Dawid Czerw - Członek Zarządu SIODO
Piotr Kitela - Sekretarz Zarządu SIODO

„Bezpieczeństwo użytkowników w ProteGO Safe”

1. Wstęp

Stany wyższej konieczności, ratowanie ludzkiego zdrowia i życia, wprowadzanie ustawowych ograniczeń jest uzasadnione i może mieć miejsce wyłącznie w zgodności z Konstytucją RP i ustawami. Okres pandemii, czas zagrożeń epidemicznych i szczególne okoliczności towarzyszące tym zdarzeniom wyzwalają potrzebę zastosowania niestandardowych rozwiązań - jednak muszą się one opierać o naczelną zasadę zgodności z prawem polskim i UE, której jesteśmy partnerem.

Warto zatem spojrzeć na element „rzeczy inteligentnej” w proponowanym wprowadzaniu aplikacji na urządzenia mobilne „dla naszego bezpieczeństwa”. Czy w takiej rzeczywistości nie zostaną przekroczone zasady i reguły określone w prawie do prywatności? Jakie gwarancje przed zastosowaniem aplikacji zostaną skonsultowane oraz jasno i czytelnie ogłoszone? Czy tak zaawansowana „inteligentna rzecz” nie przeniknie zbyt daleko w prywatność „osoby zainstalowanej” i jej otoczenia tj. innych satelitarnych osób?

2. Czym jest ProteGO Safe

W związku z nieoczekiwanym stanem pandemii wirusa SARS-CoV-2 Ministerstwo Cyfryzacji wyszło z inicjatywą (samo)kontroli stanu zdrowia obywateli poprzez aplikację ProteGO Safe na urządzenia mobilne. Aplikacja ta ma na celu weryfikację stanu zdrowia użytkownika i jego otoczenia. Poprzez wypełnienie formularza startowego, w którym użytkownik ma za zadanie odpowiedzieć na kilka krótkich pytań, aplikacja może uzyskać informacje np. o płci, grupie krwi, nałogach, dolegliwościach lub przewlekłych chorobach.

Dodatkowo aplikacja wykorzystując technologie Bluetooth w telefonie użytkownika może mieć skojarzenie się ze smartfonami (określone modele z wyłączeniem telefonów trady-

cyjnych bez możliwości instalacji dodatkowych aplikacji w danej technologii) innych użytkowników, korzystających z tej samej aplikacji, jednocześnie informując nas o potencjalnym zagrożeniu wynikającym z kontaktu z osobą, która należeć może do grupy ryzyka.[1]

Twórcy aplikacji starają się podkreślić zasady bezpieczeństwa, którymi kierowali się podczas jej tworzenia oraz zapewniają użytkowników o tym, że ich dane wprowadzane do aplikacji przechowywane są wyłącznie na jego urządzeniu. Jednak powstaje pytanie czy w ekspresowym tempie prac wykonano odpowiednie symulacje, a wyniki testów potwierdzają ich skuteczność?

Analiza charakterystyki aplikacji oraz polityki prywatności ProteGO Safe budzi wątpliwości wobec przejrzystości zasad oraz zakresu przetwarzanych danych osobowych w aplikacji i skłania do głębszego pochylenia się nad zachowaniem zasad dotyczących przetwarzania danych osobowych oraz konstytucyjnym atrybutem obywatela – jego prywatnością.

Przyznać należy, iż wyjątkowość sytuacji usprawiedliwia zaproponowane przez Ministerstwo Cyfryzacji rozwiązania. Założenie nadrzędnego celu wspomagania osób i instytucji w kontrolę oraz zahamowanie rozprzestrzeniania się wirusa SARS-CoV-2.

Gdy jest to możliwe, najnowsze technologie można wykorzystywać w celu poprawy jakości życia oraz bezpieczeństwa obywateli. Jednak zadanie twórców „inteligentnej rzeczy" to duża doza odpowiedzialności i tym samym należy zdefiniować jasne i przejrzyste zasady przetwarzania danych.

Zgodnie z zapewnieniami telefony korzystające z aplikacji wymieniać się będą tymczasowymi kodami – przypadkowymi ciągami znaków, które nie ujawnią tożsamości użytkownika. Ich zadaniem jest umożliwienie ustalenia, że w danym przedziale czasu właściciele konkretnych urządzeń spotkali się w przestrzeni fizycznej.

Szczególną uwagę zwraca zakres danych podawanych w aplikacji w celu przydziału do konkretnej grupy RYZYKA oraz wewnętrznie sprzeczne zapisy *„polityki prywatności"*.

3. Zasady przetwarzania danych w aplikacji

Wychodząc naprzeciw rzetelności oraz przejrzystości przetwarzania danych osobowych oraz troszcząc się o prawa osób, których dane będą przetwarzane[2] w aplikacji, opracowano

[1] https://www.gov.pl/web/cyfryzacja/pokonajmy-razem-koronawirusa--poznaj-protego-safe

[2] Art. 4 pkt. 2 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 -

dokument polityki prywatności zawierający założenia aplikacji i zasady przetwarzania danych osobowych.

Analizując zapisy dokumentu, może rodzić wątpliwość założenie jakoby ProteGO Safe było rozwiązaniem budowanym zgodnie z zasadami wynikającymi z przepisów o ochronie danych osobowych. W zapisach można dostrzec – „*Aplikacja **jest budowana zgodnie z zasadami** wynikającymi z ogólnego rozporządzenia o ochronie danych osobowych (RODO), w tym **minimalizacji** danych, **privacy by design, privacy by default**, **prawidłowości, integralności oraz poufności.**”*[3].

Autorzy bardzo często przytaczają w tekstach opisujących funkcjonalność aplikacji sprzeczne ze sobą sformułowania, takie jak:[4]

- ✓ *„**Staramy się** nie pozyskiwać od Ciebie informacji, które umożliwią Twoją identyfikację (tj. danych osobowych), **ale może się zdarzyć** tak, że podczas korzystania z Aplikacji podasz nam tyle informacji, że **będziemy w stanie Cię zidentyfikować** (nawet pośrednio) – oznacza to, że będziemy administratorem Twoich danych.”*
- ✓ *„**Nie będziemy mieli dostępu do informacji i danych osobowych**, które wprowadzisz do aplikacji ProteGO Safe. Nie będziemy podejmowali aktywnych działań, aby Cię zidentyfikować. Nie będziemy także analizowali jak korzystasz z ProteGO Safe.”*
- ✓ *„**Informacje wprowadzone do ProteGO Safe** związane z samooceną ryzyka infekcji wirusem SARS-CoV-2 **będą** w sposób zanonimizowany **przesłane** do Infermedica.”*
- ✓ ***„Danych Osobowych** – rozumie się przez to podstawowe dane o Użytkowniku, tj. **nazwa Użytkownika oraz inne dane** podawane podczas korzystania z ProteGO Safe i określone w niniejszej Polityce”*
- ✓ *„Administrator danych **może przetwarzać następujące Dane Osobowe** (kategorie Danych Osobowych): identyfikator Urządzenia Użytkownika, nazwa Użytkownika (imię), **dane dotyczące zdrowia**, płeć, wiek, dane dotyczące palenia papierosów i **inne** […].”*
- ✓ ***„Dane Osobowe przetwarzane są wyłącznie w następujących celach:***
  - o *przeciwdziałania pandemii wirusa SARS-CoV-2;*
  - o ***profilowanie** w celu przeciwdziałania pandemii wirusa SARS-CoV-2*

(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)

[3] https://www.gov.pl/web/cyfryzacja/protego-safe--pobierz-zainstaluj-przetestuj

[4] Polityka prywatności ProteGO Safe https://www.gov.pl/attachment/046abbfb-386d-4803-a692-af4fc2921b92

- *korzystania przez Użytkownika z Aplikacji zgodnie z Regulaminem;*
- *analiza, organizowanie i ulepszanie ProteGO Safe."*

✓ ***„Dane Osobowe nie będą poddawane profilowaniu**. Administrator nie podejmuje względem Użytkownika decyzji w sposób zautomatyzowany."*

✓ *„Dane Osobowe będą przechowywane nie dłużej niż trwa korzystanie z ProteGO Safe, a także nie dłużej niż jest to wymagane przepisami prawa i nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Po zaprzestaniu korzystania z ProteGO Safe Dane Osobowe zostaną usunięte wraz z Aplikacją."*

✓ *„Odbiorcami **zanonimizowanych** danych i informacji z ProteGO Safe mogą być:*

1) *podmioty, które współpracują z Administratorem danych w celu rozwoju i utrzymania ProteGO Safe:*
   a) *Minister Cyfryzacji z siedzibą w Warszawie, ul. Królewska 27, 00–060 Warszawa, e-mail: mc@mc.gov.pl (Administrator Systemu);*
   b) *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) *Podmiot, który dostarcza narzędzie umożliwiające samoocenę ryzyka zarażenia COVID-19: Infermedica Sp. z o.o. z siedzibą we Wrocławiu, Plac Solny 14/3, 50-062 Wrocław, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000429183, REGON 021889810, NIP 8971782877 (polityka prywatności Infermedica: https://infermedica.com/privacy-policy, informacje o Usłudze Triażu: https://developer.infermedica.com/docs/covid-19#triage);*
3) *Podmiot dostarczający infrastrukturę umożliwiającą pobranie i aktualizowanie ProteGO Safe: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irlandia VAT IE6388047V (usługa Google Firebase - https://firebase.google.com/support/privacy).*

4) ***Podmiot dostarczający w przyszłości dodatkowe funkcjonalności**: Centrum Systemów Informacyjnych Ochrony Zdrowia z siedzibą w Warszawie, ul. Stanisława Dubois 5a, 00-184 Warszawa, e-mail: biuro@csioz.gov.pl;*
5) *Minister Zdrowia z siedzibą w Warszawie, ul. Miodowa 15. 00-952 Warszawa, NIP 5251918554, Regon 000287987."*

Tyle z cytowanego i powszechnie dostępnego pisma. Po pierwsze, jeżeli według podanych informacji, dane osobowe nie są przetwarzane poza urządzeniami użytkowników, to w jakim celu wskazuje się obligatoryjnie na przesłanki przetwarzania danych w wyżej wymienionym dokumencie?

Po drugie, skoro wskazuje to bezpośrednio na fakt przetwarzania danych osobowych użytkowników czy możliwy jest jednak fakt ich pełnego zidentyfikowania?

Przetwarzanie danych, znajdujące swoją definicję w przepisach 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 w artykule 4, odnosi się do operacji na danych osobowych o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Zatem można dostrzec koniunkcję zdarzeń użytkownik plus umowa z operatorem i operator aplikacji znający dane osoby związanej umową, trudniej ustalić, czy urządzenie jest w posiadaniu właściciela czy jego rodziny lub pupila.

Należy zatem zadać kolejne pytanie, czy pozyskiwane od użytkowników dane przetwarzane będą zgodnie z zapisami polityki prywatności i zachowaniem zasad bezpieczeństwa danych?

4. Zagrożenia prywatności

Zapisy dokumentu, wprowadzają użytkownika w dysonans - zostaje zapewniony, że jego bezpośrednia identyfikacja nie będzie możliwa. Następnie stwierdzenie zostaje podważone informacją o prawdopodobnym jednak wystąpieniu stanu umożliwiającego jego pełną identyfikację.

W tym momencie należy powtórzyć pytanie, **jakiego zakresu danych może wymagać aplikacja, jeżeli Administrator będzie w stanie zidentyfikować użytkownika? Ewentualnie do jakich danych w telefonie aplikacja zażąda dostępu?** – Jeżeli nie w wersji pierwotnej, to zaktualizowanej o dodatkowe funkcjonalności, o czym mowa w dokumencie.[5]

Kolejną wątpliwą kwestią są zasady ochrony danych osobowych użytkownika, w rozumieniu zastosowanych rozwiązań technicznych. Zgodnie z motywem 26 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[6] zasady ochrony danych, w tym anonimizacja danych osobowych, nie mają zastosowania do informacji, które jak zapewniają autorzy aplikacji nie pozwalają na zidentyfikowanie danego użytkownika.

Czy można przypuszczać, że niezależnie od zakresu danych wprowadzonych przez użytkownika do aplikacji, każdy kto ją wykorzystuje, wbrew zapewnieniom Administratora będzie osobą w pełni identyfikowalną?

Dalsza analiza wskazuje na rozbieżność w zakresie dostępu przez Administratora do informacji personalnych, które użytkownik wprowadza do aplikacji. W polityce prywatności użytkownik zapewniony zostaje, że Administrator **nie będzie** miał dostępu do informacji oraz danych osobowych. W kolejnym punkcie Administrator informuje użytkownika, że informacje wprowadzone do ProteGO Safe **będą** przesłane do komercyjnego podmiotu zewnętrznego.

W kontekście zapisów dokumentu, należy wziąć pod uwagę sposób przetwarzania danych z wykorzystaniem metody profilowania, której zastosowanie w aplikacji przedstawiane jest w polityce prywatności podkreślone w sposób sprzeczny.

Z jednej strony twórcy (programu lub opisu, ufać należy, że współpracowali) informują nas, że jednym z celów przetwarzania będzie „*profilowanie w celu przeciwdziałania pandemii SARS-CoV-2”*, z drugiej zaś użytkownik zostaje zapewniony, że jego dane nie będą poddawane profilowaniu - podparte zostaje to sformułowaniem, iż „*Administrator nie podejmuje względem*

[5] Tamże.
[6] Motyw 26Rozporządzenia 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: „[…]*Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.*[…]”

użytkownika decyzji w sposób zautomatyzowany". Przytoczmy zatem co oznacza profilowanie użytkownika.

Literalnie profilowanie oznacza *dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.* W efekcie użytkownik może wątpić w jasność przekazu.

Jeśli użytkownik zostaje poinformowany, że jego dane będą profilowane, to w żadnym wypadku ta informacja nie może być negowana przez Administratora poprzez zapewnienie, iż żadna decyzja względem użytkownika nie będzie podejmowana w sposób zautomatyzowany.

Co to oznacza dla użytkownika i jego prywatności w świetle tak wielu niejasności? Swego czasu, Generalny IODO upatrywał profilowanie jako zagrożenie będące przesłanką do kategoryzowania osób według różnych cech lub zachowań. Dodatkowo możliwości wyciągania na ich temat wniosków w oparciu o zebrane i przetworzone informacje. U użytkownika budzić to może wątpliwości, czy aby na pewno jego prywatność zostanie zachowana podczas użytkowania aplikacji.

5. Wnioski

Biorąc pod uwagę założenia i istotę funkcjonalności omawianej aplikacji oraz niejasności płynące z przekazu w zakresie zachowania podstawowych praw odnoszących się do prywatności człowieka, przyznać należy, że aplikacja ma jeszcze przed sobą daleką drogę zanim będzie rozwiązaniem w pełni akceptowalnym społecznie. Pomysł ten wymaga dopracowania nie tylko kwestii technicznych, jak jest to podkreślane w wielu publikacjach, ale również pod kątem zgodności z prawem polskim i Unii Europejskiej w zakresie ochrony danych.

Społecznym czynnikiem, który może utrudniać implementację technologii na szerszą skalę jest brak zaufania do rozwiązania wymagającego, jak wykazała analiza, nieproporcjonalnego zakresu danych personalnych o użytkowniku. Dodatkowo opinie specjalistów ds. cyberbezpieczeństwa wywołują szereg teorii stojących w opozycji do pierwotnie uznanych założeń w zakresie celu wykorzystania aplikacji i wpływają na wzrost świadomości społeczeństwa co do zakresu możliwości wykorzystania ich danych.

Występowanie stanów nieprzewidywalnych, takich jak pandemia, które powodują nagły i celowy rozwój technologiczny, wymuszają edukację społeczeństwa w tym zakresie. Sytuacje takie stawiają prekursorów rozwoju sztucznej inteligencji i Internetu rzeczy przed nie lada wyzwaniem w zakresie sformułowania norm, standardów oraz granic etycznych i moralnych odnoszących się do implementacji co raz to nowych rozwiązań

Istotą jest korelacja pomiędzy wskazanymi prekursorami a ekspertami w zakresie ochrony prywatności oraz spójne działanie jednostek edukacji zmierzające do wzrostu kultury ochrony danych osobowych.

Jednym z czynników wpływających pozytywnie na postrzeganie rozwiązań wykorzystujących nowe technologie na skalę globalną jest współpraca z ekspertami ochrony prywatności oraz instytucjami edukacji, która skutkować będzie wzrostem kultury ochrony danych osobowych.

Bibliografia:

1. Gazeta Pomorska - Maciej Czerniak, „*Aplikacja ProteGO Safe śledzi każdy Twój krok. Teoretycznie ma chronić przed Covid-19*", https://pomorska.pl/aplikacja-protego-safe-sledzi-kazdy-twoj-krok-teoretycznie-ma-chronic-przed-covid19/ar/c15-14971504 (dostęp 19.05.2020)
2. Oficjalna strona internetowa Ministerstwa Cyfryzacji https://www.gov.pl/web/cyfryzacja/protego-safe--pobierz-zainstaluj-przetestuj (dostęp 19.05.2020)
3. Polska Times – Maciej Czerniack, „*ProteGO Safe -rządowa aplikacja do walki z wirusem pod okiem specjalistów. Nie gwarantuje anonimowości*", https://polskatimes.pl/protego-safe-rzadowa-aplikacja-do-walki-z-wirusem-pod-okiem-specjalistow-nie-gwarantuje-anonimowosci/ar/c1-14956642 (dostęp 19.05.2020)
4. ProteGo Safe – Polityka prywatności https://www.gov.pl/attachment/046abbfb-386d-4803-a692-af4fc2921b92
5. Rozporządzenie 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