II

(Komunikaty)

KOMUNIKATY INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

KOMISJA EUROPEJSKA

KOMUNIKAT KOMISJI

Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych

(2020/C 124 I/01)

1 KONTEKST

Pandemia COVID-19 stanowi niespotykane dotąd wyzwanie dla Unii i państw członkowskich, ich systemów opieki zdrowotnej, stylu życia, stabilności gospodarczej i wartości. Technologie i dane cyfrowe mają do odegrania ważną rolę w walce z kryzysem związanym z COVID-19. Aplikacje mobilne instalowane zwykle na smartfonach (dalej „aplikacje") mogą pomagać organom ds. zdrowia w monitorowaniu i ograniczaniu pandemii COVID-19 na szczeblu krajowym i unijnym oraz mają szczególne znaczenie w fazie znoszenia środków ograniczających rozprzestrzenianie się tego wirusa. Mogą one udzielać bezpośrednich wskazówek obywatelom i wspierać ustalanie kontaktów zakaźnych. W wielu krajach, zarówno w UE, jak i na całym świecie, władze krajowe lub regionalne albo deweloperzy ogłosili wprowadzenie na rynek aplikacji o różnych funkcjach, mających na celu wspieranie walki z wirusem.

W dniu 8 kwietnia 2020 r. Komisja przyjęła zalecenie w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności (dalej „zalecenie") ([1]). Jednym z celów tego zalecenia jest ustanowienie wspólnego, koordynowanego na poziomie UE, podejścia europejskiego („zestaw instrumentów") do korzystania z aplikacji mobilnych, pomagających obywatelom w skutecznym ograniczeniu kontaktów personalnych oraz służących ostrzeganiu przed bliskimi kontaktami, zapobieganiu tym kontaktom oraz ustalaniu kontaktów zakaźnych, aby pomóc w ograniczeniu rozprzestrzeniania się pandemii COVID-19. W zaleceniu określono ogólne zasady, którymi należy się kierować przy opracowywaniu takiego zestawu narzędzi, oraz zapowiedziano publikację dalszych wytycznych Komisji, w tym wytycznych dotyczących ochrony danych osobowych i konsekwencji dla prywatności, jakie wiążą się z korzystaniem z tego typu aplikacji.

We wspólnym europejskim planie działania prowadzącym do zniesienia środków powstrzymujących rozprzestrzenianie się COVID-19 Komisja, we współpracy z przewodniczącym Rady Europejskiej, określiła szereg zasad, którymi należy się kierować podczas stopniowego wycofywania środków ograniczających rozprzestrzenianie się COVID-19 wprowadzonych w związku z pandemią. W tym kontekście ważną rolę mogą odegrać aplikacje mobilne, w tym funkcje ustalania kontaktów zakaźnych. W zależności od funkcji aplikacji i skali ich wykorzystania przez ludność, mogą one mieć znaczny wpływ na diagnozowanie i leczenie COVID-19, a także zarządzanie tą chorobą w szpitalach i poza nimi. Aplikacje odgrywają szczególną rolę w okresie, gdy znoszone są środki ograniczające rozprzestrzenianie się wirusa, a ryzyko infekcji rośnie wraz z wznowieniem kontaktów między ludźmi. Mogą one przyczynić się do szybszego i bardziej skutecznego przerywania łańcuchów zakażeń niż ogólne środki ograniczające rozprzestrzenianie się wirusa i znacznie zmniejszyć ryzyko. Powinny one zatem stanowić ważny element strategii wyjścia, uzupełniając inne środki, takie jak zwiększenie zdolności przeprowadzania testów ([2]). Istotnym warunkiem wstępnym, od którego będzie zależeć tworzenie tych aplikacji, a także ich akceptacja i wykorzystanie przez użytkowników, jest zaufanie. Obywatele muszą mieć pewność, że zapewniona jest zgodność z prawami podstawowymi i że aplikacje będą wykorzystywane wyłącznie do ściśle określonych celów, a nie do masowej inwigilacji oraz że osoby fizyczne zachowają kontrolę nad swoimi danymi. Dzięki temu aplikacje będą dysponować rzetelnymi

([1]) Zalecenie C(2020) 2296 final z dnia 8 kwietnia 2020 r. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

danymi i będą mogły skutecznie ograniczać rozprzestrzenianie się wirusa. Konieczne jest zatem zidentyfikowanie rozwiązań, które wiążą się z jak najmniejszą interwencją i są w pełni zgodne z wymogami dotyczącymi ochrony danych osobowych i prywatności wskazanymi w prawie UE. Oprócz tego aplikacje należy zdezaktywować najpóźniej w momencie, w którym ogłoszone zostanie opanowanie pandemii. Aplikacje powinny również zawierać najnowocześniejsze zabezpieczenia z zakresu ochrony informacji.

Niniejsze wytyczne uwzględniają wkład Europejskiej Rady Ochrony Danych (EROD) ([3]) oraz dyskusje w ramach sieci e-zdrowie. EROD planuje opublikować w najbliższych dniach wytyczne w sprawie geolokalizacji i innych narzędzi służących ustalaniu kontaktów w kontekście pandemii COVID-19.

Zakres niniejszych wytycznych

W celu zapewnienia spójnego w całej UE podejścia oraz określenia wytycznych dla państw członkowskich i twórców aplikacji w niniejszym dokumencie przedstawiono funkcje i wymogi, które powinny spełniać aplikacje, aby zapewnić zgodność z unijnymi przepisami w dziedzinie ochrony prywatności i danych osobowych, w szczególności z ogólnym rozporządzeniem o ochronie danych ([4]) (RODO) oraz dyrektywą o e-prywatności ([5]). Niniejsze wytyczne nie obejmują ewentualnych dodatkowych warunków, w tym ograniczeń, które państwa członkowskie mogłyby zawrzeć w swoich przepisach krajowych w odniesieniu do przetwarzania danych dotyczących zdrowia.

Niniejsze wytyczne nie są prawnie wiążące. Pozostają one bez uszczerbku dla roli Trybunału Sprawiedliwości UE, który jest jedyną instytucją mogącą dokonywać pełnomocnej wykładni prawa UE.

Niniejsze wytyczne dotyczą wyłącznie dobrowolnie stosowanych aplikacji pomocnych w walce z pandemią COVID 19 (aplikacje pobierane, instalowane i stosowane przez osoby fizyczne na zasadzie dobrowolności), które oferują co najmniej jedną z następujących funkcji:

— przekazywanie osobom fizycznym rzetelnych informacji o pandemii COVID-19;

— udostępnianie kwestionariuszy do samodzielnej diagnozy i wytycznych dla obywateli (funkcja weryfikacji objawów) ([6]);

— ostrzeżenia dla osób, które znajdowały się przez pewien czas w pobliżu osoby zakażonej, w celu przekazania informacji np. o konieczności samoizolacji i o miejscach, gdzie można poddać się badaniu (funkcja ustalania kontaktów zakaźnych i ostrzegania);

— zapewnienie forum komunikacji między pacjentami i lekarzami w przypadku samoizolacji lub zapewnienie dalszej diagnostyki i doradztwa w zakresie leczenia (wykorzystywanie telemedycyny na szerszą skalę).

Zgodnie z dyrektywą o e-prywatności narzucenie obowiązku stosowania aplikacji wiążącego się z prawami do poufności komunikacji, o których mowa w jej art. 5, jest możliwe jedynie w drodze przepisów prawa, które są konieczne, właściwe i proporcjonalne w celu ochrony pewnych celów szczegółowych. Biorąc pod uwagę fakt, że podejście to zakłada wysoki poziom interwencji, oraz wiążące się z nim wyzwania, dotyczące m.in. wprowadzenia odpowiednich zabezpieczeń, Komisja jest zdania, że przed wprowadzeniem takiego rozwiązania należy przeprowadzić dokładną analizę. Z powyższych względów Komisja zaleca korzystanie z dobrowolnie stosowanych aplikacji.

Niniejsze wytyczne nie obejmują aplikacji mających na celu egzekwowanie obowiązku kwarantanny (w tym aplikacji, których stosowanie jest obowiązkowe).

2 WKLAD APLIKACJI W WALKE Z COVID-19

Funkcja weryfikacji objawów to narzędzie przeznaczone dla organów zdrowia publicznego, aby mogły udzielać obywatelom wskazówek dotyczących badań na obecność COVID-19, jak również przekazywać informacje o samoizolacji, sposobach unikania zakażenia innych osób oraz potrzebie zgłoszenia się po pomoc medyczną. Może być ona również uzupełnieniem podstawowej opieki zdrowotnej i zapewniać lepsze informacje na temat wskaźników zakażeń COVID-19 w danej populacji.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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 (ogólne rozporządzenie o ochronie danych), Dz.U. L 119 z 4.5.2016, s. 1.

([5]) Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37.

([6]) Jeżeli aplikacje dostarczają informacji związanych z diagnozą, zapobieganiem, monitorowaniem, przewidywaniem lub prognozowaniem, należy ocenić ich potencjalną kwalifikację jako wyroby medyczne zgodnie z ramami regulacyjnymi dotyczącymi wyrobów medycznych. Zob. przedmiotowe ramy prawne: dyrektywa Rady 93/42/EWG z dnia 14 czerwca 1993 r. dotycząca wyrobów medycznych (Dz.U. L 169 z 12.7.1993, s. 1) i rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych (Dz.U. L 117 z 5.5.2017, s. 1).

Funkcja ustalania kontaktów zakaźnych i ostrzegania to narzędzie pozwalające identyfikować osoby, które znalazły się w pobliżu osoby zakażonej COVID-19, oraz poinformować je o właściwych sposobach działania w takiej sytuacji, np. o potrzebie poddania się kwarantannie w domu czy testom na obecność wirusa. Zapewnia również porady na wypadek wystąpienia objawów choroby. Funkcja ta jest zatem przydatna zarówno dla obywateli, jak i organów zdrowia publicznego. Może ona również odgrywać ważną rolę w zarządzaniu środkami ograniczającymi rozprzestrzenianie się wirusa w fazie deeskalacji. Jej wpływ można zwiększyć za pomocą strategii wspierającej szerzej zakrojone testowanie osób z łagodnymi objawami.

Obie te funkcje mogą również stanowić istotne źródło danych dla organów zdrowia publicznego i ułatwić przekazywanie takich danych krajowym organom epidemiologicznym oraz Europejskiemu Centrum ds. Zapobiegania i Kontroli Chorób (ECDC). Ułatwiłoby to zrozumienie sposobów rozprzestrzeniania się choroby oraz, w połączeniu z wynikami badań, oszacowanie wartości predykcyjnej wyniku dodatniego dla objawów z układu oddechowego w danej społeczności i zapewnienie informacji na temat poziomu występowania wirusa.

Wiarygodność danych szacunkowych jest bezpośrednio powiązana z liczbą i wiarygodnością przekazywanych danych.

W związku z tym, w połączeniu z odpowiednimi strategiami wykonywania testów, zarówno funkcja weryfikacji objawów, jak i funkcja ustalania kontaktów zakaźnych mogą dostarczyć informacji na temat poziomu występowania wirusa, a także pomóc w ocenie skuteczności środków służących ograniczeniu kontaktów i środków izolacji. Jak określono w zaleceniu, w celu umożliwienia współpracy transgranicznej oraz w celu zapewnienia wykrywania kontaktów między użytkownikami różnych aplikacji (co jest szczególnie ważne w przypadku przemieszczania się obywateli przez granice) należy zadbać o interoperacyjność między rozwiązaniami informatycznymi w poszczególnych państwach członkowskich. Jeżeli osoba zakażona pozostaje w kontakcie z użytkownikiem aplikacji z innego państwa członkowskiego, powinno być możliwe transgraniczne przekazywanie danych osobowych takiego użytkownika organom ds. zdrowia w jego państwie członkowskim w zakresie, w jakim jest to absolutnie niezbędne. Prace nad tym zagadnieniem będą prowadzone w ramach zestawu instrumentów zapowiedzianych w zaleceniu. Interoperacyjność należy zapewnić zarówno za pomocą odpowiednich wymagań technicznych, jak i poprawy komunikacji i współpracy między krajowymi organami ds. zdrowia. Jako model zarządzania na potrzeby aplikacji służących ustalaniu kontaktów zakaźnych w czasie pandemii COVID-19 można również wykorzystać jeden z modeli szczególnej współpracy ([7]).

3 ELEMENTY ZAPEWNIAJACE WIARYGODNE I ODPOWIEDZIALNE WYKORZYSTANIE APLIKACJI

Funkcje aplikacji mogą mieć wpływ na szeroki zakres praw zapisanych w Karcie praw podstawowych Unii Europejskiej, takich jak godność ludzka, poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, swoboda przemieszczania się, niedyskryminacja, wolność prowadzenia działalności gospodarczej oraz wolność zrzeszania się i zgromadzeń. Naruszenie prywatności i prawo do ochrony danych osobowych mogą mieć szczególne znaczenie ze względu na fakt, że niektóre z funkcji aplikacji opierają się na modelu intensywnego przetwarzania danych.

Przedstawione poniżej elementy mają na celu zapewnienie wskazówek, jak ograniczyć inwazyjność funkcji aplikacji w celu zapewnienia zgodności z przepisami UE w zakresie ochrony danych osobowych i prywatności.

3.1 Krajowe organy ds. zdrowia (lub podmioty realizujące zadania w dziedzinie zdrowia w interesie publicznym) jako administrator danych

Określenie, kto podejmuje decyzje co do środków i celów przetwarzania danych (tzn. kto jest administratorem danych), ma kluczowe znaczenie dla ustalenia, kto jest odpowiedzialny za przestrzeganie unijnych przepisów o ochronie danych osobowych, a w szczególności: kto powinien przekazywać informacje osobom pobierającym daną aplikację na temat przetwarzania ich danych osobowych (już istniejących lub które mają być generowane za pośrednictwem danego urządzenia, np. smartfonu, na którym aplikacja jest instalowana), jakie będą ich prawa, kto będzie odpowiedzialny w przypadku naruszenia ochrony danych itp.

Ze względu na wrażliwy charakter takich danych osobowych oraz cele ich przetwarzania opisane poniżej, Komisja uważa, że aplikacje należy zaprojektować w taki sposób, by administratorem danych były krajowe organy ds. zdrowia (lub podmioty realizujące zadania w dziedzinie zdrowia w interesie publicznym) ([8]). Administratorzy są odpowiedzialni za zgodność z RODO (zasada rozliczalności). Zakres dostępu do danych powinien być ograniczony w oparciu o zasady opisane w sekcji 3.5 poniżej.

([7]) Tego typu współpraca ma już miejsce. Przykładem jest projekt MyHealth@EU służący wymianie kartotek pacjentów oraz elektronicznych recept. Zob. również art. 5 ust. 5 i motyw 17 decyzji wykonawczej Komisji 2019/1765.

([8]) Zob. motyw 45 RODO.

Takie rozwiązanie będzie sprzyjać większemu zaufaniu społecznemu a tym samym akceptacji takich aplikacji (i leżących u ich podstaw systemów przekazywania informacji o łańcuchach zakażeń), dzięki czemu będą one mogły spełnić przypisaną im rolę, jaką jest ochrona zdrowia publicznego. Właściwe krajowe organy ds. zdrowia powinny odpowiednio dostosować i wdrożyć w skoordynowany sposób odnośne polityki, wymogi i kontrole.

3.2 **Zapewnienie, by obywatel miał kontrolę**

Decydującym czynnikiem zaufania obywateli do aplikacji jest pokazanie, że mają kontrolę nad swoimi danymi osobowymi. Aby to zapewnić, należy – zdaniem Komisji – spełnić w szczególności następujące warunki:

— zainstalowanie aplikacji na urządzeniu powinno być dobrowolne i nie powinno być żadnych negatywnych konsekwencji dla osoby, która zdecydowała się nie pobrać lub nie używać danej aplikacji;

— poszczególne funkcje aplikacji (np. funkcja informacyjna, funkcja weryfikacji objawów oraz funkcja ustalania kontaktów zakaźnych i ostrzegania) nie powinny być powiązane, tak aby osoba fizyczna mogła udzielić odrębnej zgody na każdą funkcję. Nie powinno to jednak uniemożliwiać użytkownikowi łączenia różnych funkcji aplikacji, jeżeli dostawca oferuje taką możliwość;

— jeżeli wykorzystuje się dane dotyczące bliskości fizycznej (dane generowane przez sygnały Bluetooth o niskim zużyciu energii pomiędzy dwoma urządzeniami znajdującymi się w odległości mającej znaczenie z epidemiologicznego punktu widzenia i w okresie zagrożenia epidemiologicznego), dane te powinny być przechowywane na urządzeniu użytkownika. Jeśli takie dane miałyby być udostępnione organom ds. zdrowia, powinny zostać przekazane dopiero po potwierdzeniu, że dana osoba jest zakażona COVID-19, i pod warunkiem, że osoba ta wyrazi na to zgodę;

— organy ds. zdrowia powinny zapewnić obywatelom wszelkie niezbędne informacje dotyczące przetwarzania ich danych osobowych (zgodnie z art. 12 i art. 13 RODO oraz art. 5 dyrektywy o prywatności i łączności elektronicznej);

— obywatele powinni mieć możliwość korzystania z praw przysługujących im na mocy RODO (w szczególności prawa dostępu do danych oraz prawa do sprostowania i usunięcia danych osobowych). Wszelkie przypadki ograniczenia praw wynikających z RODO oraz dyrektywy o prywatności i łączności elektronicznej powinny być zgodne z tymi aktami oraz powinny być konieczne, proporcjonalne i przewidziane w przepisach;

— aplikacje należy zdezaktywować najpóźniej w momencie, w którym ogłoszone zostanie opanowanie pandemii. Ich dezaktywacja nie powinna wymagać usunięcia aplikacji z urządzenia przez użytkownika.

3.3 **Podstawa prawna przetwarzania**

Instalacja aplikacji i przechowywanie informacji na urządzeniu użytkownika

Jak zauważono powyżej, na mocy dyrektywy o prywatności i łączności elektronicznej (art. 5) przechowywanie informacji na urządzeniu użytkownika lub uzyskanie dostępu do informacji już przechowywanych jest dozwolone tylko wtedy, gdy (i) użytkownik wyraził zgodę lub (ii) przechowywanie lub dostęp są ściśle niezbędne dla danej usługi społeczeństwa informacyjnego (np. aplikacji) wyraźnie zażądanej (tj. zainstalowanej i aktywowanej) przez użytkownika.

Przechowywanie informacji na urządzeniu użytkownika oraz uzyskanie dostępu do informacji już przechowywanych na tym urządzeniu jest zazwyczaj niezbędne do funkcjonowania aplikacji. Ponadto funkcja ustalania kontaktów zakaźnych i ostrzegania wymaga przechowywania na urządzeniu użytkownika niektórych dodatkowych informacji (takich jak tymczasowe, okresowo zmieniane pseudonimy, identyfikatory użytkowników tej funkcji znajdujących się w pobliżu). Ponadto funkcja ta mogłaby wymagać wysyłania przez użytkowników (zakażonych lub prawdopodobnie zakażonych) danych dotyczących bliskości fizycznej. Takie wysyłanie nie jest niezbędne do funkcjonowania aplikacji jako takiej. W związku z tym wymogi dotyczące wariantu (ii), o którym mowa w poprzednim akapicie, nie są spełnione. Oznacza to, że zgoda (wariant (i) powyżej) stanowi najbardziej odpowiednią podstawę dla przedmiotowych działań. Taka zgoda powinna być „dobrowolna", „konkretna", „jednoznaczna" i „świadoma" w rozumieniu RODO. Powinna być wyrażona poprzez wyraźne działanie danej osoby; wyklucza to milczące formy zgody (np. milczenie; brak reakcji) ([9]).

([9]) Zob. wytyczne Europejskiej Rady Ochrony Danych w sprawie zgody: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Podstawa prawna przetwarzania danych przez krajowe organy ds. zdrowia – prawo Unii lub prawo państwa członkowskiego

Krajowe organy ds. zdrowia zazwyczaj przetwarzają dane osobowe, gdy istnieje prawny obowiązek przewidziany w prawie UE lub w prawie państwa członkowskiego, który przewiduje takie przetwarzanie i spełnia warunki określone w art. 6 ust. 1 lit. c) i art. 9 ust. 2 lit. i) RODO, lub gdy takie przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym uznanym przez prawo UE lub prawo państwa członkowskiego ([10]).

Wszelkie przepisy krajowe muszą przewidywać konkretne i odpowiednie środki ochrony praw i wolności osób, których dane dotyczą. Zasadniczo im większy wpływ danego środka na swobody osób fizycznych, tym silniejsze zabezpieczenia należy przewidzieć w odpowiednich przepisach.

Przepisy UE i państw członkowskich istniejące przed wybuchem pandemii COVID-19, a także przepisy przyjmowane w wielu państwach członkowskich w celu zwalczania rozprzestrzeniania się epidemii mogą, co do zasady, być wykorzystywane jako podstawa prawna przetwarzania danych osób fizycznych, jeżeli przewidują środki umożliwiające monitorowanie epidemii oraz spełniają dalsze wymogi określone w art. 6 ust. 3 RODO.

Ze względu na charakter odnośnych danych osobowych (w szczególności danych dotyczących zdrowia jako szczególnej kategorii danych osobowych), a także okoliczności związanych z obecną pandemią COVID-19, oparcie się na prawie jako podstawie prawnej przyczyniłby się do pewności prawnej, ponieważ prawo to (i) przewidywałoby szczegółowo przetwarzanie konkretnych danych dotyczących zdrowia i jasno określałoby cele przetwarzania; (ii) wyraźnie wskazywałoby, kto jest administratorem danych, tj. podmiotem przetwarzającym dane, i kto oprócz administratora może mieć dostęp do takich danych; (iii) wykluczałoby możliwość przetwarzania takich danych w celach innych niż te wymienione w prawodawstwie oraz (iv) przewidywałoby konkretne zabezpieczenia. Aby nie podważać użyteczności publicznej i akceptacji dla przedmiotowych aplikacji, prawodawca krajowy powinien zwrócić szczególną uwagę na to, by wybrane rozwiązanie jak najbardziej sprzyjało włączeniu obywateli.

Przetwarzanie danych przez organy ds. zdrowia na podstawie przepisów nie zmienia faktu, że osoby fizyczne zachowują swobodę zainstalowania aplikacji oraz swobodę dzielenia się swoimi danymi z organami ds. zdrowia. W związku z tym odinstalowanie aplikacji nie powinno mieć negatywnego wpływu na użytkowników.

Aplikacje służące ustalaniu kontaktów zakaźnych oraz aplikacje ostrzegawcze umożliwiają ostrzeganie osób fizycznych. W przypadku gdy takie ostrzeżenie jest przekazywane bezpośrednio przez aplikację, Komisja zwraca uwagę na zakaz poddawania osób fizycznych decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, która wywołuje skutek prawny lub w podobny sposób istotnie na te osoby wpływa (art. 22 RODO).

3.4 **Minimalizacja danych**

Dane uzyskane za pośrednictwem urządzeń i już wcześniej przechowywane na tych urządzeniach są chronione w następujący sposób:

— Jako „dane osobowe", tj. wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 1 RODO), są one chronione na mocy RODO. Dane dotyczące zdrowia korzystają z dodatkowej ochrony (art. 9 RODO).

— Jako „dane dotyczące lokalizacji", tj. dane przetwarzane w sieci łączności elektronicznej lub przez usługę łączności elektronicznej, wskazujące położenie geograficzne terminala użytkownika, są one chronione na mocy dyrektywy o prywatności i łączności elektronicznej (art. 5 ust. 1, art. 6 i art. 9) ([11]).

— Wszelkie informacje przechowywane na urządzeniu końcowym użytkownika i pozyskiwane z takiego urządzenia są chronione na mocy art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

Dane nieosobowe (takie jak dane nieodwracalnie zanonimizowane) nie są chronione na mocy RODO.

Komisja przypomina, że zasada minimalizacji danych wymaga, aby przetwarzane były wyłącznie dane osobowe, które są adekwatne, stosowne i ograniczone do tego, co jest niezbędne do osiągnięcia celu ([12]). Ocena konieczności przetwarzania danych osobowych i ich stosowności powinna być przeprowadzana w świetle zamierzonego celu lub celów.

Komisja zauważa na przykład, że jeżeli celami danej funkcji jest weryfikacja objawów lub telemedycyna, to cele te nie wymagają dostępu do listy kontaktowej osoby będącej właścicielem danego urządzenia.

([10]) Art. 6 ust. 1 lit. e) RODO.

([11]) W Europejskim kodeksie łączności elektronicznej przewidziano, że objęte są również usługi, które są funkcjonalnie równoważne usługom łączności elektronicznej.

([12]) Zasada minimalizacji danych.

Generowanie i przetwarzanie mniejszej ilości danych ogranicza zagrożenia dla bezpieczeństwa. W związku z tym zgodność z zasadami dotyczącymi minimalizacji danych stanowi również zabezpieczenie w zakresie bezpieczeństwa.

— Funkcja informacyjna:

Aplikacja, która zawiera jedynie tę funkcję, nie będzie musiała przetwarzać żadnych danych dotyczących zdrowia osób fizycznych. Będzie im jedynie dostarczała informacji. Aby zrealizować ten cel nie można przetwarzać informacji przechowywanych na urządzeniu końcowym i z niego pozyskiwanych poza tym, co jest niezbędne do dostarczenia informacji.

— Funkcja weryfikacji objawów i funkcja telemedycyny:

Jeżeli aplikacja zawiera jedną lub dwie z tych funkcji, będzie przetwarzała dane osobowe dotyczące zdrowia. W związku z tym wykaz danych, które mogą być przetwarzane, powinien zostać określony w podstawowych przepisach mających zastosowanie do organów ds. zdrowia.

Ponadto organy ds. zdrowia mogą potrzebować numerów telefonów osób, które korzystały z funkcji weryfikacji objawów i załadowały wyniki. Informacje przechowywane na urządzeniu końcowym i pozyskiwane z takiego urządzenia mogą być przetwarzane tylko w takim zakresie, w jakim jest to niezbędne do osiągnięcia celu aplikacji i umożliwienia jej prawidłowego funkcjonowania.

— Funkcja ustalania kontaktów zakaźnych i ostrzegania:

W większości przypadków zakażenie COVID-19 powodują kropelki, które przemieszczają się tylko w ograniczonej odległości. Jak najszybsze wykrycie osób, które przebywały w pobliżu osoby zakażonej, ma kluczowe znaczenie dla przerwania łańcucha zakażeń. Bliskość fizyczną określa się w funkcji odległości i czasu trwania kontaktu i czynność ta powinna być przeprowadzana z punktu widzenia epidemiologicznego. Przerwanie łańcucha zakażeń jest szczególnie istotne dla uniknięcia ponownego wzrostu liczby zakażeń w fazie wychodzenia z kryzysu.

W tym celu niezbędne mogą się okazać dane na temat bliskości fizycznej. Wydaje się, że łączność między urządzeniami za pośrednictwem standardu Bluetooth Low Energy (BLE) do celów pomiarów bliskości fizycznej i bliskich kontaktów jest bardziej precyzyjna, a co za tym idzie odpowiedniejsza, niż wykorzystanie danych geolokalizacyjnych (GNSS/GPS lub dane dotyczące lokalizacji telefonów komórkowych). Standard BLE pozwala uniknąć możliwości śledzenia (w przeciwieństwie do danych geolokalizacyjnych). W związku z tym Komisja zaleca stosowanie danych pochodzących z łączności BLE (lub danych generowanych przez równoważną technologię) do celów ustalania bliskości fizycznej.

Dane dotyczące lokalizacji nie są konieczne do celów funkcji ustalania kontaktów zakaźnych, ponieważ ich zadaniem nie jest śledzenie przepływu osób lub egzekwowanie zaleceń. Ponadto przetwarzanie danych dotyczących lokalizacji w kontekście ustalania kontaktów zakaźnych byłoby trudne do uzasadnienia w świetle zasady minimalizacji danych i może prowadzić do problemów w kwestii bezpieczeństwa i prywatności. Z tego powodu Komisja odradza stosowanie w tym kontekście danych dotyczących lokalizacji.

Niezależnie od środków technicznych użytych do ustalenia bliskości fizycznej, nie wydaje się konieczne przechowywanie dokładnego czasu lub miejsca kontaktu (jeżeli informacje te są dostępne). Przydatne może być jednak przechowywanie daty kontaktu, aby możliwe było zweryfikowanie, czy kontakt miał miejsce w okresie występowania objawów choroby (lub w ciągu 48 godzin przed ich wystąpieniem ([13])), a także w celu ukierunkowania informacji o działaniach następczych, na przykład zawierających porady co do tego, na jak długo należy poddać się samoizolacji.

Dane na temat bliskości fizycznej powinny być generowane i przetwarzane wyłącznie wtedy, gdy istnieje rzeczywiste ryzyko zakażenia (w zależności od bliskości i czasu trwania kontaktu).

Należy zauważyć, że konieczność i proporcjonalność gromadzenia danych będzie zatem zależeć od takich czynników, jak stopień dostępności infrastruktury do przeprowadzania testów, w szczególności w przypadku, gdy zarządzone już zostały takie środki jak izolacja. Istnieją dwa sposoby przekazania ostrzeżenia osobom, które znalazły się w ścisłym kontakcie z zakażoną osobą.

Zgodnie z pierwszym podejściem ostrzeżenie jest wysyłane automatycznie za pośrednictwem aplikacji do bliskich kontaktów, gdy użytkownik powiadomi aplikację – za zgodą lub po potwierdzeniu przez organ ds. zdrowia, na przykład za pomocą kodu QR lub kodu TAN – że uzyskał pozytywny wynik testu (proces zdecentralizowany). Treść ostrzeżenia powinna zostać określona przez organ ds. zdrowia. Zgodnie z drugim podejściem wygenerowane przez system tymczasowe identyfikatory są przechowywane na oddzielnym serwerze znajdującym się w posiadaniu organu ds. zdrowia (rozwiązanie z wykorzystaniem oddzielnego serwera). Użytkowników nie wolno bezpośrednio identyfikować za pomocą tych danych. Dzięki identyfikatorom użytkownicy, którzy znajdowali się w bliskim kontakcie z użytkownikiem, który uzyskał pozytywny wynik testu, otrzymują ostrzeżenie na swoim urządzeniu. Jeżeli organy ds. zdrowia pragną skontaktować się z użytkownikami, którzy pozostawali w bliskim kontakcie z zakażoną osobą, również za pośrednictwem telefonu lub wiadomości SMS, muszą uzyskać zgodę tych użytkowników na przekazanie ich numerów telefonu.

([13]) Osoba zakażona zaraża 48 godzin przed wystąpieniem objawów.

3.5 **Ograniczenie ujawniania danych/dostępu do danych**

— Funkcja informacyjna:

Organom ds. zdrowia nie mogą być udostępniane żadne informacje przechowywane na urządzeniu końcowym i dostępne na tym urządzeniu oprócz tych, które są niezbędne do zapewnienia funkcji informacyjnej. Ponieważ funkcja ta stanowi jedynie środek komunikacji, organy ds. zdrowia nie będą miały dostępu do żadnych innych danych.

— Funkcja weryfikacji objawów i funkcja telemedycyny:

Funkcja weryfikacji objawów może okazać się użyteczna dla państw członkowskich, które będą chciały pomóc obywatelom w ustaleniu, czy powinni się poddać testom, a także dostarczyć im informacji na temat izolacji oraz o tym, kiedy i jak uzyskać dostęp do opieki zdrowotnej, w szczególności w przypadku grup ryzyka. Może być ona również uzupełnieniem podstawowej opieki zdrowotnej i pomóc uzyskać informacje na temat wskaźników zakażeń COVID-19 w obrębie populacji. W związku z tym można podjąć decyzję, że odpowiedzialne organy ds. zdrowia i krajowe organy epidemiologiczne powinny uzyskać dostęp do informacji dostarczonych przez pacjenta. ECDC mogłoby otrzymywać zagregowane dane od krajowych organów w zakresie nadzoru epidemiologicznego.

Jeżeli wybrano udzielenie zgody na kontakt z urzędnikami służby zdrowia, a nie tylko kontakt za pomocą samej aplikacji, wówczas konieczne jest również ujawnienie krajowym organom ds. zdrowia numeru telefonu użytkowników aplikacji.

— Funkcja ustalania kontaktów zakaźnych i ostrzegania:

— Dane osoby zakażonej

Aplikacje generują pseudolosowo tymczasowe i okresowo zmieniające się identyfikatory telefonów, które pozostają w kontakcie z użytkownikiem. Jedna z opcji opiera się na zasadzie, że identyfikatory są przechowywane na urządzeniu użytkownika (tzw. procedura zdecentralizowana). W ramach drugiej opcji przewiduje się, że te wygenerowane przez system identyfikatory są przechowywane na serwerze, do którego mają dostęp organy ds. zdrowia (tzw. rozwiązanie z wykorzystaniem serwera). Rozwiązanie zdecentralizowane jest bardziej zgodne z zasadą minimalizacji. Organy ds. zdrowia powinny mieć dostęp wyłącznie do danych o bliskości fizycznej z urządzenia osoby zakażonej, tak aby były w stanie skontaktować się z osobami zagrożonymi zakażeniem.

Dane te będą dostępne dla organów ds. zdrowia dopiero wtedy, gdy osoba zakażona (po poddaniu się testowi) w sposób aktywny je im udostępni.

Osoba zakażona nie powinna być informowana o tożsamości osób, z którymi miała kontakt prowadzący potencjalnie do konsekwencji epidemiologicznych, i które zostaną o tym powiadomione.

— Dane osób, które miały kontakt (epidemiologiczny) z osobą zakażoną

Tożsamości osoby zakażonej nie należy ujawniać osobom, z którymi miała kontakt epidemiologiczny. Wystarczające jest poinformowanie ich o tym, że w ciągu ostatnich 16 dni znalazły się w kontakcie epidemiologicznym z zakażoną osobą. Jak zauważono powyżej, dane dotyczące czasu i miejsca takich kontaktów nie powinny być przechowywane. Przekazywanie tych danych nie jest zatem ani konieczne ani możliwe.

W celu prześledzenia kontaktów epidemiologicznych użytkownika aplikacji, u którego stwierdzono zakażenie, krajowe organy ds. zdrowia powinny być informowane wyłącznie o identyfikatorze osoby, z którą dana osoba miała kontakt epidemiologiczny w okresie od 48 godzin przed wystąpieniem objawów do 14 dni po wystąpieniu objawów, w oparciu o bliskość fizyczną i czas trwania kontaktu.

ECDC mogłoby otrzymywać zagregowane dane dotyczące ustalania kontaktów zakaźnych od organów krajowych do celów prowadzenia nadzoru epidemiologicznego nad wskaźnikami określonymi we współpracy z państwami członkowskimi.

3.6 **Określenie dokładnych celów przetwarzania**

Podstawa prawna (prawo Unii lub prawo państwa członkowskiego) powinna określać cel przetwarzania. Cel powinien być szczegółowo określony, tak aby nie było wątpliwości, jakiego rodzaju dane osobowe muszą zostać przetworzone w celu osiągnięcia pożądanego celu oraz jednoznaczny. .

Dokładny cel lub cele zależeć będą od funkcji, jakie spełnia dana aplikacja. Każdej z funkcji można przypisać kilka celów. Aby zapewnić osobom pełną kontrolę nad dotyczącymi ich danymi, Komisja zaleca, by poszczególne funkcje nie były łączone. Niezależnie od przypadku osoby powinny mieć możliwość wyboru między różnymi funkcjami, które służą każda innemu celowi.

Komisja odradza wykorzystywanie danych zebranych na powyżej określonych warunkach do celów innych niż walka z COVID-19. Jeśli konieczne będą cele takie jak badania naukowe czy statystyka, powinny one figurować w pierwotnym wykazie celów, a użytkownicy powinni być wyraźnie o nich powiadomieni.

— Funkcja informacyjna:

Celem tej funkcji jest dostarczanie informacji istotnych z punktu widzenia organów ds. zdrowia w kontekście kryzysu.

— Funkcja weryfikacji objawów i funkcja telemedycyny:

Funkcja weryfikacji objawów może pomóc ustalić, jaki odsetek osób wykazujących objawy choroby COVID-19 jest faktycznie zakażonych (np. przez pobieranie wymazów i poddawanie testom wszystkich lub wybranych losowo osób, które mają takie objawy, jeśli jest to możliwe do przeprowadzenia). Cel określany w tym przypadku powinien jasno wskazywać, że dane osobowe dotyczące zdrowia będą przetwarzane w celu (i) umożliwienia osobom na podstawie zestawu pytań dokonania samooceny, czy występują u nich objawy COVID-19 lub (ii) uzyskania porady medycznej w przypadku wystąpienia objawów COVID-19.

— Funkcja ustalania kontaktów zakaźnych i ostrzegania:

Samo wskazanie celu „zapobiegania dalszym zakażeniom COVID-19" nie jest wystarczająco szczegółowe. W tym przypadku Komisja zaleca dokładniejsze określenie celu (celów) w sposób zbliżony do następującego: „zachowywanie kontaktów osób, które korzystają z aplikacji i które mogły być narażone na zakażenie COVID-19 w celu ostrzeżenia tych osób, które potencjalnie mogły zostać zakażone".

3.7 **Ustalenie ścisłych ograniczeń dotyczących przechowywania danych**

Zasada ograniczenia przechowywania wymaga, aby dane osobowe nie były przechowywane dłużej, niż jest to konieczne. Okres przechowywania danych powinien zależeć od istotności tych danych z medycznego punktu widzenia (zgodnie z celem aplikacji: okres inkubacji itd.) oraz uwzględniać realistyczny termin realizacji czynności administracyjnych, które być może będzie należało wykonać.

— Funkcja informacyjna:

Jeśli jakiekolwiek dane są gromadzone przy instalowaniu tej funkcji, powinny być one natychmiast usunięte. Przechowywanie takich danych jest nieuzasadnione.

— Funkcja weryfikacji objawów i funkcja telemedycyny:

Te dane powinny zostać usunięte przez organy ds. zdrowia najpóźniej po miesiącu (okres inkubacji plus margines) lub po tym, jak dana osoba została zbadana, a wynik okazał się negatywny. Organy ds. zdrowia mogą przechowywać dane przez dłuższy okres do celów sprawozdawczości w ramach nadzoru i do celów badawczych, o ile są one zanonimizowane.

— Funkcja ustalania kontaktów zakaźnych i ostrzegania:

Dane dotyczące bliskości fizycznej powinny być usuwane, jak tylko przestają być potrzebne do celów ostrzegania. Powinno to mieć miejsce najpóźniej po miesiącu (okres inkubacji plus margines) lub po tym, jak dana osoba została zbadana, a wynik okazał się negatywny. Organy ds. zdrowia mogą przechowywać dane dotyczące bliskości fizycznej przez dłuższy okres do celów sprawozdawczości w ramach nadzoru i do celów badawczych, o ile są one zanonimizowane.

Dane powinny być przechowywane na urządzeniu użytkownika, a na serwer dostępny dla organów ds. zdrowia powinny trafiać jedynie te dane, które zostały przekazane przez użytkowników i które są niezbędne do osiągnięcia danego celu, o ile taka opcja jest przewidziana (tj. na serwer ładowane są wyłącznie dane dotyczące bliskich kontaktów osoby, u której badanie potwierdziło zakażenie COVID-19).

3.8 **Zapewnienie bezpieczeństwa danych**

Komisja zaleca, aby dane przechowywane były na urządzeniu końcowym użytkownika w zaszyfrowanej formie, przy zastosowaniu najnowocześniejszych technik kryptograficznych. Jeżeli dane przechowywane są na serwerze centralnym, należy wprowadzić logowanie w celu uzyskania dostępu, w tym dostępu administracyjnego.

Dane dotyczące bliskości fizycznej powinny być generowane i przechowywane na urządzeniu końcowym wyłącznie w zaszyfrowanej i spseudonimizowanej formie. Aby zapewnić, że śledzenie przez osoby trzecie nie będzie możliwe, należy zapewnić możliwość aktywacji Bluetooth bez konieczności aktywacji innych usług lokalizacji.

Przy gromadzeniu danych dotyczących bliskości fizycznej za pośrednictwem technologii BLE preferowane jest tworzenie i przechowywanie tymczasowych identyfikatorów użytkownika, które regularnie zmieniają się, a nie przechowywanie samego identyfikatora urządzenia. Ten środek pozwala zapewnić dodatkową ochronę przed podsłuchem i śledzeniem przez hakerów i w związku z tym utrudnia identyfikację osób.

Komisja zaleca, aby kod źródłowy aplikacji został podany do wiadomości publicznej i był dostępny do wglądu.

Można przewidzieć dodatkowe środki mające na celu zabezpieczenie przetwarzanych danych, w szczególności automatyczne usunięcie lub anonimizację danych po pewnym czasie. Ogólnie poziom bezpieczeństwa powinien odpowiadać ilości i wrażliwości przetwarzanych danych osobowych.

Każdy przekaz z urządzenia osobistego do krajowych organów ds. zdrowia powinien być szyfrowany.

W przypadku gdy prawo krajowe przewiduje, że zebrane dane osobowe mogą być również przetwarzane do celów badań naukowych, należy co do zasady stosować pseudonimizację.

3.9 **Zapewnienie rzetelności danych**

Zapewnienie prawidłowości przetwarzanych danych osobowych stanowi nie tylko warunek wstępny skuteczności aplikacji, lecz również wymóg wynikający z przepisów o ochronie danych osobowych.

W tym kontekście kluczowe znaczenie ma zapewnienie rzetelności informacji o tym, czy doszło do kontaktu z osobą zakażoną (odległość epidemiologiczna i czas trwania kontaktu), aby zminimalizować ryzyko uzyskania wyników fałszywie pozytywnych. Pozwoli to uwzględnić sytuacje, w których dwóch użytkowników aplikacji kontaktuje się na ulicy, w środkach transportu publicznego lub w budynku. Jest mało prawdopodobne, aby wykorzystanie danych dotyczących lokalizacji pochodzących z sieci telefonii ruchomej zapewniło na tyle dużą dokładność.

Zaleca się zatem, aby korzystać z technologii, które umożliwiają bardziej precyzyjną ocenę, czy doszło do kontaktu (takich jak Bluetooth).

3.10 **Zaangażowanie organów ochrony danych**

Organy ochrony danych powinny być w pełni zaangażowane w prace nad aplikacją i konsultowane w tym zakresie oraz powinny nadzorować wprowadzanie takiej aplikacji. 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), Komisja pragnie zwrócić uwagę na art. 35 RODO dotyczący oceny skutków dla ochrony danych.