Warszawa, 30-04-2020

URZĄD OCHRONY
DANYCH OSOBOWYCH
Departament
Orzecznictwa i Legislacji
Wydział Legislacji

DOL.023.426.2020.WL.TG

Pani
Agnieszka Kułakowska
Zastępca Dyrektora
Departamentu Zarządzania Danymi
w Ministerstwie Cyfryzacji
ul. Królewska 27
00-060 Warszawa
elektroniczna skrzynka podawcza
ePUAP
/MAiC/SkrytkaESP

W odpowiedzi na wiadomość przesłaną drogą elektroniczną w dniu 23 kwietnia 2020 r. dotyczącą aplikacji ProteGO Safe uprzejmie informuję, że problematyka wykorzystywania aplikacji w walce z pandemią wywołaną zarażeniami wirusem SARS-CoV-2 (choroba COVID-19) jest przedmiotem szczególnego zainteresowania zarówno poszczególnych krajowych organów do spraw ochrony danych osobowych, jak i Europejskiej Rady Ochrony Danych oraz Komisji Europejskiej. Świadczy o tym zarówno ożywiona dyskusja, która toczy się w tej sprawie między krajowymi organami

do spraw ochrony danych osobowych, jak i dokumenty, które – w ostatnim czasie – zostały wypracowane przez Komisję Europejską [*Komunikat Komisji – Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych* (Dz. Urz. UE C 124I z 17.04.2020, str. 1)] oraz Europejską Radę Ochrony Danych (*Wytyczne 04/2020 o wykorzystaniu geolokalizacji i innych narzędzi ustalania kontaktów w kontekście wybuchu epidemii COVID-19*, wydane przez Europejską Radę Ochrony Danych dnia 21 kwietnia 2020 r., dostępne na stronie internetowej https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

Opierając się na – powołanych wyżej – ustaleniach i dokumentach Prezes Urzędu Ochrony Danych Osobowych wskazuje na najistotniejsze kwestie, które muszą być uwzględnione w trakcie prac dotyczących aplikacji ProteGO Safe, dalej też „Aplikacji", i znaleźć jednoznaczne odzwierciedlenie w dokumentach opisujących tę Aplikację.

W pierwszej kolejności doprecyzowania wymaga status prawny podmiotów współpracujących czy też współdziałających w ramach aplikacji ProteGO Safe, gdyż nie jest on, niestety, określony w sposób konsekwentny ani wyczerpujący. O ile bowiem Główny Inspektor Sanitarny jest w całej dokumentacji wskazywany jako administrator w rozumieniu art. 4 pkt 7 *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)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[1)]), dalej „RODO", to już pozycja prawna Ministra Cyfryzacji nie jest jasna. W dokumencie *Regulamin ProteGO Safe* (§ 2 pkt 1) jest on nazywany „Administratorem Systemu" (a podnieść wypada, iż od rozpoczęcia bezpośredniego stosowania w polskim porządku prawnym RODO pojęcie „administratora systemu" nie jest już stosowane i nie ma przypisanego znaczenia prawnego), a w wielu dalszych przepisach *Regulaminu ProteGO Safe* mowa jest o „Administratorach" (patrz § 2 pkt 3 i n.), które to pojęcie ma zbiorczo obejmować Głównego Inspektora Sanitarnego i Ministra Cyfryzacji, choć istniejący między nimi stosunek prawny nie został wyjaśniony. W dokumencie *POLITYKA PRYWATNOŚCI*

[1)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

ProteGO Safe Minister Cyfryzacji został zaś pominięty w „Definicjach” (§ 2) i pojawia się dopiero w § 3 ust. 8 pkt 1 lit. a jako odbiorca zanonimizowanych danych i informacji z ProteGO Safe współpracujący z Administratorem Danych w celu rozwoju i utrzymania ProteGO Safe.

Jeśli dodać do tego, iż w całej dokumentacji Aplikacji wymieniana jest Infermedica Sp. z o.o. z siedzibą we Wrocławiu, a w dokumencie *POLITYKA PRYWATNOŚCI ProteGO Safe* także: TYTANI24 Sp. z o.o. z siedzibą we Wrocławiu, Google Ireland Limited, Centrum Systemów Informacyjnych Ochrony Zdrowia i Minister Zdrowia, których usytuowanie w ramach procesu przetwarzania danych osobowych z wykorzystaniem Aplikacji jest nieznane, to konieczność poprawienia dokumentacji aplikacji ProteGO Safe w zakresie statusu prawnego podmiotów współpracujących czy też współdziałających jawi się jako bezsporna – zgodnie z zasadą rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO) oraz celem zapewnienia integralności i poufności (art. 5 ust. 1 lit. f RODO) przetwarzanych danych osobowych.

Drugim zagadnieniem, co do którego zachodzi potrzeba jego dookreślenia i ostatecznego rozstrzygnięcia w dokumentacji Aplikacji, jest przesłanka dopuszczalności przetwarzania danych osobowych (art. 6 ust. 1 i art. 9 ust. 2 RODO). Zauważyć należy, że Komisja Europejska w części 3.3 „Podstawa prawna przetwarzania” „Instalacja aplikacji i przechowywanie informacji na urządzeniu użytkownika” akapit drugi *Komunikatu Komisji – Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych*, dalej „Wytyczne”, wyraźnie opowiedziała się za przesłanką zgody – art. 6 ust. 1 lit. a RODO i art. 9 ust. 2 lit. a RODO. Nadto w *Wytycznych 04/2020 o wykorzystaniu geolokalizacji i innych narzędzi ustalania kontaktów w kontekście wybuchu epidemii COVID-19*, wydanych przez Europejską Radę Ochrony Danych dnia 21 kwietnia 2020 r., wyrażono pogląd, że stosowanie aplikacji umożliwiających śledzenie kontaktów zakaźnych powinno być dobrowolne i nie powinno opierać się na śledzeniu przemieszczania się poszczególnych osób, lecz na informacjach o bliskości użytkowników.

Za – wyżej zaprezentowanymi – stanowiskami Komisji Europejskiej i Europejskiej Rady Ochrony Danych zdają się również optować autorzy dokumentacji aplikacji ProteGO Safe (§ 3 ust. 5 i 6 dokumentu *POLITYKA PRYWATNOŚCI ProteGO Safe*; § 2 pkt 7, § 3 ust. 4 i § 7 ust. 1 dokumentu *Regulamin ProteGO Safe*), a co za tym idzie niezrozumiałe jest, dlaczego w § 3 ust. 2 i 3 dokumentu *POLITYKA PRYWATNOŚCI ProteGO Safe* uznali, iż przetwarzanie danych osobowych Użytkowników

przez Administratora Danych (Głównego Inspektora Sanitarnego) odbywa się dla wypełnienia obowiązku prawnego (art. 6 ust. 1 lit. c RODO) albo ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego (art. 9 ust. 2 lit. i RODO).

Z problematyką zgody jako przesłanki legalizującej przetwarzanie wiążą się jeszcze dwie sprawy wymagające uregulowania – prawidłowe wykonywanie przez administratora obowiązku informacyjnego z art. 13 RODO wobec osób, które są użytkownikami Aplikacji (zwłaszcza w związku w wprowadzaniem kolejnych funkcjonalności aplikacji ProteGO Safe, które mogą znacząco wpłynąć na odbywający się za jej pośrednictwem proces przetwarzania danych osobowych, użytkownicy powinni być w sposób przejrzysty informowani o przysługujących im prawach wynikających z RODO, tak aby ich zgoda na przetwarzanie danych osobowych była świadoma i dobrowolna – art. 4 pkt 11 RODO) i rzetelne unormowanie zakresu danych osobowych, które będą przetwarzane z wykorzystaniem Aplikacji (§ 3 ust. 5 dokumentu *POLITYKA PRYWATNOŚCI ProteGO Safe* nie spełnia tego wymogu), by operacje przetwarzania realizowane za pośrednictwem aplikacji ProteGO Safe spełniały kryterium przejrzystości (art. 5 ust. 1 lit. a RODO) i były zgodne z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO).

Wreszcie – niebagatelne znaczenie ma, by w dokumentacji Aplikacji kategorycznie przesądzono, czy dane osobowe zbierane z pomocą aplikacji ProteGO Safe będą poddawane, silnie ingerującym w prywatność osób, których dane dotyczą, działaniom administratora, jakim jest profilowanie (art. 4 pkt 4 RODO). Należy zauważyć, iż w dokumencie *POLITYKA PRYWATNOŚCI ProteGO Safe* raz wskazuje się (§ 3 ust. 12), że dane osobowe Użytkownika nie będą poddawane profilowaniu, a raz dopuszcza się taką możliwość (§ 3 ust. 1 pkt 2). Niezbędnym jest, by dokumentacja aplikacji ProteGO Safe została ujednolicona w tym zakresie, przy czym organ właściwy w sprawie ochrony danych osobowych opowiada się przeciwko dopuszczalności profilowania, w przypadku gdy zasady tego profilowania, nawet w oparciu o zgodę, są w sposób nieprzejrzysty określone w dokumentacji Aplikacji.

Prezes Urzędu Ochrony Danych Osobowych zachęca także do przeprowadzenia oceny skutków dla ochrony danych, o której mowa w art. 35 RODO, w odniesieniu do aplikacji ProteGO Safe, co pozwoliłoby rozwiać wiele wątpliwości administratora. Nadmienić wypada, że Komisja Europejska w części 3.10 „Zaangażowanie organów ochrony danych" Wytycznych zaakcentowała potrzebę

przeprowadzenia oceny skutków dla ochrony danych w przypadku aplikacji tego rodzaju „Ze względu na to, że przetwarzanie danych w kontekście aplikacji będzie się kwalifikować jako przetwarzanie na dużą skalę szczególnych kategorii danych osobowych (tj. danych dotyczących zdrowia)…”.

Z wyrazami szacunku,

z up. Prezesa Urzędu Ochrony Danych Osobowych
Dyrektor Departamentu Orzecznictwa i Legislacji
Monika Krasińska
/ - podpisano elektronicznie/