluetooth wymagana takiego uprawnienia, co wynika z samej konstrukcji uprawnień w tym systemie. Całość uprawnień jest opisana w dokumencie „Regulamin STOP COVID - ProteGO Safe" dostępnym dla użytkownika w aplikacji oraz na stronie https://www.gov.pl/web/protegosafe/dokumenty (sekcja Materiały).

Z poważaniem,

z up. Marek Zagórski
Sekretarz Stanu
w Kancelarii Prezesa Rady Ministrów
/podpisano elektronicznie/

[7] https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf