Wytyczne 04/2020 w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19

Przyjęte 21 kwietnia 2020 r.

przyjęto

Historia wersji

Wersja 1.1	5 maja 2020 r.	Drobne korekty
Wersja 1.0	21 kwietnia 2020 r.	Przyjęcie wytycznych

Spis treści

Spis treści 3
1 Wprowadzenie i kontekst 4
2 Wykorzystywanie danych o lokalizacji 6
2.1 Źródła danych o lokalizacji 6
2.2 Koncentracja na wykorzystywaniu zanonimizowanych danych o lokalizacji 6
3 Aplikacje służące do ustalania kontaktów zakaźnych 8
3.1 Ogólna analiza prawna 8
3.2 Zalecenia i wymagania funkcjonalne 10
4 Podsumowanie 12
Załącznik – Aplikacje służące do ustalania kontaktów zakaźnych Przewodnik analityczny 13

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady 2016/679/UE 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 (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 tegoż, w kształcie zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE I KONTEKST

1 W odpowiedzi na pandemię COVID-19 rządy oraz podmioty prywatne skłaniają się ku rozwiązaniom opartym na danych, co budzi liczne obawy dotyczące prywatności.

2 EROD podkreśla, że ramy prawne ochrony danych opracowano z myślą o tym, by były elastyczne, dzięki czemu możliwa jest skuteczna reakcja, która pozwoli zarówno ograniczyć pandemię, jak i chronić podstawowe prawa i wolności człowieka.

3 EROD jest przekonana, że w sytuacji, gdy przetwarzanie danych osobowych jest konieczne, by zaradzić pandemii COVID-19, ochrona danych osobowych jest niezbędna do budowania zaufania i tworzenia warunków społecznej akceptacji dla każdego rozwiązania, a tym samym do zagwarantowania skuteczności tych środków. Ponieważ wirus nie zna granic, korzystne wydaje się opracowanie wspólnego europejskiego podejścia w odpowiedzi na obecny kryzys lub co najmniej wdrożenie ram interoperacyjnych.

4 Co do zasady EROD jest zdania, że dane oraz technologia wykorzystywane w celu zwalczania COVID-19 powinny być używane raczej do wzmacniania pozycji osób, a nie w celu ich kontrolowania, piętnowania lub uciskania. Ponadto, podczas gdy dane i technologia mogą stanowić istotne narzędzia, mają one właściwe sobie ograniczenia i mogą jedynie zwiększyć skuteczność innych środków dotyczących zdrowia publicznego. Środki przyjmowane przez państwa członkowskie lub instytucje Unii, dotyczące przetwarzania danych osobowych w celu zwalczania pandemii COVID-19, muszą opierać się na ogólnych zasadach skuteczności, niezbędności i proporcjonalności.

5 W niniejszych wytycznych doprecyzowano warunki i zasady proporcjonalnego wykorzystania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych do osiągnięcia dwóch szczegółowych celów, którymi są:

- wykorzystywanie danych o lokalizacji w celu wspierania reakcji na pandemię przez tworzenie modelu rozprzestrzeniania się wirusa, służącego ocenie skuteczności środków izolacji;
- ustalanie kontaktów zakaźnych w celu informowania poszczególnych osób o tym, że znalazły się w pobliżu osoby, w przypadku której zostanie ostatecznie potwierdzone, że

1 Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".

jest nosicielem wirusa, aby przerywać łańcuchy zakażeń na możliwie jak najwcześniejszym etapie.

6 Skuteczność wkładu aplikacji służących do ustalania kontaktów zakaźnych w kontrolowanie pandemii zależy od wielu czynników (np. od odsetka ludzi, którzy będą potrzebowali taką aplikację zainstalować; definicji „kontaktu", jeżeli chodzi o bliskość i czas trwania). Ponadto takie aplikacje muszą być elementem kompleksowej strategii zdrowia publicznego, mającej na celu zwalczanie pandemii, obejmującej m.in. badania i dalsze ustalanie kontaktów zakaźnych tradycyjnymi metodami, by rozwiać wszelkie wątpliwości. Wdrożeniu takich aplikacji powinny towarzyszyć środki wspierające mające zapewnić, aby informacje przekazywane użytkownikom były rozpatrywane w szerszym kontekście oraz aby ostrzeżenia były użyteczne dla systemu zdrowia publicznego. W przeciwnym razie aplikacje te nie będą w pełni skuteczne.

7 EROD podkreśla, że zarówno RODO, jak i dyrektywa 2002/58/WE (zwana dalej „dyrektywą") zawierają przepisy szczegółowe dopuszczające wykorzystywanie danych anonimowych lub danych osobowych w celu wspierania organów publicznych i innych podmiotów na szczeblu krajowym i unijnym w monitorowaniu i ograniczaniu rozprzestrzeniania się wirusa SARS-CoV-2[2].

8 W tym względzie EROD zajęła już stanowisko, twierdząc, że korzystanie z aplikacji służących do ustalania kontaktów zakaźnych powinno być dobrowolne i nie powinno polegać na śledzeniu poszczególnych przemieszczeń, lecz raczej powinno bazować na informacjach na temat bliskości dotyczących użytkowników[3].

[2] Zob. poprzednie oświadczenie EROD w sprawie pandemii COVID 19.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 WYKORZYSTYWANIE DANYCH O LOKALIZACJI

2.1 Źródła danych o lokalizacji

9 Istnieją dwa główne źródła danych o lokalizacji dostępne do celów tworzenia modeli rozprzestrzeniania się wirusa oraz ogólnej skuteczności środków izolacji:

- dane o lokalizacji gromadzone przez dostawców usług łączności elektronicznej (takich jak operatorzy usług telefonii komórkowej) w trakcie świadczenia usług oraz
- dane o lokalizacji gromadzone przez aplikacje podmiotów świadczących usługi społeczeństwa informacyjnego, których funkcje wymagają wykorzystania takich danych (np. nawigacja, usługi transportowe itp.).

10 EROD przypomina, że dane o lokalizacji[4] uzyskane od dostawców usług łączności elektronicznej mogą być przetwarzane wyłącznie w zakresie dopuszczonym w art. 6 i 9 dyrektywy. Oznacza to, że dane te mogą być przekazywane władzom lub innym osobom trzecim wyłącznie wówczas, gdy zostały zanonimizowane przez usługodawcę lub – w przypadku danych wskazujących położenie geograficzne terminala niebędących danymi o ruchu – po wyrażeniu przez użytkowników uprzedniej zgody[5].

11 Jeżeli chodzi o informacje – w tym dane o lokalizacji – zbierane bezpośrednio z terminala, zastosowanie ma art. 5 ust. 3 dyrektywy. W związku z tym przechowywanie informacji na urządzeniu użytkownika lub uzyskanie dostępu do informacji już przechowywanych jest dozwolone wyłącznie wtedy, gdy (i) użytkownik wyraził na to zgodę[6] lub (ii) jeżeli przechowywanie tych informacji lub dostęp do nich są ściśle niezbędne w celu świadczenia usługi społeczeństwa informacyjnego wyraźnie zażądanej przez użytkownika.

12 Wyjątki od praw i obowiązków, o których mowa w dyrektywie, są jednak możliwe zgodnie z art. 15, jeżeli stanowią niezbędny, właściwy i proporcjonalny środek w ramach społeczeństwa demokratycznego do osiągnięcia pewnych celów[7].

13 Jeżeli chodzi o ponowne wykorzystywanie danych o lokalizacji gromadzonych przez podmiot świadczący usługi społeczeństwa informacyjnego do celów tworzenia modeli (np. za pośrednictwem systemu operacyjnego lub wcześniej zainstalowanej aplikacji), muszą zostać spełnione dodatkowe warunki. Jeżeli dane gromadzono zgodnie z art. 5 ust. 3 dyrektywy, można je przetwarzać dalej za dodatkową zgodą osoby, której dane dotyczą, lub na podstawie prawa Unii lub prawa państwa członkowskiego, które stanowią niezbędny i proporcjonalny środek w społeczeństwie demokratycznym do zabezpieczenia celów, o których mowa w art. 23 ust. 1 RODO[8].

2.2 Koncentracja na wykorzystywaniu zanonimizowanych danych o lokalizacji

14 EROD podkreśla, że jeżeli chodzi o wykorzystanie danych o lokalizacji, w pierwszej kolejności należy zawsze przetwarzać dane zanonimizowane, a nie dane osobowe.

15 Anonimizacja odnosi się do wykorzystania zestawu technik w celu uniemożliwienia powiązania danych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną pomimo podjęcia wszelkich „rozsądnych" starań. „Test racjonalności" musi uwzględniać zarówno aspekty obiektywne (czas, środki techniczne), jak i elementy kontekstowe, które mogą się różnić w zależności od przypadku (rzadkość występowania danego zjawiska, przy wzięciu pod uwagę

[4] Zob. art. 2 lit. c) dyrektywy.
[5] Zob. art. 6 i 9 dyrektywy.
[6] Pojęcie zgody w dyrektywie pozostaje pojęciem zgody w RODO i musi spełniać wszystkie wymogi dotyczące zgody określone w art. 4 pkt 11 oraz w art. 7 RODO.
[7] W celu interpretacji art. 15 dyrektywy należy odnieść się także do wyroku TSUE z dnia 29 stycznia 2008 r. w sprawie C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.
[8] Zob. sekcja 1.5.3 wytycznych 1/2020 w sprawie przetwarzania danych osobowych w kontekście pojazdów podłączonych do internetu.

np. gęstości zaludnienia oraz charakteru i ilości danych). Jeżeli dane nie spełnią kryteriów tego testu, oznacza to, że nie zostały zanonimizowane, a zatem pozostają objęte zakresem RODO.

16 Ocena rzetelności anonimizacji zależy od trzech następujących kryteriów: (i) wyodrębnienia (wyizolowanie konkretnej osoby z większej grupy na podstawie danych); (ii) możliwości powiązania (powiązanie dwóch wpisów dotyczących tej samej osoby); oraz (iii) wnioskowania (wydedukowanie, z dużym prawdopodobieństwem, nieznanych informacji na temat konkretnej osoby).

17 Pojęcie anonimizacji jest często źle rozumiane i mylone z pojęciem pseudonimizacji. Podczas gdy anonimizacja umożliwia wykorzystanie danych bez żadnych ograniczeń, dane spseudonimizowane wciąż są objęte zakresem RODO.

18 Istnieje wiele możliwości skutecznej anonimizacji[9], jednak z pewnym zastrzeżeniem. Dane nie mogą zostać zanonimizowane same w sobie, tj. anonimizować można jedynie całe zbiory danych. W tym sensie każdą interwencję w pojedynczy wzorzec danych (z wykorzystaniem szyfrowania lub jakichkolwiek innych matematycznych przekształceń) można uznać w najlepszym wypadku za pseudonimizację.

19 Procesy anonimizacji i ataki mające na celu ponowną identyfikację to dziedziny, w których prowadzi się prężne badania. Kluczowe znaczenie dla każdego administratora wdrażającego rozwiązania z zakresu anonimizacji ma monitorowanie bieżących postępów w tej dziedzinie, zwłaszcza jeżeli chodzi o dane o lokalizacji (pochodzące od operatorów telekomunikacyjnych i/lub usług społeczeństwa informacyjnego), o których wiadomo, że niezwykle trudno jest je zanonimizować.

20 Rzeczywiście na podstawie licznych badań wykazano[10], że *dane o lokalizacji uważane za zanonimizowane* mogą w istocie nie być zanonimizowane. Ślady mobilności osób fizycznych są ze swej natury wysoce skorelowane i niepowtarzalne. W związku z tym mogą one w określonych okolicznościach być podatne na próby ponownej identyfikacji.

21 Nie można w pełni zanonimizować pojedynczego wzorca danych śledzącego przez dłuższy czas lokalizację danej osoby. Ocena ta może wciąż być prawdziwa, jeżeli dokładność zarejestrowanych współrzędnych geograficznych nie jest w istotny sposób obniżona lub jeżeli usunięto szczegółowe informacje na temat trasy oraz nawet jeśli zachowane jest wyłącznie położenie miejsc, w których przez znaczącą ilość czasu przebywa osoba, której dane dotyczą. Dotyczy to także słabo zagregowanych danych o lokalizacji.

22 Celem osiągnięcia anonimizacji dane o lokalizacji muszą być starannie przetwarzane w celu spełnienia wymogów testu racjonalności. W tym sensie takie przetwarzanie obejmuje rozpatrywanie zbiorów danych o lokalizacji jako całości oraz przetwarzanie danych pochodzących z racjonalnie dużego zbioru osób fizycznych z wykorzystaniem dostępnych rzetelnych technik anonimizacji, pod warunkiem że są one odpowiednio i skutecznie wdrożone.

23 Ponadto, biorąc pod uwagę złożoność procesów anonimizacji, usilnie zachęca się do zapewnienia przejrzystości w kwestii metodologii anonimizacji.

[9] Y. De Montjoye i in. (2018) „On the privacy-conscientious use of mobile phone data".
[10] Y. De Montjoye i in. (2013) „Unique in the Crowd: The privacy bounds of human mobility" oraz A. Pyrgelis i in. (2017) „Knock Knock, Who's There? Membership Inference on Aggregate Location Data".

3 APLIKACJE SŁUŻĄCE DO USTALANIA KONTAKTÓW ZAKAŹNYCH

3.1 Ogólna analiza prawna

24 Systematyczne monitorowanie na dużą skalę lokalizacji osób fizycznych i/lub kontaktów między nimi stanowi poważną ingerencję w prywatność tych osób. Można je uzasadnić jedynie opierając się na dobrowolnym przyjęciu przez użytkowników każdego z odpowiednich celów. Oznaczałoby to w szczególności, że osoby, które nie zdecydują się na korzystanie z takich aplikacji lub nie mogą z takich aplikacji korzystać, nie powinny ponosić żadnych niekorzystnych konsekwencji.

25 Zapewnienie rozliczalności wymaga wyraźnego wskazania administratora każdej aplikacji służącej do ustalania kontaktów zakaźnych. EROD uważa, że administratorami[11] takich aplikacji mogłyby być krajowe organy ds. zdrowia; można uwzględnić także innych administratorów. We wszystkich przypadkach, jeżeli we wdrażanie aplikacji służących do ustalania kontaktów zakaźnych zaangażowane są różne podmioty, ich role i obowiązki muszą od samego początku być jasno określone i wyjaśnione użytkownikom.

26 Ponadto, jeżeli chodzi o zasadę ograniczenia celu, cele muszą być wystarczająco szczegółowe, by wykluczyć dalsze przetwarzanie danych do celów niezwiązanych z zarządzaniem kryzysem zdrowotnym COVID-19 (jak np. do celów komercyjnych lub egzekwowania prawa). Kiedy cel zostanie już jasno określony, konieczne będzie zapewnienie, aby wykorzystywanie danych osobowych było adekwatne, niezbędne i proporcjonalne.

27 W kontekście aplikacji służących do ustalania kontaktów zakaźnych należy starannie uwzględnić zasadę minimalizacji danych oraz uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych:

- aplikacje służące do ustalania kontaktów zakaźnych nie wymagają śledzenia lokalizacji poszczególnych użytkowników. Zamiast tego należy korzystać z danych dotyczących bliskości fizycznej;
- ponieważ aplikacje służące do ustalania kontaktów zakaźnych mogą działać bez bezpośredniej identyfikacji poszczególnych osób, należy wdrożyć środki, które umożliwią zapobieganie ponownej identyfikacji;
- zgromadzone informacje powinny znajdować się na terminalu użytkownika i, gdy jest to bezwzględnie niezbędne, powinny być gromadzone tylko istotne informacje.

28 Jeżeli chodzi o zgodność przetwarzania z prawem, EROD zwraca uwagę, że stosowanie aplikacji służących do ustalania kontaktów zakaźnych obejmuje przechowywanie i/lub dostęp do informacji już przechowywanych na terminalu, co podlega pod art. 5 ust. 3 dyrektywy. Jeżeli operacje te są ściśle niezbędne, aby dostawca aplikacji mógł świadczyć usługę, której wyraźnie zażądał użytkownik, przetwarzanie nie wymaga zgody takiego użytkownika. Jeżeli chodzi o operacje, które nie są ściśle niezbędne, dostawca będzie musiał uzyskać zgodę użytkownika.

29 Ponadto EROD zwraca uwagę, że sam fakt, iż wykorzystanie aplikacji służących do ustalania kontaktów zakaźnych odbywa się na zasadzie dobrowolności, nie oznacza, że przetwarzanie danych osobowych będzie koniecznie odbywało się na podstawie zgody. Jeżeli organy publiczne świadczą usługę w oparciu o mandat przyznany przez prawo oraz zgodnie z określonymi w nim wymogami, najbardziej właściwą podstawą prawną przetwarzania jest niezbędność wykonania zadania realizowanego w interesie publicznym, tj. art. 6 ust. 1 lit. e) RODO.

30 W art. 6 ust. 3 RODO wyjaśniono, że podstawa przetwarzania, o którym mowa w art. 6 ust. 1 lit. e), musi być określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do

[11] Zob. także: Komisja Europejska, „Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych", C(2020) 2523 final, Bruksela, 16.04.2020.

wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi[12].

31 Podstawa prawna lub akt prawny, stanowiący zgodną z prawem podstawę stosowania aplikacji służących do ustalania kontaktów zakaźnych, powinny jednakże zawierać istotne zabezpieczenia, w tym odniesienie do dobrowolnego charakteru aplikacji. Należy w nich jasno określić cel oraz zawrzeć wyraźne ograniczenia dotyczące dalszego wykorzystywania danych osobowych, a także jednoznacznie wskazać zaangażowanego administratora lub administratorów. Należy określić także kategorie danych oraz podmioty, którym mogą zostać ujawnione dane osobowe (oraz cele, do których realizacji mogą zostać ujawnione takie dane). W zależności od poziomu ingerencji należy włączyć dodatkowe zabezpieczenia, z uwzględnieniem charakteru, zakresu i celów przetwarzania. Ponadto EROD zaleca także, aby w jak najkrótszym czasie uwzględnić kryteria pozwalające stwierdzić, kiedy aplikacja ma zostać usunięta, a także wskazać podmiot, który ponosi odpowiedzialność i będzie podlegać rozliczeniu za stwierdzenie tego.

32 Jeżeli jednak przetwarzanie danych opiera się na innej podstawie prawnej, takiej jak na przykład zgoda (art. 6 ust. 1 lit. a))[13], administrator będzie musiał zapewnić, aby spełnione zostały rygorystyczne wymagania dotyczące ważności takiej podstawy prawnej.

33 Ponadto wykorzystanie aplikacji do walki z pandemią COVID-19 może prowadzić do gromadzenia danych dotyczących zdrowia (na przykład statusu osoby zakażonej). Przetwarzanie takich danych jest dozwolone, kiedy jest ono niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, jeżeli zostaną spełnione warunki określone w art. 9 ust. 2 lit. i) RODO[14], lub do celów dotyczących opieki zdrowotnej, jak opisano w art. 9 ust. 2 lit. h) RODO[15]. W zależności od podstawy prawnej przetwarzanie może także odbywać się na podstawie wyraźnej zgody (art. 9 ust. 2 lit. a) RODO).

34 Zgodnie z pierwotnym celem w art. 9 ust. 2 lit. j) RODO dopuszcza się także możliwość przetwarzania danych dotyczących zdrowia, jeżeli jest to niezbędne do celów badań naukowych lub do celów statystycznych.

35 Trwający kryzys w dziedzinie zdrowia nie powinien być okazją do ustanawiania nieproporcjonalnych uprawnień do zatrzymywania danych. Ograniczenie przechowywania powinno uwzględniać rzeczywiste potrzeby oraz istotność danych z medycznego punktu widzenia (np. względy motywowane epidemiologicznie, takie jak okres inkubacji itd.), a dane osobowe powinny być przechowywane wyłącznie na czas trwania kryzysu wywołanego przez COVID-19. Następnie, co do zasady, wszystkie dane osobowe należy usunąć lub zanonimizować.

36 EROD uważa, że takie aplikacje mogą stanowić jedynie wsparcie dla tradycyjnych metod ustalania kontaktów zakaźnych przez wykwalifikowany personel służby zdrowia, który może stwierdzić, czy bliski kontakt może skutkować zakażeniem wirusem (np. kiedy ma miejsce kontakt z osobą chronioną przez odpowiedni sprzęt – kasjerem itp. – czy też nie), ale nie mogą ich zastąpić. EROD podkreśla, że procedury i procesy, takie jak odpowiednie algorytmy stosowane przez aplikacje służące do ustalania kontaktów zakaźnych, powinny działać pod ścisłym nadzorem wykwalifikowanego personelu, aby ograniczyć występowanie wyników fałszywie pozytywnych lub negatywnych. W szczególności zadanie polegające na udzielaniu porad dotyczących kolejnych kroków nie powinno opierać się jedynie na zautomatyzowanym przetwarzaniu.

---

[12] Zob. motyw 41.

[13] Administratorzy (zwłaszcza organy publiczne) muszą zwracać szczególną uwagę na fakt, że zgody nie należy uważać za dobrowolną, jeżeli dana osoba nie ma rzeczywistego wyboru, aby odmówić zgody lub ją wycofać bez niekorzystnych konsekwencji.

[14] Przetwarzanie musi odbywać się na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową.

[15] Zob. art. 9 ust. 2 lit. h) RODO.

37 Aby zapewnić rzetelność, rozliczalność oraz, szeroko rzecz ujmując, zgodność z prawem, algorytmy muszą być możliwe do kontrolowania i powinny podlegać regularnym przeglądom niezależnych ekspertów. Kod źródłowy aplikacji powinien być publicznie udostępniony w celu jak najszerszego nad nim nadzoru.

38 W jakimś stopniu zawsze będą pojawiały się wyniki fałszywie pozytywne. Ponieważ identyfikacja ryzyka zakażenia może prawdopodobnie mieć duży wpływ na poszczególne osoby, na przykład pozostanie w samoizolacji aż do otrzymania negatywnego wyniku testu, niezbędna jest możliwość poprawiania danych i/lub późniejszych wyników analiz. To wszystko powinno oczywiście mieć zastosowanie wyłącznie do scenariuszy i wdrożeń w przypadkach, gdy dane są przetwarzane lub przechowywane w sposób technicznie umożliwiający wprowadzanie takich poprawek oraz gdy prawdopodobne jest wystąpienie niekorzystnych skutków, o których mowa powyżej.

39 Wreszcie EROD uważa, że przed wdrożeniem takiego narzędzia należy przeprowadzić ocenę skutków dla ochrony danych, ponieważ przetwarzanie jest w tym przypadku uważane za operację, która z dużym prawdopodobieństwem może powodować wysokie ryzyko (dane dotyczące zdrowia, przewidywane wdrożenie na szeroką skalę, systematyczne monitorowanie, wykorzystanie nowego rozwiązania technologicznego)[16]. EROD zdecydowanie zaleca publikowanie ocen skutków dla ochrony danych.

3.2 Zalecenia i wymagania funkcjonalne

40 Zgodnie z zasadą minimalizacji danych, oprócz innych środków ochrony danych w fazie projektowania oraz domyślnej ochrony danych[17], przetwarzane dane należy ograniczyć do ścisłego minimum. Aplikacja nie powinna gromadzić informacji niepowiązanych lub niepotrzebnych, takich jak np. stan cywilny, identyfikatory komunikacyjne, obiekty rejestru urządzeń, wiadomości, dzienniki połączeń, dane o lokalizacji, identyfikatory urządzeń itp.

41 Dane przesyłane za pośrednictwem aplikacji muszą obejmować jedynie pewne niepowtarzalne i spseudonimizowane identyfikatory, generowane przez aplikację i dla niej właściwe. Identyfikatory te muszą być regularnie odnawiane z częstotliwością stosowną do celu, jakim jest ograniczenie rozprzestrzeniania się wirusa oraz wystarczającą, aby ograniczyć ryzyko identyfikacji i fizycznego śledzenia poszczególnych osób.

42 Wdrożenia w celu ustalania kontaktów zakaźnych mogą być oparte na podejściu scentralizowanym lub zdecentralizowanym[18]. Oba rozwiązania należy uznawać za wykonalne, pod warunkiem że zastosowano odpowiednie środki bezpieczeństwa, a każde z nich ma pewne zalety i wady. Tym samym etap tworzenia koncepcji aplikacji powinien zawsze obejmować rzetelne rozważenie obu koncepcji i ostrożne wyważenie ich wpływu na ochronę danych osobowych/prywatności, a także ich ewentualnego wpływu na prawa osób fizycznych.

43 Każdy serwer podłączony do systemu ustalania kontaktów zakaźnych musi gromadzić wyłącznie historię kontaktów lub spseudonimizowane identyfikatory użytkownika, którego zdiagnozowano jako zakażonego w wyniku odpowiedniej oceny przeprowadzonej przez organy ds. zdrowia i dobrowolnego działania podjętego przez użytkownika. Ewentualnie serwer musi przechowywać wykaz spseudonimizowanych identyfikatorów zakażonych użytkowników lub ich historię kontaktów tylko przez okres potrzebny do poinformowania potencjalnie zakażonych użytkowników o ich narażeniu i nie powinien podejmować prób identyfikacji potencjalnie zakażonych użytkowników.

---

[16] Zob. Wytyczne Grupy Roboczej Art. 29 (przyjęte przez EROD) dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679.

[17] Zob. Wytyczne EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z art. 25.

[18] Ogólnie rzecz biorąc, rozwiązanie zdecentralizowane jest bardziej zgodne z zasadą minimalizacji danych.

44 Wdrażanie globalnej metody ustalania kontaktów zakaźnych obejmującej zarówno aplikacje, jak i ustalanie tradycyjnymi metodami, może w niektórych przypadkach wymagać przetwarzania dodatkowych informacji. W tym kontekście te dodatkowe informacje powinny pozostawać na terminalu użytkownika i być przetwarzane wyłącznie wtedy, gdy jest to bezwzględnie niezbędne, oraz za uprzednią konkretną zgodą użytkownika.

45 Należy stosować zgodne ze stanem obecnej wiedzy techniki kryptograficzne, aby zabezpieczyć dane przechowywane na serwerach oraz w aplikacjach, wymianę danych między aplikacjami oraz zdalny serwer. Musi odbywać się także wzajemne uwierzytelnianie między aplikacją a serwerem.

46 Zgłaszanie użytkowników przez aplikację jako osób zakażonych SARS-CoV-2 musi podlegać odpowiedniej autoryzacji, na przykład za pośrednictwem jednorazowego kodu przypisanego do spseudonimizowanej tożsamości osoby zakażonej i powiązanego ze stacją kontrolną lub pracownikiem służby zdrowia. Jeżeli nie można uzyskać potwierdzenia w bezpieczny sposób, nie powinno mieć miejsca przetwarzanie danych, które zakłada prawidłowość statusu użytkownika.

47 Administrator, we współpracy z organami publicznymi, musi jasno i wyraźnie poinformować o łączu, pod którym można pobrać oficjalną krajową aplikację służącą do ustalania kontaktów zakaźnych w celu ograniczenia ryzyka korzystania przez obywateli z aplikacji strony trzeciej.

4 PODSUMOWANIE

48 Świat stoi w obliczu poważnego kryzysu w dziedzinie zdrowia publicznego, wymagającego zdecydowanej reakcji, której skutki będą odczuwalne w zakresie wykraczającym poza bieżącą sytuację nadzwyczajną. Zautomatyzowane przetwarzanie danych i technologie cyfrowe mogą stanowić kluczowe elementy walki z COVID-19. Należy jednak uważać na „efekt zapadki". Naszym obowiązkiem jest zapewnienie, aby każdy środek wdrożony w tych nadzwyczajnych okolicznościach był niezbędny, ograniczony w czasie, miał minimalny wymiar i podlegał okresowym i rzeczywistym przeglądom, a także kontroli naukowej.

49 EROD podkreśla, że nie powinno dochodzić do sytuacji, w których trzeba wybierać między skuteczną reakcją na bieżący kryzys a ochroną naszych praw podstawowych: możemy osiągnąć oba te cele jednocześnie, a ponadto zasady ochrony danych mogą odegrać istotną rolę w walce z wirusem. Europejskie prawo ochrony danych osobowych pozwala na odpowiedzialne wykorzystywanie danych osobowych do celów związanych z zarządzaniem zdrowiem, zapewniając jednocześnie, aby w tym procesie nie doszło do osłabienia praw i wolności osób fizycznych.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

ZAŁĄCZNIK – APLIKACJE SŁUŻĄCE DO USTALANIA KONTAKTÓW ZAKAŹNYCH
PRZEWODNIK ANALITYCZNY

0. Zastrzeżenie

Przedstawione poniżej wskazówki nie mają charakteru normatywnego ani nie są wyczerpujące, a niniejszy przewodnik ma na celu jedynie zapewnienie ogólnych wskazówek dla projektantów aplikacji służących do ustalania kontaktów zakaźnych i podmiotów, które je wdrażają. Można stosować także inne rozwiązania niż te, które opisano w niniejszym przewodniku, i mogą one być zgodne z prawem, o ile są zgodne z odpowiednimi ramami prawnymi (tj. z RODO oraz z dyrektywą).

Należy także zwrócić uwagę na fakt, że niniejszy przewodnik ma charakter ogólny. W związku z tym zaleceń i obowiązków opisanych w niniejszym dokumencie nie należy postrzegać jako wyczerpujących. Oceny należy przeprowadzać oddzielnie dla każdego przypadku, a poszczególne aplikacje mogą wymagać dodatkowych środków, których nie opisano w niniejszym przewodniku.

1. Streszczenie

W wielu państwach członkowskich zainteresowane strony rozważają wykorzystanie aplikacji służących do *ustalania kontaktów zakaźnych*, aby pomóc ludziom w rozpoznaniu, czy mieli kontakt z osobą zakażoną SARS-Cov-2.

Warunki, na których takie aplikacje mogą skutecznie przyczynić się do zarządzania pandemią, nie zostały jeszcze ustalone. Konieczne jest ustalenie ich przed rozpoczęciem wdrażania takich aplikacji. Istotne znaczenie ma jednak zapewnienie wytycznych, które dostarczą odpowiednich informacji zespołom projektantów zapoczątkowujących dany projekt, aby już od początku procesu projektowania można było zagwarantować ochronę danych osobowych.

Należy zwrócić uwagę na fakt, że niniejszy przewodnik ma charakter ogólny. W związku z tym zaleceń i obowiązków opisanych w niniejszym dokumencie nie należy postrzegać jako wyczerpujących. Oceny należy przeprowadzać oddzielnie dla każdego przypadku, a poszczególne aplikacje mogą wymagać dodatkowych środków, których nie opisano w niniejszym przewodniku. Niniejszy przewodnik ma na celu jedynie zapewnienie ogólnych wskazówek dla projektantów aplikacji służących do ustalania kontaktów zakaźnych i podmiotów, które je wdrażają.

Niektóre kryteria mogą wykraczać poza ścisłe wymogi wynikające z ram ochrony danych. Ich celem jest zapewnienie najwyższego poziomu przejrzystości celem uzyskania akceptacji społecznej dla aplikacji służących do ustalania kontaktów zakaźnych.

W tym celu wydawcy aplikacji służących do ustalania kontaktów zakaźnych powinni uwzględnić poniższe kryteria:

- korzystanie z takiej aplikacji musi być w pełni dobrowolne. Korzystanie z aplikacji nie może być warunkiem dostępu do jakichkolwiek praw gwarantowanych przepisami prawa. Osoby muszą nieprzerwanie mieć pełną kontrolę nad swoimi danymi i powinny mieć możliwość swobodnego decydowania, czy chcą korzystać z aplikacji;

- aplikacje służące do ustalania kontaktów zakaźnych z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych oraz wymagać przeprowadzenia oceny skutków dla ochrony danych przed ich wdrożeniem;
- informacje o fizycznej bliskości między użytkownikami aplikacji można uzyskać bez konieczności lokalizowania użytkowników. Ten rodzaj aplikacji nie wymaga danych o lokalizacji, a zatem nie powinien wiązać się z ich wykorzystaniem;
- w przypadku zdiagnozowania u użytkownika zakażenia SARS-CoV-2 należy poinformować o tym jedynie osoby, z którymi użytkownik miał bliski kontakt w odpowiednim z epidemiologicznego punktu widzenia w celu ustalenia kontaktów zakaźnych okresie zatrzymywania danych;
- tego typu działanie aplikacji może wymagać, w zależności od wybranej architektury, zastosowania scentralizowanego serwera. W takim przypadku oraz zgodnie z zasadami minimalizacji danych i ochrony danych w fazie projektowania, dane przetwarzane przez scentralizowany serwer powinny być ograniczone do absolutnego minimum:
    - jeżeli użytkownik zostanie zdiagnozowany jako zakażony, informacje dotyczące osób, z którymi miał wcześniej bliski kontakt, lub identyfikatory przesyłane przez aplikację użytkownika mogą być zbierane tylko za jego zgodą. Należy ustalić metodę weryfikacji, która pozwoli na stwierdzenie, że dana osoba jest rzeczywiście zakażona, bez identyfikacji użytkownika. Z technicznego punktu widzenia można to osiągnąć poprzez ostrzeżenie osób z którymi doszło do kontaktu wyłącznie po interwencji pracownika służby zdrowia, np. za pomocą specjalnego jednorazowego kodu;
    - informacje przechowywane na serwerze centralnym nie powinny umożliwiać administratorowi danych identyfikacji użytkowników, co do których stwierdzono, że są zakażeni lub kontaktowali się z takimi użytkownikami, ani nie powinny umożliwiać wnioskowania wzorców kontaktów, które nie są potrzebne do wskazania odpowiednich kontaktów;
- działanie tego typu aplikacji wymaga transmisji danych, które są odczytywane przez urządzenia innych użytkowników i odsłuchania tych komunikatów:
    - wystarczająca jest wymiana spseudonimizowanych identyfikatorów pomiędzy urządzeniami mobilnymi użytkowników (jak np. komputery, tablety, zegarki połączone (ang. connected watches) itp.), np. poprzez ich transmisję (np. za pomocą technologii Bluetooth Low Energy);
    - identyfikatory muszą być generowane przy użyciu uwzględniających aktualny stan wiedzy procesów kryptograficznych;
    - identyfikatory muszą być regularnie odnawiane, aby zmniejszyć ryzyko ataków związanych z fizycznym śledzeniem i ataków opartych na identyfikacji osoby wskutek łączenia danych pochodzących z różnych źródeł;
- tego typu aplikacja musi posiadać zabezpieczenia, aby zagwarantować bezpieczne procesy techniczne. W szczególności:
    - aplikacja nie powinna przekazywać użytkownikom informacji pozwalających na wywnioskowanie tożsamości lub diagnozy innych osób. Serwer centralny nie może ani identyfikować użytkowników, ani wnioskować informacji o nich.

Zastrzeżenie: powyższe zasady odnoszą się do zakładanego celu aplikacji służących do *ustalania kontaktów zakaźnych* i tylko do tego celu, który polega na automatycznym informowaniu osób potencjalnie narażonych na kontakt z wirusem (bez konieczności ich identyfikacji). Operatorzy aplikacji i jej infrastruktury mogą być kontrolowani przez właściwy organ nadzorczy. Przestrzeganie całości lub części tych wytycznych nie jest w sposób konieczny wystarczające do zapewnienia pełnej zgodności z ramami prawnymi ochrony danych.

2. Definicje

Kontakt	W przypadku aplikacji służącej do ustalania kontaktów zakaźnych kontaktem jest użytkownik, który uczestniczył w interakcji z użytkownikiem potwierdzonym jako nosiciel wirusa, a czas trwania kontaktu i odległość stwarzają ryzyko znacznego narażenia na zakażenie wirusem. Parametry dotyczące czasu trwania narażenia i odległości między ludźmi muszą zostać oszacowane przez organy ds. zdrowia i mogą zostać określone w aplikacji.
Dane o lokalizacji	Termin ten odnosi się do wszystkich danych przetwarzanych w sieci łączności elektronicznej lub przez usługę łączności elektronicznej, wskazujących położenie geograficzne terminala użytkownika publicznie dostępnych usług łączności elektronicznej (zgodnie z definicją zawartą w dyrektywie), jak również do danych z potencjalnych innych źródeł, odnoszących się do: • szerokości, długości i wysokości urządzenia końcowego; • kierunku przekazu użytkownika lub • czasu, w którym informacja dla danej lokalizacji została zapisana.
Interakcja	W kontekście aplikacji służącej do ustalania kontaktów zakaźnych interakcję definiuje się jako wymianę informacji pomiędzy dwoma urządzeniami znajdującymi się w bliskiej odległości od siebie (w przestrzeni i czasie), w zakresie wykorzystywanej technologii łączności (np. Bluetooth). Definicja ta nie obejmuje lokalizacji dwóch użytkowników interakcji.
Nosiciel wirusa	W niniejszym dokumencie za nosicieli wirusa uznaje się użytkowników, którzy uzyskali pozytywny wynik testu na obecność wirusa i otrzymali oficjalną diagnozę od lekarzy lub ośrodków zdrowia.
Ustalanie kontaktów zakaźnych	Osoby, które miały bliski kontakt (według kryteriów, które zostaną określone przez epidemiologów) z osobą zakażoną wirusem, są w znacznym stopniu narażone na ryzyko zakażenia się i w konsekwencji na zakażenie innych osób. Ustalanie kontaktów zakaźnych to metodologia kontrolowania choroby, która rejestruje wszystkie osoby, które przebywały w bezpośredniej bliskości nosiciela wirusa, w celu sprawdzenia, czy są one narażone na ryzyko zakażenia i zastosowania wobec nich odpowiednich środków sanitarnych.

3. Informacje ogólne

OG-1	Aplikacja musi być narzędziem uzupełniającym tradycyjne techniki ustalania kontaktów zakaźnych (w szczególności wywiady z osobami zakażonymi), tj. stanowić część szerszego programu zdrowia publicznego. Musi być wykorzystywana tylko do momentu, gdy tradycyjne techniki ustalania kontaktów zakaźnych będą w stanie samodzielnie poradzić sobie z ilością nowych zakażeń.
OG-2	Najpóźniej w momencie podjęcia decyzji o „powrocie do normalności" przez właściwe organy publiczne należy wprowadzić procedurę mającą na celu zaprzestanie gromadzenia identyfikatorów (globalna dezaktywacja aplikacji, instrukcje dotyczące odinstalowania aplikacji, automatyczne odinstalowanie itp.) oraz uruchomienie procesu usuwania wszystkich zgromadzonych danych ze wszystkich baz danych (aplikacji mobilnych i serwerów).
OG-3	Kod źródłowy aplikacji i jej zaplecza musi być otwarty, a specyfikacje techniczne muszą być podane do wiadomości publicznej, tak aby każda zainteresowana strona mogła przeprowadzić audyt kodu, a w stosownych przypadkach – uczestniczyć w jego ulepszaniu, korygowaniu ewentualnych błędów i zapewnianiu przejrzystości przetwarzania danych osobowych.
OG-4	Etapy wdrażania aplikacji muszą umożliwiać stopniowe potwierdzanie jej skuteczności z punktu widzenia zdrowia publicznego. W tym celu należy wcześniej określić protokół oceny, określający wskaźniki pozwalające na zmierzenie skuteczności aplikacji.

4. Cele

CEL-1	Celem aplikacji musi być wyłącznie ustalanie kontaktów zakaźnych, aby osoby potencjalnie narażone na kontakt z SARS-CoV-2 mogły zostać ostrzeżone i otoczone opieką. Nie można wykorzystywać jej do innego celu.
CEL-2	Nie wolno stosować aplikacji do celów innych niż jej pierwotne zastosowanie, tj. monitorowanie przestrzegania kwarantanny lub środków izolacji i/lub dystansu społecznego.
CEL-3	Aplikacji nie wolno wykorzystywać do wyciągania wniosków dotyczących lokalizacji użytkowników na podstawie ich interakcji i/lub innych środków.

5. Kwestie funkcjonalne

FUNK-1	Aplikacja musi zapewniać funkcjonalność umożliwiającą informowanie użytkowników o tym, że mogli być potencjalnie narażeni na kontakt z wirusem, przy czym informacja ta opiera się na bliskości zarażonego użytkownika w okresie X dni przed pozytywnym wynikiem badania przesiewowego (wartość X jest określana przez organy ds. zdrowia).

FUNK-2	Aplikacja powinna zawierać zalecenia dla użytkowników zidentyfikowanych jako osoby potencjalnie narażone na kontakt z wirusem. Powinna ona przekazywać instrukcje dotyczące środków, których należy przestrzegać, oraz umożliwiać użytkownikowi zwrócenie się o poradę. W takich przypadkach obowiązkowa byłaby interwencja człowieka.
FUNK-3	Algorytm mierzący ryzyko zakażenia poprzez uwzględnienie czynników odległości i czasu, a tym samym określający, kiedy należy dodać kontakt do listy na potrzeby ustalania kontaktów zakaźnych, musi być w bezpieczny sposób konfigurowalny, aby uwzględnić najnowszą wiedzę na temat rozprzestrzeniania się wirusa.
FUNK-4	**Użytkownicy muszą zostać poinformowani w sytuacji, gdy byli narażeni na kontakt z wirusem**, lub muszą regularnie otrzymywać informacje o tym, czy byli narażeni na kontakt z wirusem w okresie inkubacji wirusa.
FUNK-5	Aplikacja powinna być interoperacyjna z innymi aplikacjami opracowanymi w państwach członkowskich, tak aby możliwe było skuteczne powiadamianie użytkowników podróżujących po różnych państwach członkowskich.

6. Dane

DANE-1	Aplikacja musi posiadać funkcję przesyłania i odbierania danych za pomocą technologii komunikacji bliskiego zasięgu, takich jak Bluetooth Low Energy, aby można było ustalić kontakty zakaźne.
DANE-2	Przesyłane dane muszą zawierać kryptograficznie silne pseudolosowe identyfikatory, generowane przez aplikację i właściwe dla danej aplikacji.
DANE-3	Ryzyko konfliktu między pseudolosowymi identyfikatorami powinno być wystarczająco niskie.
DANE-4	Identyfikatory pseudolosowe muszą być regularnie odnawiane, z częstotliwością wystarczającą do ograniczenia ryzyka ponownej identyfikacji, fizycznego śledzenia lub powiązania osób, przez kogokolwiek, w tym operatorów serwerów centralnych, innych użytkowników aplikacji lub nieuczciwe osoby trzecie. Identyfikatory te muszą być generowane przez aplikację użytkownika, ewentualnie w oparciu o materiał dostarczony przez serwer centralny.
DANE-5	Zgodnie z zasadą minimalizacji danych aplikacja nie może gromadzić danych innych niż te, które są ściśle niezbędne do celów ustalania kontaktów zakaźnych.
DANE-6	Aplikacja nie może gromadzić danych o lokalizacji do celów ustalania kontaktów zakaźnych. Dane o lokalizacji mogą być przetwarzane wyłącznie w celu umożliwienia aplikacji interakcji z podobnymi aplikacjami w innych państwach i powinny być precyzyjnie ograniczone do tego, co jest ściśle niezbędne do tego celu.

DANE-7	Aplikacja nie powinna gromadzić danych dotyczących zdrowia poza tymi, które są ściśle niezbędne do realizacji jej celów, z wyjątkiem dobrowolnego gromadzenia danych wyłącznie w celu pomocy w procesie podejmowania decyzji dotyczących informowania użytkownika.
DANE-8	Użytkownicy muszą być informowani o wszystkich danych osobowych, które będą gromadzone. Dane te powinny być zbierane tylko za zgodą użytkownika.

7. Właściwości techniczne

TECH-1	Aplikacja powinna wykorzystywać takie dostępne technologie, jak technologia komunikacji bliskiego zasięgu (np. Bluetooth Low Energy) w celu wykrywania użytkowników w pobliżu urządzenia z uruchomioną aplikacją.
TECH-2	Aplikacja powinna przechowywać historię kontaktów użytkownika na urządzeniu przez ograniczony, określony wcześniej czas.
TECH-3	Aplikacja może polegać na serwerze centralnym celem wdrożenia niektórych ze swoich funkcji.
TECH-4	Aplikacja musi bazować na architekturze, która w jak największym stopniu opiera się na urządzeniach użytkowników.
TECH-5	Użytkownicy zgłoszeni jako zakażeni wirusem, których status zostanie potwierdzony przez odpowiednio upoważnionego pracownika służby zdrowia, z własnej inicjatywy powinni przesłać historię swoich kontaktów lub własne identyfikatory na serwer centralny.

8. Bezpieczeństwo

BEZP-1	Mechanizm musi weryfikować status użytkowników, którzy w aplikacji oznaczyli się jako zakażeni SARS-CoV-2, np. poprzez podanie jednorazowego kodu powiązanego ze stacją badawczą lub pracownikiem służby zdrowia. Jeżeli nie można uzyskać potwierdzenia w bezpieczny sposób, dane nie mogą być przetwarzane.
BEZP-2	Dane wysyłane do serwera centralnego muszą być przesyłane bezpiecznym kanałem. Korzystanie z usług powiadamiania świadczonych przez dostawców platform systemu operacyjnego powinno podlegać dokładnej ocenie i nie powinno prowadzić do ujawnienia danych osobom trzecim.
BEZP-3	Żądania nie mogą być narażone na manipulowanie ze strony złośliwego użytkownika.
BEZP-4	Należy wdrożyć zgodne z aktualnym stanem wiedzy techniki kryptograficzne w celu zabezpieczenia wymiany informacji między aplikacją a serwerem oraz między aplikacjami, a także, co do zasady, w celu ochrony informacji przechowywanych w aplikacjach i na serwerze. Do przykładowych technik, które mogą być stosowane, zalicza się: szyfrowanie symetryczne i asymetryczne, funkcje skrótu, test prywatnego członkostwa (ang. *private membership test*), obliczanie

	części wspólnej zbiorów prywatnych (ang. *private set intersection*), filtry Blooma, odzyskiwanie informacji prywatnych, szyfrowanie homomorficzne itp.
BEZP-5	Serwer centralny nie może przechowywać identyfikatorów połączeń sieciowych (np. adresów IP) żadnych użytkowników, w tym tych, którzy zostali pozytywnie zdiagnozowani i przesłali historię swoich kontaktów lub własne identyfikatory.
BEZP-6	Aby uniknąć podszywania się lub tworzenia fałszywych użytkowników, serwer musi uwierzytelnić aplikację.
BEZP-7	Aplikacja musi uwierzytelnić serwer centralny.
BEZP-8	Funkcje serwera powinny być chronione przed atakami polegającymi na ponownym przesłaniu komunikatu przez złośliwą stronę trzecią (ang. *replay attacks*).
BEZP-9	Informacje przesyłane przez serwer centralny muszą zostać podpisane w celu uwierzytelnienia ich pochodzenia i integralności.
BEZP-10	Dostęp do wszystkich danych przechowywanych na serwerze centralnym, które nie są publicznie dostępne, musi być zastrzeżony wyłącznie dla osób upoważnionych.
BEZP-11	Na poziomie systemu operacyjnego menedżer uprawnień urządzenia może żądać jedynie uprawnień niezbędnych do uzyskania dostępu do modułów komunikacyjnych i korzystania z nich w razie potrzeby, do przechowywania danych w terminalu oraz do wymiany informacji z serwerem centralnym.

9. Ochrona danych osobowych i prywatności osób fizycznych

Przypomnienie: poniższe wytyczne dotyczą aplikacji, której jedynym celem jest ustalanie kontaktów zakaźnych.

PRYW-1	Wymiana danych musi odbywać się z poszanowaniem prywatności użytkowników (a w szczególności z poszanowaniem zasady minimalizacji danych).
PRYW-2	Aplikacja nie może umożliwiać bezpośredniej identyfikacji użytkowników podczas korzystania z niej.
PRYW-3	Aplikacja nie może pozwalać na śledzenie przemieszczania się użytkowników.
PRYW-4	Korzystanie z aplikacji nie powinno pozwalać użytkownikom na uzyskanie jakichkolwiek informacji o innych użytkownikach (a w szczególności o tym, czy są oni nosicielami wirusa czy nie).
PRYW-5	Zaufanie do serwera centralnego musi być ograniczone. Zarządzanie serwerem centralnym musi odbywać się zgodnie z jasno określonymi zasadami zarządzania i obejmować wszystkie środki niezbędne do zapewnienia jego bezpieczeństwa. Lokalizacja serwera centralnego powinna umożliwiać właściwemu organowi nadzorczemu prowadzenie skutecznego nadzoru.
PRYW-6	Należy przeprowadzić ocenę skutków dla ochrony danych i podać ją do wiadomości publicznej.
PRYW-7	Aplikacja powinna ujawniać użytkownikowi jedynie, czy był narażony na kontakt z wirusem, oraz - w miarę możliwości bez ujawniania informacji o innych użytkownikach - liczbę i daty takich zdarzeń.
PRYW-8	Z informacji przekazywanych przez aplikację użytkownicy nie powinni być w stanie zidentyfikować osób będących nosicielami wirusa ani śledzić ich ruchów.
PRYW-9	Z informacji przekazywanych przez aplikację organy ds. zdrowia nie powinny być w stanie zidentyfikować potencjalnie narażonych osób bez ich zgody.
PRYW-10	Żądania wysyłane przez aplikację do serwera centralnego nie mogą ujawniać żadnych informacji na temat nosiciela wirusa.
PRYW-11	Żądania wysyłane przez aplikację do serwera centralnego nie mogą ujawniać żadnych informacji o użytkowniku, które nie są niezbędne, za wyjątkiem gdy jest to możliwe i tylko wówczas, gdy jest to konieczne, jej spseudonimizowanych identyfikatorów i listy kontaktów.
PRYW-12	Nie może istnieć możliwość przeprowadzania ataków opartych na identyfikacji osób wskutek łączenia danych pochodzących z różnych źródeł (ang. linkage attacks).
PRYW-13	Użytkownicy muszą mieć możliwość wykonywania swoich praw za pośrednictwem aplikacji.
PRYW-14	Usunięcie aplikacji musi skutkować usunięciem wszystkich zebranych lokalnie danych.

PRYW-15	Aplikacja powinna gromadzić jedynie dane przekazywane przez instancje aplikacji lub interoperacyjne równoważne aplikacje. Nie powinny być zbierane żadne dane odnoszące się do innych aplikacji lub urządzeń łączności bliskiego zasięgu.
PRYW-16	Aby uniknąć ponownej identyfikacji przez serwer centralny, należy zastosować serwery proxy. Zadaniem tych *niezagrażających bezpieczeństwu serwerów* (ang.: non-colluding servers) jest mieszanie identyfikatorów kilku użytkowników (zarówno nosicieli wirusa, jak i osób wysyłających żądanie) przed udostępnieniem ich serwerowi centralnemu, tak aby ten nie poznał identyfikatorów (takich jak adresy IP) użytkowników.
PRYW-17	Należy starannie opracować i skonfigurować aplikację i serwer, aby nie gromadziły niepotrzebnych danych (np. w dziennikach serwera nie należy umieszczać żadnych identyfikatorów itp.) oraz aby uniknąć korzystania z SDK stron trzecich gromadzącego dane do innych celów.

W przypadku uznania użytkownika za zakażonego w większości omawianych obecnie aplikacji służących do ustalania kontaktów zakaźnych stosuje się zasadniczo dwa podejścia: mogą one albo wysłać na serwer historię kontaktów bezpośrednich, które uzyskały poprzez skanowanie, albo wysłać listę własnych identyfikatorów, które były transmitowane. Zgodnie z tymi dwoma podejściami odrzuca się następujące zasady. Chociaż podejścia te zostały omówione w niniejszych wytycznych, nie oznacza to, że inne podejścia nie są możliwe lub nawet preferowane, np. podejścia, w ramach których wykorzystuje się pewną formę szyfrowania E2E lub stosuje inne technologie służące wzmocnieniu ochrony bezpieczeństwa i prywatności.

9.1. Zasady, które obowiązują tylko wtedy, gdy aplikacja przesyła listę kontaktów na serwer

KON-1	Serwer centralny musi zebrać historię kontaktów użytkowników zgłoszonych jako osoby zakażone SARS-CoV-2, w wyniku dobrowolnego działania z ich strony.
KON-2	Serwer centralny nie może przechowywać ani rozpowszechniać listy spseudonimizowanych identyfikatorów użytkowników będących nosicielami wirusa.
KON-3	Historia kontaktów przechowywana na serwerze centralnym musi zostać usunięta po powiadomieniu użytkowników o ich bliskim kontakcie z osobą zakażoną.
KON-4	Z wyjątkiem przypadków, gdy użytkownik, w przypadku którego ustalono, iż ma pozytywny wynik testu, udostępnia swoją historię kontaktów na serwerze centralnym lub gdy wysyła na serwer prośbę o przekazanie informacji o potencjalnym narażeniu na wirusa, żadne dane nie mogą opuścić urządzenia użytkownika.
KON-5	Każdy identyfikator zawarty w lokalnej historii musi zostać usunięty po upływie X dni od jego dodania (wartość X jest określana przez organy ds. zdrowia).
KON-6	Historie kontaktów przekazywane przez różnych użytkowników nie powinny być dalej przetwarzane, np. wzajemnie korelowane w celu stworzenia globalnych map bezpośrednich kontaktów.

KON-7	Dane w dziennikach serwera muszą być ograniczone do minimum i muszą być zgodne z wymogami ochrony danych.

9.2. Zasady, które obowiązują tylko wtedy, gdy aplikacja przesyła listę własnych identyfikatorów na serwer

ID-1	Serwer centralny musi zebrać identyfikatory przesłane przez aplikację użytkowników zgłoszonych jako osoby zakażone SARS-CoV-2, w wyniku dobrowolnego działania z ich strony.
ID-2	Serwer centralny nie może przechowywać ani rozpowszechniać historii kontaktów użytkowników będących nosicielami wirusa.
ID-3	Identyfikatory przechowywane na serwerze centralnym muszą zostać usunięte po ich rozesłaniu do pozostałych aplikacji.
ID-4	Z wyjątkiem przypadków, gdy użytkownik, w przypadku którego ustalono, iż ma pozytywny wynik testu, udostępnia swoje identyfikatory na serwerze centralnym lub gdy wysyła na serwer prośbę o przekazanie informacji o potencjalnym narażeniu na wirusa, żadne dane nie mogą opuścić urządzenia użytkownika.
ID-5	Dane w dziennikach serwera muszą być zminimalizowane i muszą być zgodne z wymogami ochrony danych.