



Warszawa, dnia 01 czerwca 2020 r.

RZECZPOSPOLITA POLSKA
MINISTERSTWO CYFRYZACJI

Biuro Ministra

BM-WOP.0122.161.2020

Pan
Paweł Litwiński

Dot. wniosku o udostępnienie informacji publicznej z 30 kwietnia br.

Szanowny Panie,

zgodnie z art. 35 ust 1 „Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych”.

Ponadto art. 35 ust. 3 RODO nakazuje, aby ocenę taką przeprowadzać w szczególności, jeżeli operacje przetwarzania dotyczą:

- a. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- b. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10;

lub

- c. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Niezależnie od powyższych warunków, ocenę skutków zgodnie z art. 35 ust 4 należy przeprowadzić, jeżeli istnieje wysokie ryzyko naruszenia praw lub wolności osób fizycznych w związku z operacjami, których wykaz określa organ nadzorczy państwa członkowskiego, którym w Polsce jest Prezes Urzędu Ochrony Danych Osobowych. Zgodnie z [Komunikatem Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony](#), w wykazie tym wskazano między innymi, że ocenę skutków

należy przeprowadzić jeżeli przetwarzane są dane dotyczące „szczególnych kategorii danych osobowych” – poz. 4 ww. wykazu.

Zarówno jednak w komunikacie Prezesa UODO, jak i w dokumencie WP 248 rev.01 Grupy Roboczej art. 29 wydanym 4 października 2017 r. „Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679” wskazano, że:

„Zgodnie z przewidzianym w RODO podejściem opartym na analizie ryzyka przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe w przypadku każdej operacji przetwarzania. Przeprowadzenia oceny skutków dla ochrony danych wymaga się natomiast wyłącznie w przypadku, gdy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych” (art. 35 ust. 1). Sam fakt niespełnienia warunków nakładających obowiązek przeprowadzenia oceny skutków dla ochrony danych nie zmniejsza jednak ogólnego obowiązku wdrożenia przez administratorów środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia prawa i wolności osób, których dane dotyczą. W praktyce oznacza to, że administratorzy muszą stale oceniać ryzyko powodowane przez czynności przetwarzania w celu określenia, kiedy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”.

W odniesieniu do Aplikacji ProteGO Safe w wersji aktualnie udostępnionej przez Głównego Inspektora Sanitarnego, biorąc pod uwagę fakt, że:

- projekt zakłada profilowanie (prognozowanie) w stosunku do podmiotów danych – użytkowników aplikacji,
- zakłada się powszechne stosowanie aplikacji, co powoduje, że dane przetwarzane będą na dużą skalę,
- projekt zakłada wykorzystywanie innowacyjnych rozwiązań technologicznych i organizacyjnych,

oceniono, że ocenę skutków dla ochrony danych należy przeprowadzić i ocenę taką przeprowadzono zgodnie z metodyką stosowaną w tym zakresie w Ministerstwie Cyfryzacji.

Z przeprowadzonej oceny skutków dla ochrony danych wynika, że dla obecnie dostępnej wersji aplikacji ProteGO Safe nie występuje „wysokie ryzyko naruszenia praw lub wolności osób fizycznych”, gdyż:

- wynik triażu, czyli samooceny ryzyka zarażenia wirusem SARS-CoV-2 zapisywane są w pamięci lokalnej urządzenia, na którym zainstalowana jest aplikacja,
- w Aplikacji nie rejestruje się żadnych danych identyfikujących osobę Użytkownika za wyjątkiem nazwy – sugeruje się, aby było to imię Użytkownika Aplikacji – co nie

przesądza o tym, aby zakwalifikować je jako dane identyfikujące osobę, czyli dane osobowe. Do informacji przechowywanych na urządzeniu użytkownika GIS i MC nie mają dostępu,

- dane o stanie zdrowia wprowadzone w celu samooceny ryzyka infekcji wirusem SARS-CoV-2 są przechowywane w pamięci tymczasowej urządzenia, a następnie przesyłane do Infermedica w sposób uniemożliwiający identyfikację konkretnego użytkownika. Dane te nie są przechowywane w pamięci lokalnej urządzenia,
- do oceny ryzyka na podstawie wprowadzonych danych wykorzystywany jest kwestionariusz WHO, w którym nie podaje się danych identyfikujących osobę, lecz wyłącznie dane o stanach chorobowych i aktualnych objawach takich stanów (temperatura, duszności, bóle),
- zebrane na urządzeniu Użytkownika dane są wyłącznie pod kontrolą Użytkownika, którego one dotyczą,
- Użytkownik w każdej chwili może usunąć zebrane w aplikacji ProteGO Safe dane.

Nad Aplikacją ProteGO Safe prowadzone są dalsze badania mające na celu jej rozwój o dodatkowe funkcjonalności, w tym rejestrowanie anonimowych informacji o Aplikacjach innych użytkowników znajdujących się w najbliższym otoczeniu (zasięgu sygnału Bluetooth) oraz anonimowego powiadamiania Użytkownika Aplikacji, jeśli okaże się, że u osoby, której obecność zarejestrowano w pobliżu, stwierdzono zakażenie wirusem SARS-CoV-2.

W odniesieniu do nowej wersji Aplikacji z wbudowanymi mechanizmami rejestrowania osób znajdujących się w najbliższym otoczeniu, próbuje się zastosować rozwiązania mające na celu zapewnienie jeszcze większej anonimowości niż planowano pierwotnie przy wykorzystaniu standardu Open Trace. Jest to związane z zaawansowanymi pracami nad narzędziem, które zapewni wyższą skuteczność oraz przyjęcie modelu rozproszonego (zdecentralizowanego), przygotowywanego przez konsorcjum Google i Apple („Privacy-Preserving Contact Tracing”).

Uruchomienie nowej wersji Aplikacji ProteGO Safe z mechanizmami ostrzegania w przypadku, jeśli Użytkownik znalazł się przez określony czas w niewielkiej odległości od osoby, u której stwierdzono zakażenie wirusem SARS-CoV-2, nastąpi jeśli wyniki ponownie przeprowadzanej oceny skutków dla wersji z zastosowaniem wymienionego wyżej rozwiązania nazywanego „Privacy-Preserving Contact Tracing” nie stwierdzą wysokiego zagrożenia, że naruszone zostaną prawa i wolności Użytkowników aplikacji.

Z poważaniem,

Monika Skrzyńska
Zastępca Dyrektora Biura Ministra
/-podpisano elektronicznie/