

Olivier Micol

Bruksela, 14 kwietnia 2020 r.

Kierownik Działu, Komisja Europejska
DG ds. Sprawiedliwości i Konsumentów
Dział C.3 – Ochrona Danych
Belgia

Dotyczy: OUT2020-0028

Szanowny Panie,

bardzo dziękuję za nawiązanie współpracy i zwrócenie się do Europejskiej Rady Ochrony Danych (EROD) o poradę w sprawie projektu wytycznych dotyczących aplikacji, które pomagają w przeciwdziałaniu pandemii COVID-19. W istocie EROD dokłada starań, aby sprawnie prowadzić prace w tym zakresie: 19 marca opublikowała oświadczenie, a w przyszłym tygodniu planuje wydać dodatkowe wytyczne dotyczące śledzenia, badań naukowych i telepracy. Niektóre krajowe organy nadzorcze również opracowują wytyczne na poziomie krajowym, aby udzielić swoim rządów i operatorom telekomunikacyjnym porad w zakresie najlepszych sposobów przestrzegania przepisów o ochronie danych. EROD z zadowoleniem przyjmuje inicjatywę Komisji dotyczącą wypracowania ogólnoeuropejskiego i skoordynowanego podejścia, w ramach którego aplikacje mobilne mogą stać się jednym z proponowanych środków zwiększających możliwości osób fizycznych w przeciwdziałaniu pandemii. EROD wielokrotnie stwierdzała, że wdrażanie zasad ochrony danych i poszanowanie podstawowych praw i wolności to nie tylko obowiązek prawny, ale również wymóg służący zwiększaniu skuteczności inicjatyw związanych z danymi w celu zwalczania rozprzestrzeniania się wirusa wywołującego COVID-19 oraz w celu przekazywania informacji o strategiach deeskalacji.

EROD zdaje sobie sprawę, że nie ma żadnego uniwersalnego rozwiązania przedmiotowego problemu, a dostępne opcje wymagają uwzględnienia wielu czynników, w tym możliwego wpływu na zdrowie ludzi. Dlatego też przewidywane rozwiązania techniczne należy analizować szczegółowo i w sposób indywidualny. Dodatkowo EROD uważa, że właściwym krokiem jest podkreślenie zasadniczej potrzeby przeprowadzenia konsultacji z organami ochrony danych w celu zapewnienia przetwarzania danych osobowych zgodnie z prawem – z poszanowaniem praw osób fizycznych i przepisów dotyczących ochrony danych.

Tworzenie omawianych aplikacji powinno się odbywać w sposób odpowiedzialny, a odnośna ocena skutków w zakresie ochrony danych powinna obejmować wszystkie wdrożone mechanizmy ochrony

prywatności już w fazie projektowania i domyślnej ochrony prywatności. Kod źródłowy powinien być upubliczniony i poddany jak najszerzym badaniom prowadzonym przez naukowców.

Na tym etapie, na podstawie informacji przekazanych przez Komisję, EROD może się skupić jedynie na ogólnym celu przewidywanych aplikacji, polegającym na sprawdzeniu, czy są one zgodne z zasadami ochrony danych, oraz na mechanizmach służących wykonywaniu praw i wolności ludzi. EROD liczy, że dzięki temu Komisja bardziej szczegółowo rozważy niektóre elementy w celu ewentualnego dostosowania wybranych rozwiązań przedstawionych w dokumencie lub w celu przeanalizowania nowych opcji technicznych. W każdym razie EROD dokładniej zbada tę kwestię w najbliższych wytycznych.

W niniejszej odpowiedzi EROD chciałaby się w szczególności odnieść do stosowania aplikacji do ustalania kontaktów zakaźnych i funkcji ostrzegania, ponieważ na te obszary należy zwrócić większą uwagę w celu zminimalizowania ingerencji w życie prywatne, przy jednoczesnym umożliwieniu przetwarzania danych w celu ochrony zdrowia publicznego.

W przypadku, gdyby takie aplikacje okazały się odpowiednie we wdrażaniu niektórych elementów polityki zdrowia publicznego, ich maksymalną efektywność można osiągnąć jedynie, jeśli są one stosowane przez jak największą część ludności, we wspólnym dążeniu do zwalczania wirusa. Wszelka niejednorodność funkcji, brak interoperacyjności lub nawet indywidualne różnice w użyciu aplikacji mogą powodować negatywne efekty zewnętrzne w stosunku do innych osób i prowadzić do zmniejszenia korzyści zdrowotnych. EROD zdecydowanie popiera wnioski Komisji dotyczące dobrowolnego stosowania takich aplikacji: to osoby fizyczne powinny dokonywać tego wyboru w ramach wspólnej odpowiedzialności. Należy podkreślić, że dobrowolne stosowanie aplikacji wiąże się z zaufaniem danej osoby, a tym samym jeszcze bardziej odzwierciedla znaczenie zasad ochrony danych.

EROD podkreśla, że sam fakt wykorzystania funkcji ustalania kontaktów zakaźnych na zasadzie dobrowolności nie oznacza, że przetwarzanie danych osobowych przez organy publiczne musi odbywać się za zgodą danej osoby. Gdy organy publiczne świadczą usługę na podstawie mandatu powierzonego im mocą prawa i zgodnie z wymogami prawnymi, najważniejszą podstawą prawną przetwarzania danych jest, jak się wydaje, konieczność wykonania zadania w interesie publicznym. Podstawą prawną użycia aplikacji może być wdrażanie krajowych przepisów prawnych, zachęcających do ich dobrowolnego stosowania, bez żadnych negatywnych skutków dla osób, które ich nie używają. Takie interwencje ustawodawcze nie powinny w związku z tym służyć wywieraniu presji na obowiązkowe stosowanie danej aplikacji, a osoby fizyczne powinny mieć swobodę jej zainstalowania i odinstalowania według swojego uznania. Aktom prawnym mogą towarzyszyć odpowiednie działania komunikacyjne promujące dane narzędzia na poziomie krajowym, w tym kampanie informacyjne i pomoc dla małoletnich, osób z dysfunkcjami oraz grup społecznych o niższym poziomie umiejętności lub wykształcenia, aby zapobiec rozproszonemu stosowaniu aplikacji, brakiem wiedzy na temat rozprzestrzeniania się epidemii oraz potencjalnemu rozwarstwieniu w zakresie zdrowia. W istocie brak danych, wynikający z nieuważnego stosowania aplikacji przez użytkowników lub choćby z awarii baterii urządzenia, może poważnie obniżyć ogólną użyteczność społeczną takich instrumentów.

Aplikacje służące do ustalania kontaktów zakaźnych nie wymagają śledzenia lokalizacji poszczególnych użytkowników. Ich celem nie jest śledzenie przemieszczania się osób fizycznych ani egzekwowanie zaleceń. Ich głównym zadaniem jest wykrywanie zdarzeń (kontaktów z osobami z pozytywnym wynikiem testu), które są jedynie prawdopodobne, a dla większości użytkowników mogą nawet nie zaistnieć, zwłaszcza w fazie deeskalacji. Gromadzenie danych o przemieszczaniu się osób fizycznych w ramach aplikacji służących do ustalania kontaktów zakaźnych naruszałoby zasadę minimalizacji danych. Dodatkowo stwarzałoby poważne zagrożenia dla bezpieczeństwa i prywatności.

Organy służby zdrowia i naukowcy z tej dziedziny mogą wskazać, co ma być udostępnianym zdarzeniem w przypadku, miejscu i czasie jego zaistnienia, pod warunkiem rygorystycznego weryfikowania konieczności danej czynności na podstawie przepisów prawa; powinni też określić niektóre wymogi funkcjonalne aplikacji. Inną omawianą kwestią jest przechowywanie danych o zdarzeniach. Rozważa się dwa główne warianty: lokalne przechowywanie danych w urządzeniach osób fizycznych lub przechowywanie scentralizowane. EROD jest zdania, że oba warianty mogą być właściwymi rozwiązaniami alternatywnymi, pod warunkiem że zostaną wprowadzone odpowiednie środki bezpieczeństwa oraz pod warunkiem, że różne podmioty mogą być uznane również za administratorów danych w zależności od ostatecznego przeznaczenia aplikacji (np. administrator danych i przetwarzane dane mogą być inne w przypadku, gdy celem jest przekazywanie informacji w ramach aplikacji, i inne w przypadku, gdy celem jest na przykład telefoniczny kontakt z daną osobą). W każdym razie EROD chce podkreślić, że przechowywanie scentralizowane jest bardziej spójne z zasadą minimalizacji danych.

Ponadto przedmiotowe aplikacje nie są platformami społecznościowymi do rozpowszechniania społecznych ostrzeżeń lub wzbudzania jakiegokolwiek rodzaju stygmatyzacji. W rzeczywistości powinny być narzędziami do umożliwienia ludziom wypełnienia swojego zadania. Jak ujęto w projekcie wytycznych, ich wyłącznym celem jest, „aby organy publicznej opieki zdrowotnej zidentyfikowały osoby, które miały kontakt z osobą zakażoną COVID-19, wezwały je do samokwarantanny, szybko poddały je testom, a także udzieliły im, w odpowiednich przypadkach, informacji o kolejnych etapach, między innymi o tym, co należy robić w przypadku wystąpienia objawów”. W działaniach tych nadrzędne znaczenie ma jakość przetwarzanych danych. Kroki, które należy podjąć w celu „zidentyfikowania osób, które miały kontakt z osobą zakażoną COVID-19”, nie są łatwe i bezpośrednie. Powiadomienie danej osoby w aplikacji może się odbywać w taki sposób, aby były przetwarzane jedynie przypadkowo generowane pseudonimy. Dodatkowo powinien istnieć mechanizm zapewniający, aby w przypadku stwierdzenia, że jakaś osoba jest zakażona COVID-19, informacje wprowadzane do aplikacji były prawidłowe, ponieważ inne osoby mogą otrzymywać powiadomienia o tym, że są narażone. Mechanizm taki może wykorzystywać na przykład jednorazowy kod, który skanuje się w momencie odebrania wyniku testu. Każdy kontakt z daną osobą może nawiązać tylko organ służby zdrowia po dokonaniu oceny solidnych danych potwierdzających, przy jak najmniejszej dozie wnioskowania. Ponadto Komisja powinna wyjaśnić opisaną w wytycznych rolę „listy kontaktowej właściciela urzędu”.

Algorytmy wykorzystywane w aplikacjach służących do ustalania kontaktów zakaźnych powinny podlegać ścisłemu nadzorowi sprawowanemu przez wykwalifikowany personel w celu ograniczenia fałszywych wyników dodatnich i ujemnych, a zadanie „udzielania informacji o kolejnych etapach” nie może być w żadnym razie całkowicie zautomatyzowane. Zaleca się wprowadzenie mechanizmu kontaktu zwrotnego, w ramach którego zainteresowana osoba otrzymuje numer telefonu lub dostęp do kanału kontaktowego w celu uzyskania dodatkowych informacji od osoby obsługującej. Ponadto, aby zapobiegać stygmatyzacji, wspomniane „informacje” nie mogą zawierać żadnych potencjalnych elementów identyfikujących inną osobę, której dane dotyczą, a użycie aplikacji lub jej części (np. pulpitu, ustawień konfiguracji itp.) nie może pozwalać na ponowną identyfikację innych osób, niezależnie od tego, czy są one zakażone COVID-19 czy nie. EROD zdecydowanie zaleca, aby nie przechowywać żadnych bezpośrednich danych identyfikacyjnych w urządzeniach użytkowników i aby dane takie były w każdym razie jak najszybciej usuwane.

EROD zdecydowanie popiera zawartą w zaleceniach koncepcję, aby po zakończeniu obecnego kryzysu nie używać w dalszym ciągu przedmiotowego systemu zarządzania sytuacjami wyjątkowymi, a zebrane dane powinny, co do zasady, być usunięte lub zanonimizowane.

Wreszcie EROD i jej członkowie, którzy zajmują się udzielaniem porad i zapewnianiem prawidłowego stosowania RODO oraz dyrektywy o prywatności i łączności elektronicznej, powinni w pełni uczestniczyć w całym procesie opracowywania i wdrażania opisywanych środków. EROD przypomina, że zamierza opublikować w najbliższym czasie wytyczne dotyczące geolokalizacji i innych narzędzi służących do ustalania kontaktów zakaźnych w kontekście pandemii COVID-19.

Niezależnie od okoliczności EROD jest zawsze gotowa udzielać dalszych wskazówek instytucjom UE oraz wszystkim zainteresowanym stronom zaangażowanym w tworzenie i wykorzystywanie omawianych aplikacji mobilnych do przeciwdziałania COVID-19.

Z poważaniem

Andrea Jelinek