Wytyczne

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

Przyjęte dnia 21 kwietnia 2020 r.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

przyjęto

Historia wersji

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

Spis treści

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 do tego Porozumienia, zmienione 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 coraz powszechniej zwracają 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 trwający 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 po to, by dawać ludziom możliwości, a nie w celu ich kontrolowania, piętnowania lub uciskania. Ponadto, mimo że 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, konieczności i proporcjonalności.

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

- wykorzystywanie danych dotyczących lokalizacji w celu wspierania odpowiedzi na pandemię przez modelowanie rozprzestrzeniania się wirusa na potrzeby oceny 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 dotyczącej zdrowia publicznego mającej na celu zwalczanie pandemii, w tym m.in. badania i dalszego ustalania 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 zanonimizowanych 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 DOTYCZĄCYCH LOKALIZACJI

2.1 Źródła danych dotyczących lokalizacji

9 Istnieją dwa główne źródła danych dotyczących lokalizacji dostępne do celów modelowania rozprzestrzeniania się wirusa oraz ogólnej skuteczności środków izolacji:

- dane dotyczące lokalizacji gromadzone przez dostawców usług łączności elektronicznej (takich jak operatorzy usług telefonii komórkowej) w trakcie świadczenia usług oraz
- dane dotyczące 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 dotyczące 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 urządzenia końcowego niebędących danymi o ruchu – po wyrażeniu przez użytkowników uprzedniej zgody[5].

11 Jeżeli chodzi o informacje – w tym dane dotyczące lokalizacji – zbierane bezpośrednio z urządzeń końcowych, 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 Odstępstwa 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 dotyczących lokalizacji gromadzonych przez podmiot świadczący usługi społeczeństwa informacyjnego do celów modelowania (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 w społeczeństwie demokratycznym stanowią konieczny i proporcjonalny środek do zabezpieczenia celów, o których mowa w art. 23 ust. 1 RODO[8].

2.2 Skoncentrowanie na wykorzystywaniu zanonimizowanych danych dotyczących lokalizacji

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

15 Anonimizacja odnosi się do wykorzystania zestawu technik w celu uniemożliwienia połączenia danych z określoną lub możliwą do identyfikacji osobą fizyczną pomimo wszelkich „rozsądnych" starań. „Test racjonalności" musi uwzględniać zarówno aspekty obiektywne (czas, środki techniczne), jak i elementy kontekstowe, które mogą różnić się w zależności od

---

[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.

przypadku (rzadkość występowania danego zjawiska, biorąc pod uwagę np. gęstość zaludnienia oraz charakter i ilość danych). Jeżeli dane nie przejdą tego testu, oznacza to, że nie zostały zanonimizowane, a zatem pozostają objęte zakresem RODO.

16 Ocena odporności 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 istotnym 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 pseudonimiczne 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 każdy zabieg na pojedynczym schemacie danych (z wykorzystaniem szyfrowania lub jakichkolwiek innych matematycznych przekształceń) można uznać w najlepszym wypadku za pseudonimizację.

19 Procesy anonimizacji i ataki mające na celu deanonimizację 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 dotyczące lokalizacji (pochodzące od operatorów telekomunikacyjnych lub z usług społeczeństwa informacyjnego), o których wiadomo, że niezwykle trudno jest je zanonimizować.

20 Rzeczywiście na podstawie licznych badań wykazano,[10] że *dane dotyczące 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 być podatne na próby deanonimizacji w określonych okolicznościach.

21 Nie można w pełni zanonimizować pojedynczego schematu 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 danych dotyczących lokalizacji zagregowanych w niewielkim stopniu.

22 W celu osiągnięcia anonimizacji należy starannie przetworzyć dane dotyczące lokalizacji, by spełniły one wymogi testu racjonalności. W tym sensie takie przetwarzanie obejmuje rozpatrywanie zbiorów danych dotyczących 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 metody 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 lub kontaktów między nimi stanowi poważne naruszenie prywatności tych osób. Tego typu działania można uznać za zgodne z prawem wyłącznie w przypadku dobrowolnej akceptacji przez użytkowników na potrzeby realizacji każdego z odpowiednich celów. Oznaczałoby to w szczególności, że osoby fizyczne, które nie zdecydują się na korzystanie z takich aplikacji lub nie mogą z takich aplikacji korzystać, nie powinny odczuwać z tego powodu jakichkolwiek niedogodności.

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 w sytuacji kryzysu w dziedzinie zdrowia wywołanego przez 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 ochronę danych już w fazie projektowania i domyślną ochronę 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 fizycznych, należy wdrożyć środki, które umożliwią zapobieganie deanonimizacji;
- zgromadzone informacje powinny znajdować się na urządzeniu końcowym użytkownika, a gromadzić należy tylko istotne informacje i wyłącznie wtedy, gdy jest to bezwzględnie konieczne.

28 Jeżeli chodzi o legalność przetwarzania danych, EROD zwraca uwagę, że stosowanie aplikacji służących do ustalania kontaktów zakaźnych obejmuje przechowywanie informacji w urządzeniu końcowym lub dostęp do przechowywanych tam informacji, co podlega przepisom 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 na podstawie upoważnienia przyznanego im w przepisach oraz zgodnie z określonymi w nich wymogami, najbardziej odpowiednią podstawą prawną przetwarzania wydaje się konieczność wykonania zadania realizowanego w interesie publicznym, tj. art. 6 ust. 1 lit. e) RODO.

30 W art. 6 ust. 3 RODO wyjaśniono, że podstawę przetwarzania, o którym mowa w art. 6 ust. 1 lit. e), określa prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator.

[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.

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 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 jednak 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 podmiot będący administratorem. 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 jak najszybciej uwzględnić kryteria pozwalające stwierdzić, kiedy aplikację trzeba odinstalować, a także wskazać podmiot, który ponosi odpowiedzialność za stwierdzenie tego.

32 Jeżeli jednak przetwarzanie danych odbywa 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 z uwagi na względy interesu publicznego 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 początkowym 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 dotyczące epidemiologii takie jak okres inkubacji itd.), a dane osobowe powinny być przechowywane wyłącznie na czas trwania kryzysu wywołanego przez COVID-19. Po wyjściu z kryzysu, 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.), ale nie mogą go 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 w rzeczywistości możliwości odmowy lub wycofania swojej zgody 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 sprawiedliwość, rozliczalność oraz, szeroko rzecz ujmując, zgodność z prawem, algorytmy muszą być możliwe do kontrolowania i powinny podlegać regularnym przeglądom przez niezależnych ekspertów. Kod źródłowy aplikacji powinien być publicznie udostępniony w celu jak najszerszego nadzoru.

38 Do pewnego stopnia 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 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 istnieje duże prawdopodobieństwo wystąpienia niekorzystnych skutków, o których mowa powyżej.

39 Ponadto EROD uważa, że ocenę skutków dla ochrony danych należy przeprowadzać przed wdrożeniem takiego narzędzia, ponieważ przetwarzanie uważane jest 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 wśród innych środków z zakresu uwzględniania 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, pozycje katalogu urządzeń, wiadomości, spisy połączeń, dane dotyczące lokalizacji, identyfikatory urządzeń itp.

41 Dane przesyłane za pośrednictwem aplikacji muszą obejmować jedynie pewne niepowtarzalne i pseudonimizowane identyfikatory generowane przez aplikację i właściwe dla danej aplikacji. 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 mieć miejsce w następstwie scentralizowanego lub zdecentralizowanego podejścia[18]. Oba rozwiązania należy uznawać za realne, pod warunkiem że będą obowiązywać 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 skutków dla ochrony 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 pseudonimizowane 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 pseudonimizowanych identyfikatorów zakażonych użytkowników lub ich historię kontaktów tylko i wyłącznie do momentu poinformowania potencjalnie zakażonych

[16] Zob. Grupa Robocza Art. 29, Wytyczne (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 art. 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych".
[18] Ogólnie rzecz biorąc, rozwiązanie zdecentralizowane jest bardziej zgodne z zasadą minimalizacji.

użytkowników o ich narażeniu i nie powinien podejmować prób identyfikacji potencjalnie zakażonych użytkowników.

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 urządzeniu końcowym użytkownika i być przetwarzane wyłącznie wtedy, gdy jest to bezwzględnie niezbędne, oraz za uprzednią specjalną zgodą użytkownika.

45 Należy stosować najnowsze techniki kryptograficzne, aby zabezpieczyć dane przechowywane na serwerach oraz w aplikacjach, wymianę danych między aplikacjami oraz zdalnym serwerem. 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 pseudonimicznej 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 zakładające ważność statusu użytkownika.

47 Administrator we współpracy z organami publicznymi musi jasno i wyraźnie poinformować o linku, pod którym można pobrać oficjalną krajową aplikację służącą do ustalania kontaktów zakaźnych w celu ograniczenia ryzyka korzystania przez obywateli z aplikacji osoby 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 konieczny, ograniczony w czasie, miał minimalny wymiar i podlegał okresowym i rzeczywistym przeglądom, a także ocenie 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 dotyczące ochrony danych osobowych mogą odegrać istotną rolę w walce z wirusem. Na podstawie europejskich przepisów dotyczących ochrony danych osobowych dopuszcza się odpowiedzialne wykorzystywanie danych osobowych do celów związanych z zarządzaniem zdrowiem, zapewniając jednocześnie, aby w tym procesie nie doszło do ograniczenia praw i wolności osób fizycznych.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

ZAŁĄCZNIK – APLIKACJE SŁUŻĄCE DO USTALANIA KONTAKTÓW ZAKAŹNYCH
PRZEWODNIK DOTYCZĄCY ANALIZY

0. Zastrzeżenie

Przedstawione poniżej wytyczne nie mają charakteru nakazowego 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. Dlatego też 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 wczesnego etapu projektowania można było zagwarantować ochronę danych osobowych.

Należy zwrócić uwagę na fakt, że niniejszy przewodnik ma charakter ogólny. Dlatego też 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 osobowych. Ich celem jest zapewnienie najwyższego poziomu przejrzystości, aby promować akceptację społeczną takich 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 fizyczne 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 na temat znajdowania się w pobliżu innego użytkownika aplikacji można uzyskać bez konieczności lokalizowania użytkowników. Ten rodzaj aplikacji nie wymaga danych dotyczących lokalizacji, a zatem nie powinien wiązać się z ich wykorzystaniem;
- w przypadku zdiagnozowania u użytkownika zakażenia SARS-CoV-2 należy poinformować jedynie osoby, z którymi użytkownik miał bliski kontakt w odpowiednim z epidemiologicznego punktu widzenia okresie przechowywania danych w celu ustalenia kontaktów zakaźnych;
- 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 kontaktu wyłącznie po interwencji pracownika służby zdrowia, np. za pomocą specjalnego kodu jednorazowego;
    - informacje przechowywane na serwerze centralnym nie powinny umożliwiać administratorowi danych identyfikacji użytkowników, co do których stwierdzono, że są zakażeni lub kontaktowali się z tymi użytkownikami, ani nie powinny umożliwiać formowania wniosków dotyczących wzorców kontaktów, które nie są potrzebne do wskazania odpowiednich osób z kontaktu;
- działanie tego typu aplikacji wymaga przysłania danych, które są odczytywane przez urządzenia innych użytkowników, i odsłuchania tych komunikatów:
    - wystarczy wymienić pseudonimizowane identyfikatory pomiędzy urządzeniami mobilnymi użytkowników (jak np. komputery, tablety, sparowane zegarki itp.), np. poprzez ich przesłanie (np. za pomocą technologii Bluetooth Low Energy);
    - identyfikatory muszą być generowane przy użyciu najnowocześniejszych procesów kryptograficznych;
    - identyfikatory muszą być regularnie odnawiane, aby zmniejszyć ryzyko ataków związanych z fizycznym namierzaniem i łączeniem;
- tego typu aplikacja musi posiadać zabezpieczenia, aby zagwarantować bezpieczne procesy techniczne. W szczególności:
    - aplikacja nie powinna przekazywać użytkownikom informacji pozwalających na rozpoznanie tożsamości lub poznanie diagnozy innych osób. Serwer centralny nie może ani identyfikować użytkowników, ani interpretować informacji o nich.

Zastrzeżenie prawne: powyższe zasady odnoszą się do deklarowanego 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 musi być warunkiem wystarczającym do zapewnienia pełnej zgodności z ramami ochrony danych.

2. Definicje

Osoba z kontaktu	W przypadku aplikacji służącej do ustalania kontaktów zakaźnych osoba z kontaktu to 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 dotyczące lokalizacji	Termin ten odnosi się do wszystkich danych przetwarzanych w sieci łączności elektronicznej lub przez usługę łączności elektronicznej, wskazujących położenie geograficzne urządzenia końcowego 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 lub wysokości geograficznej urządzenia końcowego; • kierunku podróży użytkownika lub • czasu, w którym informacja o lokalizacji została zarejestrowana.
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 komunikacyjnej (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 zagrożone tym, że same się zarażą i będą zarażać inne osoby. Ustalanie kontaktów zakaźnych to metoda kontrolowania choroby polegająca na wymienieniu wszystkich osób, które znajdowały się w bliskiej odległości od nosiciela wirusa, w celu sprawdzenia, czy są one narażone na ryzyko zakażenia, i zastosowania wobec nich odpowiednich środków sanitarnych.

3. Informacje ogólne

GEN-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.
GEN-2	Najpóźniej po podjęciu decyzji o „powrocie do normalności" przez właściwe organy publiczne należy wprowadzić procedurę mającą na celu zaprzestanie gromadzenia identyfikatorów (globalne wyłączenie aplikacji, instrukcje dotyczące odinstalowania aplikacji, automatyczne odinstalowanie itp.) oraz uruchomienie procesu usuwania wszystkich zgromadzonych danych ze wszystkich baz danych (aplikacji mobilnych i serwerów).
GEN-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.
GEN-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

PUR-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.
PUR-2	Nie wolno stosować aplikacji do celów innych niż jej pierwotne zastosowanie, tj. monitorowanie przestrzegania kwarantanny lub środków izolacji, czy też ograniczenia kontaktów personalnych.
PUR-3	Aplikacji nie wolno wykorzystywać do wyciągania wniosków dotyczących lokalizacji użytkowników na podstawie ich interakcji lub innych środków.

5. Kwestie funkcjonalne

FUNC-1	Aplikacja musi zapewniać funkcjonalność umożliwiającą poinformowanie użytkowników o tym, że mogli mieć 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).

FUNC-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.
FUNC-3	Algorytm mierzący ryzyko zakażenia poprzez uwzględnienie czynników odległości i czasu, a tym samym określający, kiedy należy dodać osobę z kontaktu do listy na potrzeby ustalania kontaktów zakaźnych, musi być w bezpieczny sposób konfigurowalny, aby uwzględnić najnowszą wiedzę na temat rozprzestrzeniania się wirusa.
FUNC-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.
FUNC-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

DATA-1	Aplikacja musi posiadać funkcję przesyłania i odbierania danych za pomocą technologii komunikacji zbliżeniowej, takich jak Bluetooth Low Energy, aby można było ustalić kontakty zakaźne.
DATA-2	Przesyłane dane muszą zawierać kryptograficznie silne pseudolosowe identyfikatory, generowane przez aplikację i właściwe dla danej aplikacji.
DATA-3	Ryzyko konfliktu między pseudolosowymi identyfikatorami powinno być wystarczająco niskie.
DATA-4	Identyfikatory pseudolosowe muszą być regularnie odnawiane, z częstotliwością wystarczającą do ograniczenia ryzyka deanonimizacji, 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.
DATA-5	Zgodnie z zasadą minimalizacji danych aplikacja nie może gromadzić danych innych niż te, które są ściśle niezbędne do celów ustalania kontaktów zakaźnych.
DATA-6	Aplikacja nie może gromadzić danych dotyczących lokalizacji do celów ustalania kontaktów zakaźnych. Dane dotyczące 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.

DATA-7	Aplikacja nie powinna gromadzić danych dotyczących zdrowia poza tymi, które są absolutnie niezbędne do realizacji jej celów, z wyjątkiem dobrowolnego gromadzenia danych wyłącznie w celu pomocy w procesie podejmowania decyzji dotyczących informowania użytkownika.
DATA-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 zbliżeniowej (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	Działanie niektórych funkcji aplikacji może zależeć od podłączenia z serwerem centralnym.
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

SEC-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.
SEC-2	Dane wysyłane do serwera centralnego muszą być przesyłane bezpiecznym kanałem. Korzystanie z usług powiadamiania świadczonych przez dostawców platform OS powinno podlegać dokładnej ocenie i nie powinno prowadzić do ujawnienia danych osobom trzecim.
SEC-3	Żądania nie mogą być narażone na manipulowanie ze strony złośliwego użytkownika.
SEC-4	Należy wdrożyć najnowsze 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.
SEC-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.
SEC-6	Aby uniknąć podszywania się lub tworzenia fałszywych użytkowników, serwer musi uwierzytelnić aplikację.
SEC-7	Aplikacja musi uwierzytelnić serwer centralny.
SEC-8	Funkcje serwera powinny być chronione przed atakami przez powtórzenie (ang. *replay attacks*).
SEC-9	Informacje przesyłane przez serwer centralny muszą zostać podpisane w celu uwierzytelnienia ich pochodzenia i integralności.
SEC-10	Dostęp do wszystkich danych przechowywanych na serwerze centralnym, które nie są publicznie dostępne, musi być zastrzeżony wyłącznie dla osób upoważnionych.
SEC-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.

PRIV-1	Wymiana danych musi odbywać się z poszanowaniem prywatności użytkowników (a w szczególności z poszanowaniem zasady minimalizacji danych).
PRIV-2	Aplikacja nie może umożliwiać bezpośredniej identyfikacji użytkowników podczas korzystania z niej.
PRIV-3	Aplikacja nie może pozwalać na śledzenie ruchów użytkowników.
PRIV-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).
PRIV-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 nadzoru prowadzenie skutecznego nadzoru.
PRIV-6	Należy przeprowadzić ocenę skutków dla ochrony danych i podać ją do wiadomości publicznej.
PRIV-7	Aplikacja powinna ujawniać użytkownikowi jedynie, czy był narażony na kontakt z wirusem, oraz, w miarę możliwości bez ujawniania informacji o innych użytkownikach, czas i daty narażenia.
PRIV-8	Z informacji przekazywanych przez aplikację użytkownicy nie powinni być w stanie zidentyfikować osób będących nosicielami wirusa ani śledzić ich ruchów.
PRIV-9	Z informacji przekazywanych przez aplikację organy ds. zdrowia nie powinny być w stanie zidentyfikować potencjalnie narażonych osób bez ich zgody.
PRIV-10	Żądania wysyłane przez aplikację do serwera centralnego nie mogą ujawniać żadnych informacji na temat nosiciela wirusa.
PRIV-11	Żądania wysyłane przez aplikację do serwera centralnego nie mogą ujawniać żadnych zbędnych informacji o użytkowniku, z wyjątkiem, ewentualnie i tylko wówczas, gdy jest to konieczne, jej pseudonimizowanych identyfikatorów i listy kontaktów.
PRIV-12	Nie może istnieć możliwość przeprowadzania ataków związanych z łączeniem.
PRIV-13	Użytkownicy muszą mieć możliwość korzystania ze swoich praw za pośrednictwem aplikacji.
PRIV-14	Usunięcie aplikacji musi skutkować usunięciem wszystkich zebranych lokalnie danych.
PRIV-15	Aplikacja powinna gromadzić jedynie dane przekazywane przez wystąpienia aplikacji lub interoperacyjne równoważne aplikacje. Nie gromadzi się żadnych danych odnoszących się do innych aplikacji lub urządzeń łączności zbliżeniowej.

PRIV-16	Aby uniknąć deanonimizacji przez serwer centralny, należy zastosować serwery proxy. Zadaniem tych *niezagrażających bezpieczeństwu serwerów* 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.
PRIV-17	Należy starannie opracować i skonfigurować aplikację i serwer, aby nie gromadziły niepotrzebnych danych (np. w logach serwera nie należy umieszczać żadnych identyfikatorów itp.) oraz aby uniknąć wykorzystania SDK firmy zewnętrznej 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 zbliżeniowych, które uzyskali poprzez skanowanie, albo wysłać listę własnych identyfikatorów, które zostały przesłane na aplikację. 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 osób z kontaktu na serwer

CON-1	Serwer centralny musi zebrać historię kontaktów użytkowników, u których potwierdzono zakażenie SARS-CoV-2, w wyniku dobrowolnego działania z ich strony.
CON-2	Serwer centralny nie może przechowywać ani rozpowszechniać listy pseudonimizowanych identyfikatorów użytkowników będących nosicielami wirusa.
CON-3	Historia kontaktów przechowywana na serwerze centralnym musi zostać usunięta po powiadomieniu użytkowników o ich bliskim kontakcie z osobą zakażoną.
CON-4	Z wyjątkiem przypadków, gdy zakażony użytkownik 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.
CON-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).
CON-6	Historie kontaktów przekazywane przez różnych użytkowników nie powinny być dalej przetwarzane, np. w celu stworzenia globalnych map zbliżeniowych.
CON-7	Dane w logach 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, u których potwierdzono zakażenie 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 zakażony użytkownik 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 logach serwera muszą być ograniczone do minimum i muszą być zgodne z wymogami ochrony danych.