Umowa nr 12 /DRU/2020

na rozwój aplikacji na urządzenia mobilne proteGO Safe przeznaczonej do wsparcia autodiagnozy osób, które mogły być narażone na ryzyko zakażenia COVID-19

zawarta w Warszawie, pomiędzy:

Skarbem Państwa - **Ministrem Cyfryzacji**, z adresem do korespondencji: ul. Królewska 27, 00-060 Warszawa, NIP 521-362-16-97, REGON 145881488, zwanym dalej „**Zamawiającym**", reprezentowanym przez:

Pana Tomasza Napiórkowskiego – Dyrektora Departamentu Rozwoju Usług na podstawie pełnomocnictwa, którego kopia stanowi **Załącznik nr 1** do Umowy,

a

TYTANI24 Spółka z ograniczoną odpowiedzialnością z siedzibą we Wrocławiu, ul. Ząbkowicka 55, 50 – 511 Wrocław (adres biura: ul. Kościerzyńska 32A, Wrocław, 51 – 410), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000725465, REGON 369879064, NIP 8992843182, o kapitale zakładowym opłaconym w całości w wysokości 20 000,00 zł, reprezentowaną przez:
Pana Mateusza Romanowa - Prezesa zarządu

zwanym dalej „**Wykonawcą**",

Zamawiający oraz Wykonawca zwani dalej również łącznie „**Stronami**" lub indywidualnie „**Stroną**".

Zważywszy, że:

1) Wykonawca, na podstawie umowy nr 7/DRU/2020 zawartej w dniu 17 kwietnia 2020 r. wykonał na rzecz Skarbu Państwa - Ministra Cyfryzacji system i aplikację na urządzenia mobilne pn. ProteGO Safe 1.0 (zwane dalej **„Aplikacją"**) mającą na celu samoocenę ryzyka infekcji wirusem SARS-CoV-2, wsparcie w profilaktyce i zapobieganiu zarażeniem, ostrzeganie o ryzyku potencjalnego zarażenia COVID-19 oraz przekazywanie informacji profilaktycznych związanych z pandemią wirusa SARS-CoV-2;
2) Minister Cyfryzacji oraz Główny Inspektor Sanitarny identyfikując potrzebę budowy nowego narzędzia informatycznego, wspierającego proces wychodzenia z epidemii oraz wsparcia osób, które mogły być narażone na ryzyko zakażenia COVID-19; zawarli porozumienie dotyczące współpracy przy utrzymaniu i rozwoju Aplikacji;
3) w związku rozpoczętym przez Radę Ministrów procesem wychodzenia z najpoważniejszych obostrzeń wdrożonych do walki z epidemią COVID-19 zachodzi konieczność dalszego rozwoju Aplikacji, w celu ułatwienia monitorowania ryzyka infekcji wirusem SARS-CoV-2. przez indywidualne powiadamianie użytkownika aplikacji czy znajduje się w grupie zagrożonych ryzykiem zakażenia, a zatem osób, które

miały styczność z osobą zakażoną. W szczególności w związku z przeprowadzonymi oraz planowanymi zmianami w obowiązujących przepisach prawa;

4) rozwój Aplikacji na zasadach określonych w Umowie ma na celu wsparcie procesu wychodzenia z najpoważniejszych obostrzeń wdrożonych do walki z epidemią COVID-19
5) Wykonawca posiada szerokie doświadczenie i kompetencje niezbędne do realizacji przedmiotu Umowy z należytą starannością oraz aktualną wiedzą techniczną i informatyczną;

na podstawie na podstawie art. 6 ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. poz. 374 z późn. zm.), Strony postanowiły zawrzeć Umowę o następującej treści:

§ 1

Definicje i skróty stosowane w Umowie

1. Strony ustalają wyłącznie dla potrzeb interpretacji Umowy znaczenie następujących pojęć i skrótów:

Aplikacja	aplikacja pn. ProteGO Safe przeznaczona na urządzenia mobilne przeznaczona dla nieograniczonej liczby użytkowników do wykonania czynności oceny grupy ryzyka w oparciu o system klasyfikacji TRIAGE z możliwością odnotowania wyniku i jego zaprezentowania; co do których istnieje podejrzenie, że mogą być nosicielami choroby zakaźnej COVID-19, a także umożliwiająca tworzenie historii napotkanych urządzeń z zainstalowaną Aplikacją, a historia ta umożliwia poinformowanie użytkowników za pośrednictwem Aplikacji o tym, że mogą znajdować się w grupie wysokiego ryzyka zarażenia COVID-19.
Dokumentacja	Wszelka dokumentacja dotycząca przedmiotu Umowy, dostarczona lub wykonana w ramach realizacji Umowy.
Dzień Roboczy	Dzień od poniedziałku do piątku, w godzinach od 9:00 do 17:00,za wyjątkiem dni ustawowo wolnych od pracy.
Etap	Wyodrębniona część realizacyjna Umowy, obejmująca wykonanie określonych Prac przez Wykonawcę, szczegółowo opisanych w SOPU. Etapy podlegają Odbiorom.

Informacje poufne	informacje – niezależnie od formy ich utrwalenia lub przekazania – które nie zostały podane do publicznej wiadomości, a zostały przekazane Wykonawcy w związku z realizacją Umowy, które Zamawiający oznaczył jako poufne lub w inny sposób poinformował Wykonawcę, że traktuje je jako poufne.
Infrastruktura Zamawiającego	Infrastruktura informatyczna (w tym sprzęt i oprogramowanie sprzętowe) Zamawiającego, na której prowadzone będą prace związane z rozwojem Aplikacji, chyba że Strony postanowią inaczej.
Koordynator Umowy	Przedstawiciel Strony powołany w celu podejmowania decyzji oraz bieżącego zarządzania realizacją Umowy i poszczególnymi Etapami
Odbiór	Potwierdzenie przez Zamawiającego wykonania Etapu Umowy. Dowodem dokonania Odbioru jest odpowiedni Protokół Odbioru.
Oprogramowanie Open Source	Oprogramowanie dystrybuowane na warunkach tzw. licencji otwartych (*open source*).
Personel Wykonawcy	Pracownicy Wykonawcy oraz osoby zatrudnione w oparciu o umowę cywilnoprawną, w tym także prowadzące jednoosobową działalność gospodarczą, którym Wykonawca powierzył realizację poszczególnych czynności w ramach wykonywania Umowy.
Podwykonawca	Podmiot, któremu Wykonawca, za zgodą Zamawiającego, powierzył wykonanie części Prac wynikających z Umowy. W celu uniknięcia wątpliwości Strony potwierdzają, że Podwykonawcą nie jest członek Personelu Wykonawcy.
Prace	Czynności podjęte przez Wykonawcę zmierzające do realizacji przedmiotu Umowy zgodnie z postanowieniami Umowy.

Protokół Odbioru	Dokument potwierdzający wykonanie przez Wykonawcę Etapu i jego odebranie przez Zamawiającego na warunkach określonych w Umowie sporządzony zgodnie ze wzorem stanowiącym Załącznik nr 4 do Umowy.
Serwis GitHub	hostingowy serwis internetowy działający w domenie https://github.com/ przeznaczony dla projektów programistycznych. Wykonawca będzie zamieszczał kolejne wersje Aplikacji oraz Dokumentację Aplikacji w odpowiednim repozytorium Serwisu GitHub.
SOPU	Szczegółowy Opis Przedmiotu Umowy opisany w Załączniku nr 2 do Umowy.
Toolbox	wytyczne dotyczące ochrony prywatności użytkowników aplikacji zostały określone przez Europejską Radę Ochrony Danych w dokumencie pn. „Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection", który stanowi załącznik nr 3 do Umowy.
Umowa	Niniejsza umowa wraz z załącznikami.
Ustawa o prawie autorskim	Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j., Dz. U. z 2019 r. poz. 1231 z późn. zm.).
Utwór	Każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia, zgodnie z art. 1 Ustawy o prawie autorskim.
Wynagrodzenie	Łączne maksymalne wynagrodzenie brutto opisane w § 5 ust. 1 Umowy.

2. W przypadku terminów pisanych z wielkiej litery i niezdefiniowanych w Umowie oraz jej załącznikach, w razie wątpliwości należy uznać, że stanowią one nazwy własne.

§ 2
Przedmiot i termin realizacji Umowy

1. Przedmiotem Umowy jest wykonanie przez Wykonawcę na rzecz Zamawiającego prac związanych z rozwojem Aplikacji wraz z usługami utrzymania wraz z zapewnieniem

gwarancji na okres 3 miesięcy od dnia odbioru Aplikacji oraz usługami dodatkowymi, zgodnie ze Szczegółowym Opisem Przedmiotu Umowy (zwany dalej „SOPU"), stanowiącym załącznik nr 2 do Umowy.

2. Wykonawca wykona przedmiot Umowy zgodnie z wyraźnie wskazanymi przez Zamawiającego wytycznymi dotyczącymi ochrony prywatności użytkowników aplikacji uwzględniając w szczególności Toolbox.
3. Strony zgodnie potwierdzają, że podstawowym celem współpracy w ramach Umowy jest zapewnienie Zamawiającemu możliwości optymalnego dla Zamawiającego korzystania z Aplikacji, realizujących wszystkie funkcje przewidziane dla tych Aplikacji w SOPU w sposób na tyle zgodny z Toolbox na ile jest to możliwe biorąc pod uwagę SOPU. W przypadku sprzeczności wytycznych dotyczących ochrony prywatności określonych w Toolbox z SOPU, Wykonawca jest związany SOPU.
4. Wykonawca będzie realizował Umowę w Etapach i terminach wynikających z SOPU.
5. Procedura odbioru poszczególnych Etapów została określona w załączniku nr 4 do Umowy.

§ 3
Ogólne zasady realizacji Umowy

1. Strony deklarują współpracę w celu realizacji przedmiotu Umowy. W szczególności Strony zobowiązane są do wzajemnego powiadamiania o ważnych okolicznościach mających lub mogących mieć wpływ na wykonanie Umowy, w tym na ewentualne opóźnienia w zakresie realizacji przedmiotu Umowy. Powyższe nie wyłącza ani nie ogranicza ewentualnej odpowiedzialności Stron.
2. Wykonawca zobowiązuje się wykonywać Umowę z zachowaniem należytej staranności i profesjonalizmu uwzględniających zawodowy charakter prowadzonej przez niego działalności, zgodnie z SOPU oraz z uwzględnieniem Toolbox oraz w świadomości działania w interesie zdrowia publicznego zagrożonego rozprzestrzenianiem się choroby zakaźnej COVID-19.
3. W przypadkach, uzasadnionych względami technicznymi, Zamawiający może, w formie dokumentowej, wyrazić zgodę na użycie rozwiązań alternatywnych wobec Toolbox, jeżeli zapewniać będą one minimalny poziom ochrony praw użytkowników wynikających z RODO. Zgoda, o której mowa w zdaniu poprzedzającym, nie jest wymagana w przypadku, gdy SOPU zakłada rozwiązania alternatywne wobec Toolbox.
4. Wykonawca oświadcza, że dołoży należytej staranności, aby spełnić wymagania określone w Toolbox, które nie wpływają na SOPU, a także posiada niezbędną wiedzę, doświadczenie, potencjał techniczny i ekonomiczny oraz personel zdolny do wykonania przedmiotu Umowy, jak również, że znajduje się w sytuacji finansowej zapewniającej wykonanie Umowy.
5. Zamawiający przyjmuje do wiadomości, że terminowość i jakość wykonania Aplikacji zależy od współdziałania Zamawiającego z Wykonawcą, w tym właściwego zaangażowania Zamawiającego w szczególności co do:
   1) przekazywanych informacji Wykonawcy oraz
   2) podejmowania decyzji niezbędnych do prawidłowego przebiegu prac nad Aplikacją, w najkrótszych możliwych terminach (nie dłuższych jednak niż ustalone przez Strony w trakcie wykonywania prac wdrożeniowych).
6. Wykonawca za działania lub zaniechania osób trzecich, którymi posługuje się przy realizacji Umowy ponosi odpowiedzialność jak za działania lub zaniechania własne.

7. Wykonawca oświadcza, że realizacja Umowy nie naruszy praw osób trzecich, w szczególności autorskich praw majątkowych oraz praw licencyjnych. W przypadku naruszenia takich praw, Wykonawca ponosi odpowiedzialność względem osób trzecich i Zamawiającego. Wykonawca zwolni Zamawiającego od obowiązku zaspokojenia takich roszczeń oraz pokryje wszelkie uzasadnione, niezbędne i udokumentowane koszty obrony Zamawiającego przed roszczeniami osób trzecich, pod warunkiem, że Zamawiający łącznie:
   1) niezwłocznie poinformuje Wykonawcę o takim roszczeniu,
   2) nie uzna odpowiedzialności z tytułu takiego roszczenia,
   3) umożliwi włączenie się wykonawcy do procesu negocjacji lub postępowania sądowego w przedmiocie sporu.

W takim przypadku Wykonawca ponosi odpowiedzialność względem Zamawiającego za to, że osoby trzecie nie będą dochodziły zaspokojenia swoich roszczeń bezpośrednio od Zamawiającego.

8. Językiem Umowy i językiem stosowanym podczas jej realizacji jest język polski. Dotyczy to także całej komunikacji między Stronami. Wszystkie Produkty Umowy – o ile Umowa nie stanowi inaczej – zostaną dostarczone w języku polskim lub angielskim. Zamawiający dopuszcza dostarczenie Dokumentacji i innych materiałów dotyczących Oprogramowania w innym języku, jeśli zostały w tym języku opracowane przez producenta Oprogramowania. Zamawiający dopuszcza dostarczenie dokumentacji w postaci elektronicznej na adres email wskazany w § 15 ust. 1 pkt 1 Umowy.
9. Wykonanie Umowy nastąpi na Infrastrukturze Zamawiającego, którą Zamawiający ma obowiązek udostępniać w okresie obowiązywania Umowy w celu należytej realizacji Umowy, chyba że w Strony postanowią inaczej.
10. Zasady zdalnego połączenie Wykonawcy ze Środowiskiem Zamawiającego będą ustalane na bieżąco w trakcie realizacji prac i będą się odbywać za pomocą szyfrowanych połączeń (w tym za pomocą tunelu VPN). Zamawiający ma obowiązek na każde żądanie Wykonawcy umożliwić zdalne połączenie ze Środowiskiem Zamawiającego w uzgodniony sposób.
11. W celu uniknięcia wątpliwości Strony potwierdzają, że na podstawie Umowy Wykonawca nie odpowiada za działanie lub utrzymanie Infrastruktury Zamawiającego, chyba że nieprawidłowe działanie jest następstwem działania Wykonawcy w ramach realizacji przedmiotu Umowy.
12. Wykonawca zobowiązuje się do przekazania Zamawiającemu raportu z testów bezpieczeństwa identyfikującego ryzyka dla Aplikacji do wersji 3.1 w postaci elektronicznej na adres email wskazany w § 15 ust. 1 pkt 1 Umowy.

§ 4

Oświadczenia i zobowiązania Stron

1. W związku z realizacją Umowy, Zamawiający zobowiązuje się w szczególności do:
   1) współdziałania z Wykonawcą w granicach określonych obowiązującymi przepisami prawa oraz Umową.
   2) udostępnienia Wykonawcy wymaganych do realizacji Umowy materiałów, w szczególności informacji i dokumentów, które są lub będą w posiadaniu Zamawiającego. Zakres, warunki i terminy zapewnienia Wykonawcy dostępu do materiałów zostaną ustalone przez Strony w trakcie realizacji Umowy niezwłocznie w miarę pojawiających się potrzeb Wykonawcy. Strony ustalają, że przekazane materiały

będą mogły być wykorzystywane, modyfikowane i przekazywane pracownikom i Podwykonawcom przez Wykonawcę, stosownie do potrzeb wynikających z realizacji Umowy;

3) niezwłocznego informowania Wykonawcy o:
   a) zamiarze wprowadzenia zmian organizacyjnych u Zamawiającego lub podmiotów współpracujących z Zamawiającym, mogących mieć wpływ na przebieg Prac lub innych czynności związanych z realizacją przedmiotu Umowy;
   b) planowanych i przewidywanych zmianach w zakresie przedmiotu Umowy lub jego modyfikacji.

2. Wykonawca jest zobowiązany realizować Umowę z dochowaniem należytej staranności, przy uwzględnieniu zawodowego charakteru tej działalności, z wykorzystaniem całej posiadanej wiedzy i doświadczenia, zgodnie z SOPU oraz Toolbox oraz w świadomości działania w interesie zdrowia publicznego zagrożonego rozprzestrzenianiem się choroby zakaźnej COVID-19
3. Wykonawca zobowiązuje się w szczególności do:
   1) przekazywania na żądanie Zamawiającego informacji związanych z Umową, w szczególności informacji dotyczących postępów Prac, przyczyn ewentualnych opóźnień lub przyczyn nienależytego wykonania Umowy. Informacje będą przekazywane za pośrednictwem e-mail lub w formie pisemnej do Zamawiającego w uzasadnionym terminie wskazanym w żądaniu Zamawiającego pozwalającym na jego realizację, w tym na udzielenie odpowiedzi bez negatywnego wpływu na przebieg Prac
   2) bieżącego informowania Zamawiającego o realizacji Umowy,
   3) wykorzystania i modyfikacji zasobów udostępnionych przez Zamawiającego wyłącznie do celów związanych z realizacją Umowy;
   4) ile nic innego nie wynika wprost z Umowy, Wykonawca jest zobowiązany zapewnić narzędzia, w tym oprogramowanie, licencje i inne zasoby niezbędne do realizacji przedmiotu Umowy swojemu personelowi.

§ 5
Wynagrodzenie i warunki płatności

1. Wynagrodzenie za realizację przedmiotu Umowy wynosi 1 884 000 zł netto [słownie: jeden milion osiemset osiemdziesiąt cztery tysiące złotych 00/100], co wraz z podatkiem VAT w wysokości 433 320 zł [słownie: czterysta trzydzieści trzy tysiące trzysta dwadzieścia złotych 00/100] stanowi kwotę 2 317 320 zł [słownie: dwa miliony trzysta siedemnaście tysięcy trzysta dwadzieścia złotych 00/100], w tym za wynagrodzenie za poszczególne Etapy:
   Etap 1 Aplikacja wersja 2.0: 290.000,00 zł. (słownie: dwieście dziewięćdziesiąt tysięcy),
   Etap 2 Aplikacja wersja 3.0: 280.000,00 zł. (słownie: dwieście osiemdziesiąt tysięcy),
   Etap 3 Aplikacja wersja 3.1: 364.000,00 zł. (słownie: trzysta sześćdziesiąt cztery tysiące),
   Etap 4 Aplikacja wersja 3.2: 335.000,00 zł. (słownie: trzysta trzydzieści pięć tysięcy),
   Etap 5 Aplikacja wersja 3.3: 140.000,00 zł. (słownie: sto czterdzieści tysięcy),
   Etap 6 Testy manualne i maszynowe: 120.000,00 zł. (słownie: sto dwadzieścia tysięcy),
   Etap 7 Testy cyberbezpieczeństwa: 240.000,00 zł. (słownie: dwieście czterdzieści tysięcy),
   Etap 8 Komunikacja Aplikacji: 95.000,00 zł (dziewięćdziesiąt pięć tysięcy),
   Etap 9 Przygotowanie raportu implementacji API Google w Aplikacji: 20.000,00 zł. (słownie: dwadzieścia tysięcy).
2. Wykonawcy nie przysługują żadne inne roszczenia poza Wynagrodzeniem, określonym w ust. 1, w stosunku do Zamawiającego, w szczególności zwrot kosztów podróży oraz

zakwaterowania czy też zwrot jakichkolwiek innych, dodatkowych kosztów ponoszonych przez Wykonawcę związanych z wykonywaniem Umowy. Wynagrodzenie obejmuje w szczególności wynagrodzenie za wykonanie Przedmiotu Umowy, przeniesienie autorskich praw majątkowych, udzielenie licencji lub udzielenie Zamawiającemu innych uprawnień wskazanych w paragrafie regulującym prawa własności intelektualnej.

3. Podstawą do wystawienia faktury VAT będą odpowiednie Protokoły Odbioru podpisane przez obie Strony.
4. Wynagrodzenie należne Wykonawcy w ramach realizacji Zamówienia płatne będzie na podstawie prawidłowo wystawionych faktur VAT, w terminie do 14 dni od daty dostarczenia Zamawiającemu faktury VAT, na rachunek bankowy wskazany na fakturze VAT.
5. Za termin płatności przyjmuje się dzień obciążenia rachunku bankowego Zamawiającego.
6. Zamawiający wyraża zgodę na wystawianie i przesyłanie faktur VAT w formie elektronicznej na adres mailowy: mc@mc.gov.pl.

§ 6.

Prawa własności intelektualnej

1. Wykonawca oświadcza, iż jest twórcą Aplikacji w wersji 1.0 i przeniósł na podstawie zawartej pomiędzy Stronami umowy z dnia 17 kwietnia 2020 r. odpowiednio prawa autorskie bądź udzielił licencji do systemu i Aplikacji w wersji 1.0 a zakres przysługujących mu praw umożliwia dokonanie zmian w systemie i Aplikacji do kolejnych wersji wskazanych w Umowie i ma prawo do przeniesienia bądź udzielenia licencji Zamawiającemu.
2. Jeżeli w wyniku realizacji Umowy powstaną Utwory zastosowanie mają postanowienia niniejszego paragrafu.
3. Wykonawca oświadcza, że na podstawie Umowy – odpowiednio – przeniesie na Zamawiającego majątkowe prawa autorskie zgodnie z § 7 lub udzieli mu licencji opisanych Umową zgodnie z § 8 Umowy, lub w inny sposób opisany Umową upoważni go do korzystania ze wszystkich dóbr własności intelektualnej wykonanych lub dostarczonych w ramach Umowy, w szczególności do Utworów
4. Wykonawca jest świadomy, że celem Zamawiającego jest możliwość samodzielnego lub za pomocą osób trzecich wdrożenia nowych funkcjonalności i dalszego rozwoju Aplikacji. Wykonawca oświadcza, że warunki, na których kolejne wersje Aplikacji będą udostępniane Zamawiającemu, nie będą zawierać ograniczeń, które uniemożliwiałyby dokonanie takich czynności przez Zamawiającego lub osoby trzecie.
5. Wykonawca oświadcza, że przekazane w ramach Umowy Utwory nie będą posiadały żadnych wad prawnych, nie będą ograniczać Zamawiającego w korzystaniu z tych dóbr z zastrzeżeniem postanowień stosownych licencji lub w inny sposób ani nie będą naruszać praw, w tym praw własności intelektualnej, osób trzecich.
6. Przy wytwarzaniu kolejnych wersji Aplikacji Wykonawca może wykorzystać Oprogramowanie Open Source.
7. W każdym przypadku wykorzystania Oprogramowania Open Source Wykonawca zapewnia, że jego wykorzystanie na potrzeby wykonywania Umowy będzie zgodne z postanowieniami licencji, na jakiej dane Oprogramowanie Open Source jest udostępniane.
8. Licencja na Oprogramowanie Open Source nie może ograniczać Zamawiającego i nakładać na Zamawiającego obowiązku odprowadzania jakichkolwiek opłat lub wynagrodzenia na

rzecz podmiotów uprawnionych do takiego oprogramowania, chyba że Strony postanowią inaczej, co zostanie potwierdzone w formie pisemnej.

9. W przypadku korzystania z podwykonawców, Wykonawca zobowiązuje się do nabycia praw, w tym praw własności intelektualnej w zakresie pozwalającym na wykonanie zobowiązań wobec Zamawiającego określonych w Umowie.
10. Wykonawca zobowiązuje się i gwarantuje, że osoby uprawnione z tytułu autorskich praw osobistych do Utworów w rozumieniu Prawa autorskiego, dostarczonych lub wykonanych w ramach Umowy, nie będą wykonywać tych praw w stosunku do Zamawiającego lub osób trzecich działających na zlecenie Zamawiającego. W odmiennym przypadku zastosowanie znajdzie § 3 ust. 6 Umowy.
11. Jeżeli Zamawiający nie będzie mógł korzystać z kolejnych wersji Aplikacji z uwagi na okoliczności leżące po stronie Wykonawcy, Wykonawca, na swój koszt uzyska niezwłocznie dla Zamawiającego stosowne prawa lub zezwolenia umożliwiające kontynuowanie korzystania z niej.
12. Jakiekolwiek postanowienie Umowy, w tym załączników do niej, nie ogranicza uprawnień Zamawiającego wynikających z obowiązujących przepisów prawa, w tym z art. 75 ust. 1 - 3 Prawa autorskiego.

§ 7.

Prawa autorskie

1. Z dniem podpisania odpowiedniego Protokołu Odbioru Wykonawca przenosi na Zamawiającego, w ramach wynagrodzenia za dany Etap, autorskie prawa majątkowe do Utworów wytworzonych lub dostarczonych w ramach realizacji Umowy:
   1) kodu źródłowego kolejnych wersji Aplikacji;
   2) odpowiedniej Dokumentacji kolejnych wersji Aplikacji, która będzie publikowana w repozytorium Serwisu GitHub;
   3) materiałów graficznych wykorzystanych w kolejnych wersjach Aplikacji;

a Zamawiający je przyjmuje. Przeniesienie na Zamawiającego autorskich praw majątkowych do Utworów dla swojej skuteczności nie będzie wymagało dodatkowych czynności rozporządzających.

2. Przeniesienie praw autorskich, o którym mowa w ust. 1, następuje na następujących polach eksploatacji:
   1) w stosunku do Utworów nie będących programami komputerowymi:
      a) w zakresie utrwalania i zwielokrotniania Utworu - trwałe lub czasowe utrwalanie i zwielokrotnianie Utworów w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, w tym także utrwalanie i zwielokrotnianie Utworów dowolną techniką, w tym techniką zapisu magnetycznego lub techniką cyfrową, taką jak zapis na płycie CD, DVD, Blu-ray, urządzeniu z pamięcią flash lub jakimkolwiek innym nośniku pamięci;
      b) w zakresie obrotu oryginałem albo egzemplarzami, na których Utwór utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarz;
      c) w zakresie rozpowszechniania Utworów w inny sposób, w tym ich publiczne wykonywanie, wystawianie, wyświetlanie, odtwarzanie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć dostęp do Utworów w miejscu i w czasie przez siebie wybranym.
   2) w stosunku do Utworów będących programami komputerowymi:

a) trwałego lub czasowego zwielokrotnienia programu komputerowego w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie; w zakresie, w którym dla wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania programu komputerowego niezbędne jest jego zwielokrotnienie, czynności te wymagają zgody uprawnionego;
b) tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym, z zachowaniem praw osoby, która tych zmian dokonała;
c) rozpowszechniania, w tym użyczenia lub najmu, programu komputerowego lub jego kopii.

3. Z dniem podpisania odpowiedniego Protokołu Odbioru, w ramach wynagrodzenia za wykonanie danego Etapu, Wykonawca:
   1) zapewnia zezwolenie autora Utworu na wykonywanie zależnych praw autorskich do wszelkich zmian i opracowań Utworów (lub ich poszczególnych elementów), tj. zezwalania na rozporządzanie i korzystanie z takich opracowań na polach eksploatacji wskazanych w ust. 2;
   2) przenosi na Zamawiającego własność wydanych Zamawiającemu nośników, na których zostały utrwalone Utwory (lub ich poszczególne elementy) w celu przekazania ich Zamawiającemu.
4. Zamawiający jest uprawniony do korzystania z Utworów w zakresie wskazanym w ust. 2 i ust. 3 od daty udostępnienia Utworów Zamawiającemu do daty nabycia autorskich praw majątkowych przez Zamawiającego, a Wykonawca zapewnia, że takie korzystanie nie będzie naruszać praw osobistych lub majątkowych Wykonawcy ani osób trzecich i nie będzie powodować obowiązku zapłaty jakichkolwiek dodatkowych opłat.
5. Wykonawca zobowiązuje się do niewykonywania praw osobistych do Utworów, jak również zobowiązuje się, iż osoby uprawnione z tytułu osobistych praw do Utworów nie będą wykonywać tych praw.
6. Zamawiający zobowiązany jest do niezwłocznego powiadomienia Wykonawcy na piśmie o wystąpieniu osób trzecich z roszczeniami z tytułu korzystania przez Zamawiającego z Utworów.
7. Wykonawca udostępni Zamawiającemu kod źródłowy kolejnych wersji Aplikacji, również w formie wykonywalnej, wraz z całą dokumentacją i wyraża zgodę na jego modyfikację przez Zamawiającego lub za pomocą osób trzecich.
8. Zamawiający zobowiązuje Wykonawcę do opublikowania kodu źródłowego kolejnych wersji Aplikacji (także w formie wykonywalnej), wraz z całą dokumentacją w repozytorium Serwisu GitHub na minimum 24 godziny przed publikacją kolejnych wersji Aplikacji zgodnie z SOPU. Wykonawca zamieści w dokumentacji Serwisu GitHub informację, że Zamawiający udziela na Aplikację licencji GNU General Public Licence 3.0. Licencja GNU General Public License 3.0 jest licencją typu Open Source, co oznacza, że po przeniesieniu na Zamawiającego autorskich praw majątkowych oraz licencji zgodnie odpowiednio z §9 oraz §8, Zamawiający udziela licencji Open Source na każdą kolejną wersję Aplikacji, a zatem Aplikacja przyjmie status Oprogramowania Open Source.

§ 8.
Licencja

1. W zakresie w jakim przeniesienie autorskich praw majątkowych na Zamawiającego okaże się niemożliwe, Wykonawca oświadcza, że w ramach realizacji Umowy udziela

Zamawiającemu prawa do korzystania z kolejnych wersji Aplikacji bez żadnych ograniczeń czasowych, terytorialnych, liczby serwerów, userów z możliwością wykorzystania przez Skarb Państwa bez żadnych ograniczeń, z prawem do modyfikacji, bez prawa do udzielenia sublicencji, na następujących polach eksploatacji:

1) trwałego lub czasowego zwielokrotnienia kolejnych wersji Aplikacji w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie; w zakresie, w którym dla wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania kolejnych wersji Aplikacji niezbędne jest jej zwielokrotnienie;
2) tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w kolejnych wersjach Aplikacji, z zachowaniem praw osoby, która tych zmian dokonała;
3) rozpowszechniania, w tym użyczenia lub najmu, i Aplikacji lub ich kopii, Zamawiający może zainstalować, używać, wyświetlać, konfigurować lub w inny sposób korzystać interaktywnie (działania te są łącznie zwane dalej "URUCHAMIANIEM") z 1 kopii Aplikacji zainstalowanej na pojedynczym serwerze dla nieograniczonej liczby użytkowników - pracujących na komputerach, stacjach roboczych, terminalach, komputerach przenośnych, smartfonach, tabletach lub innych cyfrowych urządzeniach elektronicznych oraz za pośrednictwem Internetu;
4) Zamawiający ma prawo przechowywać lub zainstalować kopię kolejnych wersji Aplikacji na urządzeniu do przechowywania danych, takim jak serwer sieciowy, wykorzystywanym do uruchamiania Aplikacji na innych komputerach lub urządzeniach mobilnych Zamawiającego w ramach jego wewnętrznej sieci;
5) Zamawiający uzyskuje prawo do posługiwania się analogicznymi do dowolnego środowiska produkcyjnego środowiskiem zapasowym i środowiskiem testowym, zainstalowanymi na oddzielnych serwerach;
6) Zamawiający ma prawo udzielać nieodpłatnie swoją licencję innym organom państwa;
7) w ramach udzielonej licencji Zamawiający ma prawo korzystać z aplikacji w modelu SaaS lub on-premise, a także równocześnie w obydwu tych modelach, według własnego uznania.

§ 9.
Odpowiedzialność i kary umowne

1. Zamawiający naliczy Wykonawcy karę umowną za niewykonanie lub nienależyte wykonanie Umowy w następujących przypadkach i wysokościach:
   1) za zwłokę w realizacji każdego z Etapów wykonania Aplikacji w wysokości 0,5 % Wynagrodzenia za realizację Etapu, za każdy dzień zwłoki względem terminu określonego w SOPU;
   2) w przypadku naruszenia zasad poufności w wysokości 5.000 zł (słownie: pięć tysięcy złotych) za każdy przypadek naruszenia;
   3) w przypadku naruszenia zasad ochrony lub zasad przetwarzania danych osobowych w wysokości 5.000 zł (słownie: pięć tysięcy złotych) za każdy przypadek naruszenia;
   4) za zwłokę w realizacji Utrzymania, o którym mowa w pkt. 5 SOPU, w terminach o których mowa w pkt. 5 ppkt. 7 SOPU w wysokości odpowiednio:
      a) 1000 zł (słownie: jeden tysiąc złotych 00/100) za każdy rozpoczęty dzień roboczy zwłoki w usunięciu Błędu Krytycznego,
      b) 250 zł (słownie: dwieście pięćdziesiąt złotych 00/100) za każdy rozpoczęty dzień roboczy zwłoki w usunięciu każdego innego błędu.

2. W przypadku odstąpienia przez Zamawiającego od Umowy z winy Wykonawcy, Zamawiający naliczy Wykonawcy karę umowną w wysokości 10 % maksymalnego Wynagrodzenia.
3. Naliczenie kar umownych zostanie udokumentowane wystawieniem i przesłaniem noty księgowej wraz z uzasadnieniem naliczenia kary umownej.
4. Kary umowne płatne będą w terminie 14 dni od otrzymania noty księgowej przez Stronę zobowiązaną do zapłacenia kary umownej, z zastrzeżeniem, iż Zamawiający może potrącić kary umowne z wynagrodzenia Wykonawcy.
5. Naliczenie zastrzeżonych Umową kar umownych nie wyłącza prawa Stron do dochodzenia odszkodowania przewyższającego wysokość kar umownych na zasadach ogólnych do pełnej wysokości szkody poniesionej przez daną Stronę w związku ze zdarzeniem, które było podstawą naliczenia danej kary, z zastrzeżeniem ust. 7.
6. Strony zgodnie ustalają, że kary umowne nałożone na Wykonawcę w związku z realizacją Umowy nie mogą przekroczyć wartości 100% Wynagrodzenia za realizację Zamówienia, którą to wartość Strony przyjmują, jako maksymalny i łączny limit kar umownych.
7. Odpowiedzialność Wykonawcy z tytułu realizacji niniejszej Umowy jest w każdym przypadku ograniczona do wysokości 100% wynagrodzenia należnego Wykonawcy za wykonanie Umowy.
8. Odpowiedzialność Wykonawcy z tytułu realizacji niniejszej Umowy jest oparta na zasadzie winy i powinna uwzględniać stopień przyczynienia się przez Zamawiającego do wystąpienia szkody lub okoliczności, która tą szkodę spowodowała. Strony uzgadniają, że odpowiedzialność Stron za utracone korzyści oraz szkody pośrednie zostaje niniejszym wyłączona.

§ 10.
Podwykonawstwo

1. Wykonawca może zlecić, za pisemną zgodą Zamawiającego, część zadań wynikających z realizacji Umowy podwykonawcom.
2. Zamawiający wyraża zgodę na skorzystanie przez Wykonawcę z następujących podwykonawców:
    1) The Coders Sp. z o.o. KRS 0000719006, NIP 8971852135;
    2) Webini Sp. z o.o. KRS 0000609484, NIP 8943075719;
    3) Sigma Connectivity Sp. z o.o. KRS 0000550367, NIP 5272732872;
    4) 25wat Sp. z o.o. KRS 0000628003, NIP 8982222308;
    5) Mobile Flag Piotr Wicherski NIP 9522031820, REGON 385066963;
    6) HOLDAPP ARTUR OZIERAŃSKI NIP 899-26-35-130, REGON 021929159.
3. Wykonawca ponosi odpowiedzialność za wszelkie działania i zaniechania podwykonawców związane z realizacją przedmiotu Umowy, w tym za bezpieczeństwo przekazanych danych, jak za działania i zaniechania własne, niezależnie od podjętych przez Zamawiającego działań sprawdzających wynikających z Umowy lub przepisów prawa.
4. Wykonawca gwarantuje, że podwykonawcy uczestniczący w wykonaniu Umowy spełnią wyraźnie wskazane przez Zamawiającego lub Wykonawcę wymagania określone w Toolbox, a także posiadają niezbędną wiedzę, doświadczenie, potencjał techniczny i ekonomiczny oraz personel zdolny do wykonania przedmiotu Umowy.

§ 11.

Rozwiązanie Umowy

1. Zamawiający jest uprawniony do odstąpienia od Umowy w części, która nie została odebrana w przypadku, gdy Wykonawca:
   1) nie realizuje Umowy i pozostaje bezczynny po upływie wyznaczonego terminu, pomimo uprzedniego wezwania Wykonawcy przez Zamawiającego do przystąpienia do realizacji Umowy z jednoczesnym określeniem terminu, nie krótszego niż 2 dni robocze, z zagrożeniem odstąpienia od Umowy w razie jego bezskutecznego upływu;
   2) realizuje Umowę w sposób niezgodny z celem Umowy, postanowieniami Umowy lub przepisami prawa, pomimo uprzedniego wezwania Wykonawcy przez Zamawiającego do zaprzestania i usunięcia skutków naruszeń z jednoczesnym określeniem terminu, nie krótszego niż 2 dni robocze, z zagrożeniem odstąpienia od Umowy w razie jego bezskutecznego upływu;
   3) w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie przedmiotu Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy.
2. Strony zastrzegają dla oświadczenia o odstąpieniu od Umowy formę pisemną lub elektroniczną opatrzoną podpisem kwalifikowanym, zaufanym lub osobistym pod rygorem nieważności.
3. Strony zobowiązują się w terminie 5 Dni roboczych od dnia odstąpienia od Umowy do sporządzenia protokołu, który będzie stwierdzał stan realizacji Umowy do dnia odstąpienia od Umowy.
4. Zamawiający w protokole, o którym mowa w ust.3, wskaże, które Prace chce zatrzymać, a Wykonawca zachowa prawo do wynagrodzenia za te Prace w wysokości wynikającej z Umowy, a jeżeli będzie to niewystarczające (np. w przypadku niedokończonych Prac) – w stosunku do udokumentowanego nakładu pracy Wykonawcy od dnia odbioru ostatniego etapu Prac do dnia odstąpienia przez Zamawiającego.
5. Zamawiający z dniem podpisania protokołu, o którym mowa w ust.4, nabędzie autorskie prawa majątkowe do Utworów stanowiących przedmiot Prac na polach eksploatacji wskazanych w § 7 ust. 2 lub. 3 lub Wykonawca udzieli licencji na polach eksploatacji wskazanych w § 8 ust. 1.

§ 12.
Poufność

1. Wykonawca zobowiązuje się:
   1) nie ujawniać Informacji poufnych innym podmiotom bez zgody Zamawiającego, udzielonej na piśmie pod rygorem nieważności;
   2) wykorzystywać Informacje poufne jedynie na potrzeby realizacji Umowy;
   3) nie powielać Informacji poufnych w zakresie szerszym, niż jest to potrzebne dla realizacji Umowy;
   4) zabezpieczać otrzymane Informacje poufne przed dostępem osób nieuprawnionych w stopniu niezbędnym do zachowania ich poufnego charakteru, ale przynajmniej w takim samym stopniu, jak postępuje wobec własnej tajemnicy przedsiębiorstwa.
2. Dla uniknięcia wątpliwości Strony potwierdzają, że za Informacje poufne nie są uważane informacje, które Zamawiający jest zobowiązany ujawnić na mocy obowiązujących przepisów, w tym ustawy – Prawo zamówień publicznych i ustawy o dostępie do informacji publicznej.

3. Wykonawca może, jeżeli jest to niezbędne do realizacji Umowy, udostępnić Informacje poufne personelowi Wykonawcy, przy czym korzystanie z informacji poufnych przez takie podmioty nie może wykroczyć poza zakres, w jakim Wykonawca może z nich korzystać. Wykonawca zobowiąże te osoby do przestrzegania poufności. Wykonawca jest odpowiedzialny za naruszenia postanowień Umowy spowodowane przez takie osoby.
4. W przypadku rozwiązania Umowy (niezależnie od powodu rozwiązania) lub jej wygaśnięcia Wykonawca zwróci w terminie 7 (słownie: siedmiu) dni materiały zawierające informacje poufne, a informacje poufne przechowywane w wersji elektronicznej usunie ze swoich zasobów i nośników elektronicznych. Ten sam obowiązek będzie ciążył na podwykonawcach.
5. Wykonawca na pisemne żądanie Zamawiającego zobowiązuje się do niezwłocznego zniszczenia materiałów zawierających Informacje poufne.

§ 13.
Ochrona danych osobowych

1. Wykonawca zobowiązuje się do zapewnienia operacji przetwarzania danych osobowych zgodnie z wymaganiami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
2. Szczegółowe ustalenia w zakresie dotyczącym przetwarzania danych osobowych przy użyciu Aplikacji zawarte zostały w Załącznik nr 5 stanowiącym umowę powierzenia przetwarzania danych osobowych, która zostanie podpisana przed rozpoczęciem przetwarzania danych.

§ 14.
Gwarancja

1. W ramach Wynagrodzenia Wykonawca udziela Zamawiającemu gwarancji na utwory wskazane w § 7 ust 1 na okres 3 miesięcy licząc od daty podpisania odpowiedniego ~~Protokołu Odbioru Etapu.~~
2. Gwarancja udzielona zostaje bez ograniczeń terytorialnych, tj. obejmuje terytorium Rzeczypospolitej Polskiej i całego świata.
3. Dla uniknięcia wątpliwości przyjmuje się, że Wykonawca usunie zgłoszone wady pomimo zakończenia okresu gwarancyjnego, o ile zostały one zgłoszone przed zakończeniem terminu obowiązywania gwarancji.
4. Wykonawca nie odpowiada w ramach udzielonej gwarancji, o której mowa w ust. 1, za wady powstałe w wyniku niewłaściwej obsługi lub modyfikacji Aplikacji, tj. obsługi niezgodnej z dostarczoną dokumentacją lub bez uprzedniej konsultacji z Wykonawcą połączenia z innymi programami komputerowymi lub aplikacjami.
5. Umowa stanowi dokument gwarancyjny bez konieczności składania dodatkowego dokumentu na okoliczność udzielenia gwarancji.
6. Zamawiający uprawniony jest do wykonywania uprawnień z tytułu rękojmi za wady Zamówienia, niezależnie od uprawnień wynikających z gwarancji, przy czym Strony ograniczają obowiązywanie rękojmi do ostatniego dnia okresu gwarancji.

§ 15.

Postanowienia końcowe

1. Strony wyznaczają następujące osoby jako Koordynatorów Umowy oraz podpisanie odpowiedniego Protokołu Odbioru Etapu:
   1) ze strony Zamawiającego: Tomasz Napiórkowski,
   2) ze strony Wykonawcy: Mateusz Romanów,
2. Zmiana osób i danych wskazanych w ust. 1 nie wymaga zmiany Umowy i następuje w drodze pisemnego poinformowania drugiej Strony.
3. Wykonawca nie jest uprawniony do przeniesienia praw, obowiązków, ani wynikających z Umowy na osobę trzecią bez pisemnej zgody Zamawiającego.
4. Korespondencję przesłaną na adresy Stron określone w komparycji Umowy uważa się za skutecznie doręczoną, chyba że Strony poinformują się pisemnie o zmianie adresów.
5. W sprawach nieuregulowanych Umową zastosowanie mają w szczególności przepisy ustawy — kodeksu cywilnego.
6. Zmiany Umowy wymagają zachowania formy pisemnej lub postaci elektronicznej opatrzonej podpisem kwalifikowanym, zaufanym lub osobistym pod rygorem nieważności.
7. W przypadku, gdy poszczególne postanowienia niniejszej Umowy zostaną uznane za nieważne lub bezskuteczne, nieważność lub bezskuteczność danego przepisu nie ma wpływu na ważność lub skuteczność pozostałych postanowień niniejszej Umowy. Strony dołożą wszelkich starań, aby zastąpić nieważne lub nieskuteczne postanowienie innymi, ważnymi postanowieniami.
8. Spory wynikłe w związku z realizacją Umowy będzie rozpoznawał sąd właściwy miejscowo dla siedziby Zamawiającego.
9. Integralną część Umowy stanowią:
   1) Załącznik nr 1 – Pełnomocnictwo dla Pana Tomasza Napiórkowskiego do zawarcia Umowy,
   2) Załącznik nr 2 – Szczegółowy Opis Przedmiotu Umowy,
   3) Załącznik nr 3 – Toolbox,
   4) Załącznik nr 4 – Procedura odbioru prac,
   5) Załącznik nr 5 – Wzór umowy powierzenia przetwarzania danych osobowych.

Ze strony Zamawiającego	**Ze strony Wykonawcy**
Tomasz Napiórkowski	**Mateusz Romanów**
Dyrektor Departamentu Rozwoju Usług	**Prezes Zarządu**
W Ministerstwie Cyfryzacji	**TYTANI24 Spółka z ograniczoną odpowiedzialnością**
/podpisano elektronicznie/	/podpisano elektronicznie/

Szczegółowy Opis Przedmiotu Zamówienia

Przedmiotem Umowy jest opracowanie i dostarczenie aplikacji na urządzenia mobilne przeznaczonej dla nieograniczonej liczby użytkowników do wykonania czynności oceny stanu zdrowia z możliwością odnotowania wyniku i jego zaprezentowania; co do których istnieje podejrzenie, że mogą być nosicielami choroby zakaźnej COVID-19 (zwane dalej „Aplikacją" lub "ProteGO Safe"). Aplikacja będzie również posiadała zaimplementowany moduł Bluetooth służący do tzw. Bluetooth Tracing. Moduł ten umożliwia tworzenie historii napotkanych urządzeń z zainstalowaną Aplikacją, a historia ta umożliwia poinformowanie użytkowników za pośrednictwem Aplikacji o tym, że mogą znajdować się w grupie wysokiego ryzyka zarażenia COVID-19. Aplikacja zostanie wykonana zgodne z KEY VISUAL brandingu gov.pl bazując na przykładowych projektach interfejsu aplikacji dostępnym pod linkiem: https://zpl.io/a70ZWnW.

1. Opis procesu UX do implementacji w aplikacji:

1.1. Etap 1 - Zakres funkcjonalności dla wersji 2.0

1. Użytkownik instaluje Aplikację na telefonie Android,
2. Użytkownik otwiera Aplikację i wyświetlają mu się informacje o sposobie jej działania i potrzebnych zgodach/uprawnieniach (akceptacja Regulaminu i Polityki Prywatności).
3. Użytkownik uzupełnia metrykę zdrowia.
4. Użytkownik wypełnia pierwszy test oceny ryzyka (triaż).
5. Użytkownik dostaje pierwszy wynik klasyfikacji swojego stanu zdrowia (triaż).
6. Użytkownik odbiera notyfikacje push przypominające o potrzebie wypełnienia testu oceny ryzyka.
7. Aplikacja prowadzi użytkownika przez porady i zachowania związane z jego stanem zdrowia na podstawie oceny ryzyka (triażu).
8. Użytkownik może wypełniać dowolną ilość razy dziennie: test oceny ryzyka (triaż) i dziennik zdrowia.
9. Po trzech dniach, w których użytkownik przynajmniej raz dziennie wypełnił test oceny ryzyka w Aplikacji wyświetla się odznaka "Dbam o siebie i bliskich".
10. W przypadku Aplikacji dla systemu iOS - użytkownik musi wyrazić zgodę na "Pozwolenie na wysyłanie notyfikacji".

Zakres:
- celowy i pożądany brak synchronizacji z Google Analytics
- brak rejestracji użytkownika w Aplikacji przy użyciu numeru telefonu

- dane z modułów: Metryka, test oceny ryzyka i dziennik zdrowia są zapisywane lokalnie na telefonie

1.2. Etap 2 - Zakres funkcjonalności dla wersji 3.0

1. Użytkownik pobiera aplikację ProteGO Safe 3.0 z modułem OpenTrace i nie ma w niej możliwości (i widoku) podania numeru telefonu (użytkownik nie podaje numeru telefonu w aplikacji - nie zbieramy tych danych w żaden sposób). Serwer Firebase przyznaje aplikacji (a nie numerowi telefonu) UID czyli zanonimizowany indywidualny numer danej instalacji (aplikacji).
2. Backend Firebase Google Authenticator ProteGO Safe (MC) zapisuje UID aplikacji - przez co jest w stanie komunikować się z aplikacją. Do każdego UID backend generuje TempID (zapisuje na urządzeniu tablicę z listą numerów TempID na 2 tygodnie do przodu, które aplikacja będzie cyklicznie, co 15 minut, zmieniała). TempID służą do anonimizacji użytkowników w module tracingowym (kontakt Bluetooth w "realu").
3. Użytkownik jest proszony o wyrażenie zgody na:
    3.1. Android: Lokalizacja (żeby skanować inne urządzenia w okolicy trzeba mieć zgodę na "Lokalizację". W praktyce jest to możliwość tracingu przez bluetooth; nie ma możliwości ustalania geolokalizacji urządzenia za pośrednictwem GPS).
    3.2. iOS: "Pozwolenie na używanie modułu Bluetooth".
4. Po wyrażeniu zgody, określonej w pkt. 3, aplikacja uruchamia moduł OpenTrace, który działa w tle (tylko w systemie Android, w systemie iOS możliwości działania Bluetooth w aplikacji działającej "w tle" są bardzo ograniczone), również po opuszczeniu aplikacji i zablokowaniu ekranu (na tyle na ile pozwala na to system operacyjny). Moduł bluetooth nie działa przy wyłączonej aplikacji.
5. Moduł OpenTrace rozgłasza się po Bluetooth ze swoim TempID.
6. TempID aplikacji jest rotowane tj. zmieniane co 15 minut zgodnie z bazą zapisaną na telefonie ilość kodów określimy w parametrach(tablica). Częstotliwość pobierania nowej paczki TemID jest również określana jako parametr w konfiguracji.
7. Moduł OpenTrace skanuje otoczenie w celu wykrycia innych użytkowników i zapisuje dane: timestamp, msg (TempID), modelC, modelP, rssi, txPower, org. . Dane te są zapisywane w lokalnej pamięci telefonu. Zapewnienie bezpieczeństwa prywatności użytkownika odbywa się poprzez ukrycie go pod TempID zmieniającym się co 15 min.

Zakres:
- bez kalibracji urządzeń pod kątem mocy sygnału Bluetooth
- bez wymiany danych do serwera
- bez analityki po stronie backend
- bez integracji z EWP.

1.3. Etap 3 - Zakres funkcjonalności dla wersji 3.1

1. Aplikacja zostaje rozszerzona o funkcjonalność generowania kodów QR (kod QR jest ustandaryzowany z TempID).
2. Dla każdego statusu triażu użytkownika jest przypisany kod QR w kolorze triażu
3. Aplikacja zyskuje funkcjonalność skanowania kodów QR wygenerowanych na innych urządzeniach z aplikacją PS,

4. Użytkownik jednej aplikacji może łatwo zeskanować kod QR drugiego użytkownika; w ten sposób TempID urządzenia zapisuje takie spotkanie jako bezpośrednie; jeżeli zestaw danych ze skanowania Bluetooth wykaże, że urządzenia widziały się przez więcej niż 15 min, oznacza to, że był to kontakt bezpośredni trwający więcej niż 15 minut.
5. Aplikacja w tej wersji obejmuje możliwość wyboru pomiędzy korzystaniem z aplikacji w trybie osoby fizycznej oraz instytucji.
6. Dodanie parametru osoba/instytucja do przyznawania UID
7. Tryb Instytucji obsługuje następujące funkcje:
    7.1. Rejestracja konta Instytucji
    7.2. Oparcie rejestracji Instytucji o wymagalność aktualnego kodu NIP danej Instytucji. Aplikacja będzie umożliwiała import danych z bazy CEIDG a następnie ich akceptację przez Użytkownika Aplikacji na koncie Instytucji
    7.3. Zapisanie danych kontaktowych Instytucji
    7.4. Wygenerowanie kodu QR przypisanego do TempID Instytucji.
    7.5. Wygenerowanie akcji stworzenia plakatu z kodem QR instytucji i nazwą instytucji wynikającą z NIP.
    7.6. Możliwość wysłania plakatu z kodem QR instytucji na podanego przy rejestracji instytucji emaila do kontaktu
    7.7. Możliwość wyświetlania w koncie Instytucji listy ostrzeżeń aplikacji, związanych z danymi wysyłanymi z OP BACKEND, o zweryfikowanych chorych na COVID-19 którzy potwierdzili swoją obecność w Instytucji poprzez zeskanowanie kodu QR wyświetlonego w trybie Instytucji przez Instytucję. Ostrzeżenia/notyfikacje o których mowa w niniejszym punkcie nie będą zawierały danych umożliwiających bezpośrednią identyfikację osoby fizycznej.
    7.8. Możliwość ręcznej weryfikacji podmiotów zakładających konta Instytucji
    7.9. Możliwość tymczasowego zawieszenia/odwieszenia konta Instytucji.

Use case'y (kontekst):

7.10. W zakładzie u fryzjera/kosmetyczki jest wydrukowany kod QR-kod. Po skorzystaniu z usługi użytkownik dobrowolnie może zeskanować kod – teraz jeżeli okaże się, że osoba wykonująca zabieg była nosicielem COVID-19 klient odpowiednio wcześnie dostanie taką informację.
7.11. Pracownicy pracujący na zmianie w fabryce w swoim bezpośrednim sąsiedztwie odbijają się raz dziennie;
7.12. W każdej taksówce kod QR kierowcy z możliwością odbijania się pasażerów.
7.13. Uczestnicy spotkania dostają materiały (cyfrowe/papierowe) i na tych kartkach gdzieś na marginesie albo w stopce strony są QRy wszystkich jego uczestników, bo je wcześniej nadesłali osobie organizującej spotkanie. Wtedy nie trzeba "pokazywać sobie telefonów".
7.14. Uczestnicy spotkania biznesowego 1to1 lub w innym mniejszym gronie; w tym wizyty przedstawicieli handlowych;

Wizyta w salonie samochodowym/u mechanika / na stacji kontroli pojazdów Zakres:

- rozbudowa JSON o parametr pewności kontaktu

1.4. Etap 4 - Zakres funkcjonalności dla wersji 3.2

Kontekst: Osoba zdiagnozowana medycznie jako chora na chorobę COVID-19 podaje swój numer telefonu do przedstawiciela organu zdrowia - w praktyce ten numer jest dołączony do testu na COVID-19.

Pracownik medyczny/laboratorium dodaje numer telefonu osoby zakażonej do rejestru CSIOZ.

1. Serwer z backend (codename: OP-BACKEND, do decyzji MC jaki podmiot będzie administrował Serwerem OP-BACKEND) odbiera informacje z rejestru CSIOZ (codename bazy: EWP) o osobie z potwierdzonym zakażeniem COVID-19 (numer telefonu, data diagnozy).
2. Centrum Kontaktu podejmuje kontakt telefoniczny z osobą zarażoną COVID-19 i pyta, czy osoba ta ma zainstalowaną aplikację ProteGO Safe.
   1.1. Chory NIE JEST użytkownikiem aplikacji:
   Proces kontaktu się kończy.
   2.1. Chory JEST użytkownikiem aplikacji:
   Operator prosi użytkownika o podanie kodu PIN, który zostanie wyświetlony na urządzeniu po użyciu funkcji PIN w jego aplikacji. Operator wprowadza kod PIN w OP-BACKEND.
3. OP-BACKEND wykonuje połączenie ID użytkownika z numerem telefonu (autoryzacja i połączenie numeru telefonu z ID aplikacji/użytkownika) - w ten sposób łączy konkretną zainfekowaną osobą z konkretnym urządzeniem, z którego ta osoba korzysta.
4. Po poprawnym wprowadzeniu PIN dane z historią spotkanych TempID innych urządzeń z ostatnich (do decyzji MC) z parametrem ilości dni są wysyłane z urządzenia osoby zakażonej na Serwer z backendem ProteGO Safe.
5. Moduł zapisu danych historycznych (listy spotkanych urządzeń - lista TempID) zapisuje w bazie danych na Serwerze uploadowane dane (powiązane z danym UID użytkownika i datą uploadu oraz PINem).
   5.1. Gdy dane zostały wysłane z aplikacji aplikacja zmienia status TRIAGE w aplikacji na "Chory na COVID-19". - musimy mieć pewność, że backend odebrał dane.
   5.2. Aplikacja umożliwia zdjęcie statusu „Chory na COVID-19" po wprowadzeniu stosownej notyfikacji ze strony GIS.
6. Moduł przetwarzający i analizujący dane historyczne analizuje dane i określa jakie TempID miały kontakt z osobą zarażoną spełniające kryteria kwalifikacji kontaktu (minimum 15 minut) jako narażający osobę na zarażenie. Moduł ten kojarzy TempID z ID użytkowników w aplikacji.
7. Backend ProteGO Safe wysyła powiadomienia PUSH do osób zakwalifikowanych jako osoby będące w grupie wysokiego ryzyka zarażeniem z zestawem danych: o zmianie grupy ryzyka na wysoką, że miał kontakt z osobą chorą na COVID-19 na podstawie parametrów określonych na backendzie (parametryzowane dane: czas inkubacji choroby, czas kwarantanny, czas zbierania i przechowywania, parametry spotkania tj. czas i odległość w ciągu ostatnich X-dni-parametr dni lub ilości dni od dnia uruchomienia OpenTrace jeżeli ten został uruchomiony w czasie krótszym niż 14 dni.
8. Aplikacja zmienia status grupy ryzyka w TRIAGE (funkcja samooceny ryzyka zarażenia) na WYSOKA GRUPA RYZYKA i wyświetla stosowne dalsze wytyczne.

9. Użytkownik, który został oznaczony jako "grupa wysokiego ryzyka", zostaje poinformowany przez aplikację pod jaki numer Centrum Kontaktu ma dzwonić. Jeżeli użytkownik zadzwoni do Centrum Kontaktu, jest prowadzony i wspierany przez Centrum Kontaktu. System przewiduje możliwość zniesienia informacji „chory na COVID" w oparciu o parametr dostarczony przez GIS.

- Opis integracji OP-BACKEND z rozwiązaniem ProteGO Safe: łączymy się bezpośrednio z bazą Firestore, umiejscowioną na hostingu FireBase w organizacji MC z której korzysta app ProteGO Safe w celu uzupełniania listy dostępnych kodów PIN i ich zarządzania.

1.5. Etap 5 - Zakres funkcjonalności dla wersji 3.3

1. Stworzenie modułów automatycznej aktualizacji treści w Aplikacji z danymi dostępnymi na stronach rządowych.
2. Automatyzacja projektu (przygotowanie skryptów które będą automatycznie synchronizowały ProteGO Safe).
3. Automatyzacja zostanie zaimplementowana dla zestawów danych:
   3.1. synchronizacja danych z pacjent.gov.pl;
   3.2. synchronizacja danych z pytań i odpowiedzi z https://www.gov.pl/web/koronawirus/pytania-i-odpowiedzi;
   3.3. synchronizacja danych teleadresowych szpitalów zakaźnych;
   3.4. synchronizacja i rozwój porad przekazywanych Użytkownikom Aplikacji ze stron rządowych https://www.gov.pl/web/koronawirus/porady.

1.6. Etap 6 - Testy manualne i maszynowe

1. W skład wykonywanych typów testów wchodzą przede wszystkim testy funkcjonalne, których głównym celem jest wykrywanie błędów implementacji funkcjonalności zawartych w dokumentacji.
2. Przeprowadzenie analizy na podstawie wymagań platformowych produktu i dostępnych analiz rynkowych w celu zidentyfikowania urządzeń, i ich odpowiedniej konfiguracji, niezbędnych do przeprowadzenia testów. Analiza będzie dotyczyć pokrycia platformowego produktu stronę web, PWA, aplikację na platformę Android i aplikację na platformę iOS. W skład analizy wchodzą zarówno konfiguracje o największej krytyczności jak i najpopularniejsze urządzenia w celu zwiększenia pokrycia urządzeń, na których będzie dokonywana kalibracja aplikacji.
3. Stworzenie dokumentu określającego plan testów przeprowadzanych w ramach zapewniania jakości w procesie wytwarzania produktu.
4. Stworzenie dokumentacji technicznej procesu testowego, w skład której wchodzą narzędzia, opisy procesów i wszystkie niezbędne informacje dla osób powiązanych z procesem QA.

5. Przeprowadzenie testów akceptacyjnych w formie Beta testów i testów eksploracyjnych na użytkownikach niezwiązanych z procesem wytwórczym produktu.
6. Wszelkie problemy i sugestie będą zbierane w dedykowanym narzędziu do zarządzania błędami. Każde zgłoszenie będzie analizowane i wprowadzane do systemu zarządzania zadaniami projektowymi.
7. Przeprowadzenie testów kompatybilności z urządzeniami i wersjami platform o najwyższym priorytecie poprzez uruchomienie testów dymnych z wykorzystaniem narzędzi typu Crawler.
8. Przeprowadzenie testów eksploracyjnych i zdrowotnych na aplikacji w wersjach 3.0, 3.1, 3.2 i 3.3 w formie przedwydaniowej na urządzeniach fizycznych.
9. Zestaw skrytów weryfikujących poprawność działania podstawowych ścieżek krytycznych w aplikacji PWA, w celu monitorowania ciągłości stabilności wdrożeń na środowisku testowym.

1.7. Etap 7 - Testy cyberbezpieczeństwa

Analiza infrastruktury i bezpieczeństwa

1. Testy bezpieczeństwa - pierwszy podmiot o renomowanej rynkowo opinii z zakresu testów bezpieczeństwa
2. Testy bezpieczeństwa - przeprowadzone przez drugi podmiot o renomowanej rynkowo opinii z zakresu testów bezpieczeństwa
3. Kod źródłowy Aplikacji trafia do prywatnego repozytorium w Serwisie Github,
4. Jeśli kod trafił do tak zwanego pre-release jest wykonywany automatyczny proces
   - budowania Aplikacji z ustawieniami dla środowiska dev/stage,
   - podstawowy test potwierdzający, że Aplikacja się zbudowała,
   - uruchamiany jest skaner automatycznie wykrywający znane podatności. Wybraliśmy do tego celu dostępne w ramach GitHub Marketplace rozwiązanie Whitesource for Github
   - następnie czekamy na drugą opinię skanera podatności tym razem dostarczanego przez firmę Snyk również przez GitHub marketplace.
5. Jeśli któryś z elementów drzewa zależności Aplikacji wymaga poprawek a są one dostępne następuje próba usunięcia podatności.
6. Jeśli nie mamy już zgłoszeń od wewnętrznych testerów przekazujemy Aplikację do środowiska produkcyjnego.
7. Kod źródłowy Aplikacji trafia do publicznego repozytorium w Serwisie Github
8. Jeśli kod łączony jest z masterem po manualnym potwierdzeniu i review przez min 2 uprawnionych użytkowników (powoływana jest kolejna oficjalna produkcyjna wersja Aplikacji) jest wykonywany automatyczny proces
   - budowania Aplikacji z ustawieniami dla środowiska produkcyjnego,
   - podstawowy test potwierdzający, że aplikacja się zbudowała,

- uruchamiany jest skaner automatycznie wykrywający znane podatności. Wybraliśmy do tego celu dostępne w ramach GitHub Marketplace rozwiązanie Whitesource for Github,
- następnie czekamy na drugą opinię skanera podatności tym razem dostarczanego przez firmę Snyk również przez GitHub marketplace,
Jeśli któryś z elementów drzewa zależności Aplikacji wymaga poprawek a są one dostępne następuje próba usunięcia podatności.

9. Jeśli nie mamy już zgłoszeń od wewnętrznych testerów przekazujemy aplikację do środowiska produkcyjnego.

1.8. Etap 8 - Komunikacja Aplikacji

1. Warsztat projektowy analizujący komunikacje celem przygotowania brandingu Aplikacji.
2. Stworzenie nowego logotypu w oparciu o wytyczne.
3. Przygotowanie paczki z logotypami w formatach .png .jpg i .pdf,
4. Stworzenie key visual w oparciu o materiały gov.pl
5. Optymalizacja fanpage pod kątem informacji o projekcie ProteGO Safe
6. Zaprojektowanie 3 głównych grafik w 15 formatach (PR,Social Media) wg wytycznych od Zamawiającego w celu komunikacji o projekcie ProteGO Safe
7. Zaprojektowanie serii grafik w 2 formatach dla umieszczenia aplikacji w Google Store i Apple Store,
8. Przygotowanie opisów aplikacji dla umieszczenia aplikacji w Google Store i Apple Store (w sumie +4000zzs) i przesłanie do Zamawiającego.
9. Przygotowanie szablonów edytowalnych grafik ProteGO Safe i przesłanie do Zamawiającego
10. monitoring mediów w zakresie komunikacji i obserwacja opinii publicznej

1.9. Etap 9 – Przygotowanie raportu implementacji API Google w Aplikacji

Wykonawca przeanalizuje dokumentację API Google contact tracing wydane przez Google LLC z siedzibą w 1600 Amphitheatre Parkway, Mountain View, Kalifornia, Stany Zjednoczone Ameryki, a następnie przygotuje raport implementacji API Google contact tracing w Aplikacji. Raport, o którym mowa w zdaniu poprzedzającym zostanie sporządzony w terminie 14 dni od opublikowania przez Google kompletnej dokumentacji dotyczącej API Google contact tracing. Raport, o którym mowa w zdaniu pierwszym niniejszego punktu będzie zawierał w szczególności opis środowiska API Google, możliwości implementacji API Google contact tracing w Aplikacji, a także harmonogram oraz szacunkowy koszt takiej implementacji.

I. Wymagania dla urządzeń końcowych:

a) Smartfon z systemem operacyjnym Android nie starszym niż wersja 6 oraz nie nowszym niż aktualna, publicznie dostępna wersja systemu operacyjnego na dzień zawarcia umowy, z aktualnym oprogramowaniem w postaci przeglądarki Internet (Chrome lub Safari aktualne wstecz 2 miesiące od wersji systemu aktualnej w dniu ukazania się określonej wersji app PS) oraz aktywnym dostępem do sieci.

b) Smartfon z systemem iOS nie starszym niż 12.1 oraz nie nowszym niż aktualnie, publicznie dostępna wersja systemu operacyjnego na dzień zawarcia umowy, z aktualnym oprogramowaniem w postaci przeglądarki Internet (Chrome lub Safari aktualne wstecz 2 miesiące od wersji systemu aktualnej w dniu ukazania się określonej wersji app PS) oraz aktywnym dostępem do sieci.

II. Harmonogram realizacji

Data wdrożenia	Etap	Wersja Aplikacji (jeśli dotyczy)	Odpowiedzialny	Opis wdrożenia
27/04/2020	Etap 1	2.0	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.1
27/04/2020	Etap 2	3.0	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.2
08/05/2020	Etap 3	3.1	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.3
13/05/2020	Etap 4	3.2	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.4

25/05/2020	Etap 5	3.3	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.5
25/05/2020	Etap 6	-	Wykonawca	Zgodny z Zakresem opisanym w punkcie 1.6
25/05/2020	Etap 7	-	Wykonawca (przy wsparciu podwykonawców)	Zgodny z Zakresem opisanym w punkcie 1.7
30/06/2020	Etap 8	-	Wykonawca	Zgodny z Zakresem opisanym w punkcie 1.8
14 dni od opublikowania stosownej dokumentacji	Etap 9	-	Wykonawca	Zgodny z Zakresem opisanym w punkcie 1.9

2. Sposób realizacji wdrożenia

Poniższa tabela przedstawia harmonogram realizacji wdrożenia zawierający rozpisane zadania, wraz z opisem technicznym i końcową datą ich wykonania.

2.1 Etap 1 – wersja aplikacji 2.0

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Integracja modułu PWA	Integracja SafeSafe w aplikacji Android	Aktywność wyświetlająca moduł PWA z poprawną obsługą nawigacji w aplikacji, obsługa layoutów.	Do 27.04.2020	290 000 PLN
	Integracja SafeSafe w aplikacji iOS	Aktywność wyświetlająca moduł PWA z poprawną	Do 27.04.2020	

		obsługą nawigacji w aplikacji, obsługa layoutów.		
Powiadomienia PUSH z wykorzystaniem Firebase Cloud Messaging	Opracowanie powiadomień PUSH	Opracowanie i dokumentacja typów powiadomień PUSH, wykorzystywanych modeli danych i potrzebnych kanałów dystrybucyjnych (topiców).	Do 27.04.2020	
	Powiadomienia PUSH w aplikacji Android	Integracja z Firebase, obsługa kilku typów powiadomień FCM, rejestracja na odpowiednie kanały dystrybucyjne, wstrzykiwanie danych z notyfikacji do aplikacji i przekazanie ich do modułu PWA.	Do 27.04.2020	
	Powiadomienia PUSH w aplikacji iOS	Integracja z Firebase, obsługa kilku typów powiadomień FCM, rejestracja na odpowiednie kanały dystrybucyjne, wstrzykiwanie danych z notyfikacji do aplikacji i przekazanie ich do modułu PWA.	Do 27.04.2020	
Komunikacja PWA i native	Opracowanie komunikacji pomiędzy kodem natywnym i modułem PWA.	Opracowanie i dokumentacja metod i modeli danych dla JS Bridge'a do komunikacji pomiędzy natywnym kodem aplikacji a modułem PWA.	Do 27.04.2020	
	Wdrożenie komunikacji pomiędzy natywnym kodem i modułem PWA w aplikacji Android.	Implementacja JS bridge'a w aplikacji Android.	Do 27.04.2020	
	Wdrożenie komunikacji pomiędzy natywnym kodem i modułem PWA w	Implementacja JS bridge'a w aplikacji iOS.	Do 27.04.2020	

	aplikacji iOS.		
Publikacja aplikacji	Publikacja aplikacji Android w sklepie Google Play.	Przygotowanie wersji release aplikacji, uzupełnienie informacji o aplikacji, wdrożenie wersji produkcyjnej do sklepu, obsługa releasów wersji pośrednich (z poprawkami błędów i nowymi zmianami), prace związane z review aplikacji, przyspieszeniem publikacji.	Do 27.04.2020
	Publikacja aplikacji iOS w sklepie Apple App Store.	Przygotowanie wersji release aplikacji, uzupełnienie informacji o aplikacji, wdrożenie wersji produkcyjnej do sklepu, obsługa releasów wersji pośrednich (z poprawkami błędów i nowymi zmianami), prace związane z review aplikacji, przyspieszeniem publikacji.	Do 27.04.2020
Uruchomienie projektu developerskiego	Wytworzenie środowiska developerskiego	Konfiguracja narzędzi do obsługi środowiska testowego	Do 27/04/2020
	Wytworzenie i konfiguracja środowiska staging	Konfiguracja narzędzi do wytwarzania kodu w projekcie	Do 27/04/2020
	Dodanie funkcjonalności autodeploy na środowisko stage	Konfiguracja narzędzi do publikacji kodu na środowisko testowe	Do 27/04/2020
	- wybicia taga z wersją na gitlab - manual przycisk do deploy	Automatyzacja deploy na produkcję	Do 27/04/2020
Produkcja aplikacji	Napisanie kodu frontend i logiki backend do obługi	Przygotowanie logiki do realizacji kolejnych zadań w projekcie	Do 27/04/2020

	MVP aplikacji		
	Analiza dokumentacji technicznej API Infermedica	Analiza techniczna działania API i przygotowanie do użycia w aplikacji	Do 27/04/2020
	Analiza dokumentacji technicznej API Infermedica	Sprawdzenie i zweryfikowanie kluczy API Infermedica	Do 27/04/2020
		Wdrożenie i przetestowanie flow API z Infermedica	Do 27/04/2020
		Dodanie klikalnego numeru telefonu w treści	Do 27/04/2020
		Dodanie walidacji pól tam, gdzie jest to możliwe. Akceptacja zgód, Imię, Wiek, Liczba lat	Do 27/04/2020
		Opracowanie możliwości współpracy między ReactNative a Android dla Bluetooth	Do 27/04/2020
		Zaprojektowanie i wdrożenie UI dla ekranu instalacyjnego PWA Android	Do 27/04/2020
		Zaprojektowanie i wdrożenie UI dla ekranu instalacyjnego PWA IOS	Do 27/04/2020
		Dodanie ekranu "jak to działa"	Do 27/04/2020
		Funkcjonalność zapisywania danych z metryczki	Do 27/04/2020
		Dodanie ekranów końcowych	Do

		"co mam zrobić"	27/04/2020
		Dodanie regulaminu aplikacji	Do 27/04/2020
		Dodanie "numerów alarmowych"	Do 27/04/2020
		Dodanie ekranu "profilaktyka"	Do 27/04/2020
		Ankieta Oceny Ryzyka dodać funkcjonalność wielowyboru	Do 27/04/2020
		Dodanie funkcjonalności usunięcia danych dotyczących zdrowia	Do 27/04/2020
		Dodanie widoku podsumowania metryczki	Do 27/04/2020
		Dodanie ekranu ładowania po wypełnieniu ankiety	Do 27/04/2020
		Dodanie loadera pomiędzy ekranami ankiety	Do 27/04/2020
		Implementacja kontentu w aplikacji	Do 27/04/2020
		Wykrywanie czy jesteśmy w WebView - Podczas uruchamiania aplikacji w androidzie w web view nie należy pokazywać ekranów instalacji	Do 27/04/2020

		Zmiana funkcjonowania menu w zależności od środowiska PWA/Desktop	Do 27/04/2020
		Zmiana layoutu w Ankiecie oceny ryzyka - zależne od kontentu	Do 27/04/2020
		Możliwość odznaczenia odpowiedzi w ankiecie - zmiana względem pierwotnego założenia	Do 27/04/2020
		Dodanie polityki prywatności	Do 27/04/2020
		Dodanie funkcjonalności "cofnij" przy wypełnianiu metryczki	Do 27/04/2020
		Dodanie funkcjonalności "zaktualizuj aplikację"	Do 27/04/2020
		Wygenerowanie APK dla Android z webview	Do 27/04/2020
		Opracowanie sposobu komunikacji pomiędzy webview a Android	Do 27/04/2020
	Stylowanie Frontend	Zmienione copy na nowe. Odseparowanie elementu PL i numeru telefonu	Do 27/04/2020
		W dzienniku zdrowia usunięcie numeru telefonu	Do 27/04/2020
		Dodanie numeru telefonu podczas "rejestracji"	Do 27/04/2020
		Zmiana koloru pod imieniem	Do

		na zgodny z brandbook ministerstwa	27/04/2020
		Zmiana designu pierwszego ekranu powitalnego na zgodny z Ministerstwem	Do 27/04/2020
		Dodanie nowego widoku "szpitali zakaźnych"	Do 27/04/2020
		Wstrzyknięcie hashu numeru telefonu dla Android'a	Do 27/04/2020
		Dodanie buttona "pomoc"	Do 27/04/2020
		Zmiana górnego zdjęcia na niebieską belkę - zgodną z Ministerstwem	Do 27/04/2020
		Zmiana stylowania buttonów - np. "dalej" na zgodne z Ministerstwem	Do 27/04/2020
		Dodanie ekranu urządzeń z którymi był kontakt powyżej 5 minut	Do 27/04/2020
		Stworzenie środowiska deweloperskiego w raz z automatyzacją budowania i releasowania aplikacji	Do 27/04/2020
		Osadzenie modułu skanowania Bluetooth w aplikacji	Do 27/04/2020
		Opracowanie scenariusza testowego Bluetooth dla GovTech	Do 27/04/2020
		Wprowadzenie plików Aplikacji do repozytorium	Do 27/04/202

		GitHub. Obrandowanie repozytorium.	0
		Wybór i wdrożenie platformy zarządzania treścią	Do 27/04/2020
		Podmiana logotypu aplikacji	Do 27/04/2020
		Redesign widoku "numery alarmowe"	Do 27/04/2020
		Aktualizacja ekranów wynikowych testu (triage) - 6 różnych widoków	Do 27/04/2020
		Przerobienie na nowy design bocznego menu	Do 27/04/2020
		Aktualizacja widoków wynikowych TRIAGE - synchro z Pacjent.gov.pl	Do 27/04/2020
		Przerobienie widoku ankiety oceny ryzyka	Do 27/04/2020
		Przerobienie widoków rejestracji zgodnie z nowymi wytycznymi	Do 27/04/2020
		Prace nad rozpoznawaniem przeglądarek w trybie PWA	Do 27/04/2020
		Fixy związane z błędnie działającym buttonem "powrót"	Do 27/04/2020
		Dodanie nowej belki nawigacyjnej do stopki	Do 27/04/2020

		Zmiany w funkcjonowaniu zakładki "szpitale zakaźne"	Do 27/04/2020	
		Update zakładki SPOTKANIE URZĄDZENIA	Do 27/04/2020	
		Dodanie trzech widoków explainera na pierwszych ekranach aplikacji	Do 27/04/2020	
		Zmiana fontów w aplikacji PWA	Do 27/04/2020	
		Usunięcie przycisku "cofnij" na ekranie "home" aplikacji	Do 27/04/2020	
		Obsługa powiadomień [push notifications]	Do 27/04/2020	
		Nowy design ekranu zakończenia pierwszego kwestinariusza	Do 27/04/2020	
	Opracowanie dokumentacji Aplikacji w wersji 2.0	Opracowanie dokumentacji funkcjonalności Aplikacji w wersji 2.0 oraz opublikowanie dokumentacji w repozytorium Serwisu GitHub.	Do 27/04/2020	

2.2 Etap 2 – wersja aplikacji 3.0

Analiza rozwiązania OpenTrace (BlueTrace)	Analiza dokumentacji technicznej i kodu źródłowego projektu OpenTrace	Dogłębna analiza rozwiązań technicznych zastosowanych w OpenTrace w obszarach: - contact tracing z wykorzystaniem technologii Bluetooth	Do 27/04/2020	280 000 PLN

		- security - cloud integration	
Integracja OpenTrace w aplikacji	Dodanie modułu OpenTrace w aplikacji Android	Integracja kodu źródłowego, przerobienie interfejsu pomiędzy warstwą UI oraz warstwą biznesową (logiczną), usunięcie widoków OpenTrace, debugowanie i testy.	Do 27/04/2020
	Dodanie modułu OpenTrace w aplikacji iOS	Integracja kodu źródłowego, przerobienie interfejsu pomiędzy warstwą UI oraz warstwą biznesową (logiczną), usunięcie widoków OpenTrace, debugowanie i testy.	Do 27/04/2020
UX	Obudowanie aplikacji Android o wymagane flow i widoki UI.	Analiza wymagań UX dla obsługi modułu OpenTrace, dodanie obsługi wymaganych pozwoleń i ustawień w systemie, dodanie odpowiednich powiadomień i widoków pozwalających użytkownikowi przygotować aplikację do wydajnego działania. Obsługa działania aplikacje w tle, w sposób ciągły, również po restarcie telefonu. Obsługa stanów aplikacji i telefonu.	Do 27/04/2020
	Obudowanie aplikacji iOS o wymagane flow i widoki UI.	Analiza wymagań UX dla obsługi modułu OpenTrace, dodanie obsługi wymaganych pozwoleń i ustawień w systemie, dodanie odpowiednich powiadomień i widoków pozwalających użytkownikowi przygotować aplikację do wydajnego działania. Obsługa działania aplikacje w tle, w sposób	Do 27/04/2020

		ciągły, również po restarcie telefonu. Obsługa stanów aplikacji i telefonu.	
Integracja z Backend	Integracja z częścią serwerową systemu w aplikacji Android.	Przygotowanie i wdrożenie komunikacji z Backend osadzonym w środowisku Firebase z uwzględnieniem rozwiązań zastosowanych w OpenTrace, z naciskiem na bezpieczeństwo danych. wdrożenie autoryzacji w trybie anonimowym. Opracowanie i wdrożenie rozwiązań transferu danych zgromadzonych w aplikacji na Backend dla użytkownika potwierdzonego zarażeniem.	Do 27/04/2020
		Przygotowanie i wdrożenie komunikacji z Backend osadzonym w środowisku Firebase z uwzględnieniem rozwiązań zastosowanych w OpenTrace, z naciskiem na bezpieczeństwo danych. wdrożenie autoryzacji w trybie anonimowym.	Do 27/04/2020
	Integracja z częścią serwerową systemu w aplikacji iOS.	Opracowanie i wdrożenie rozwiązań transferu danych zgromadzonych w aplikacji na Backend dla użytkownika potwierdzonego zarażeniem.	
		Nowy ekran podglądu wpisu do Dziennika zdrowia	Do 27/04/2020
		Implementacja nowego kontraktu pomiędzy native, a web	Do 27/04/2020
		Ukrycie w kroku rejestracji podania numeru telefonu	Do 27/04/2020
		Dziennik zdrowia - dodanie	Do

		nowego formularza	27/04/2020	
		Wystawienie nowego kontrakt bridge'u pomiędzy webview a nativeapp	Do 27/04/2020	
		Wytworzenie dokumentacji bridge pomiędzy PWA a Nativeapp	Do 27/04/2020	
		Zmiana nagłówka do wersji z logotypem Protego Safe	Do 27/04/2020	
Bug bash 3.0	Przeprowadzenie zbiorowych testów eksploracyjnych aplikacji w wersji 3.0		Do 27/04/2020	

2.3 Etap 3 – wersja aplikacji 3.1 kody QR

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Stworzenie dokumentacji		Dokumentacja developerska projektu - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 08/05/2020	174 000 PLN
Zarządzanie repozytorium	dodajemy plik licencji	Ustrukturyzowanie i uporządkowanie	Do 08/05/202	

GitHub	synchronizacja release/3.2.0 z masterem	repozytorium Aplikacji w serwisie Github, która umożliwi zapewnienie transparentności prac nad Aplikacją.	0	
Funkcjonalność skanowania kodów QR	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Aplikacja zyskuje możliwość skanowania kodów QR z wynikiem triażu	Do 08/05/2020	
Funkcjonalność generowania kodów QR	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Aplikacja zyskuje możliwość generowania kodów QR z wynikiem triażu	Do 08/05/2020	
Stworzenie dokumentacji obrazującej funkcjonalność konta Instytucji	Wykonanie dokumentacji tekstowej i graficznej	Opis wszystkich procesów niezbędnych do zachowania ciągłości dostępności konta Instytucji	Do 08/05/2020	5 000 PLN
Stworzenie dokumentacji developerskiej funkcjonalności Instytucji	Wykonanie dokumentacji tekstowej	Dokumentacja developerska projektu konta Instytucji - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 08/05/2020	5 000 PLN
Stworzenie dwóch rodzajów kont: konto osoby fizycznej i konto Instytucji	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Użytkownik aplikacji może zdecydować z jakiego konta chce korzystać. Umożlwiamy dwa konteksty: Kontekst Osoby Fizycznej i Instytucji	Do 08/05/2020	10 000 PLN
Rejestracja konta Instytucji	1. Wykonanie widoku UI. 2. Obsługa wersji	Aplikacja wprowadza nowy rodzaj konta: konto Instytucji z osobnym parametrem	Do 08/05/202	20 000 PLN

	Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	zapisywane na OP-BACKEND	0	
Import danych po numerze NIP	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Oparcie rejestracji Instytucji o wymagalność aktualnego kodu NIP danej Instytucji	Do 08/05/2020	15 000 PLN
Kod QR Instytucji	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Wygenerowanie kodu QR przypisanego do TempID Instytucji na stałe (w przeciwieństwie do końca osoby fizycznej gdzie TempID są rotowane)	Do 08/05/2020	15 000 PLN
Tworzenie plakatu z kodem QR Instytucji	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Wygenerowanie na backendzie akcji stworzenia plakatu z kodem QR instytucji i nazwą instytucji wynikającą z NIP.	Do 08/05/2020	20 000 PLN
Wysyłka plakatu z kodem QR na email	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Możliwość wysłania plakatu z kodem QR instytucji na podanego do kontaktu emaila	Do 08/05/2020	10 000 PLN
Ostrzeżenia kontaktów osób chorych na COVID-19	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Możliwość wyświetlania w koncie Instytucji listy ostrzeżeń aplikacji, związanej z danymi wysyłanymi z OP BACKEND, o zweryfikowanych chorych na COVID-19 którzy potwierdzili swoją obecność z	Do 08/05/2020	10 000 PLN

		Instytucji poprzez zeskanowanie kodu QR w Instytucji (plakat).		
Oprogramowanie funkcjonalności backend do weryfikacji kont	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Rozbudowanie zaplecza backend o 1. Możliwość ręcznej weryfikacji podmiotów zakładających konta Instytucji 2. Możliwość zakładania kont operatorów i ich weryfikacji 3. System ticketowania Instytucji na backendzie	Do 08/05/2020	50 000 PLN
Funkcja zawieszania/odwieszania konta instytucji	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Możliwość tymczasowego zawieszenia/odwieszenia konta Instytucji. Wykonanie widoków UI po stronie OP-Backend oraz po stronie aplikacji użytkownika końcowego, którego konto zostało tymczasowo zawieszone/odwieszone	Do 08/05/2020	20 000 PLN
Funkcja zdalnego blokowania kodu QR Instytucji	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS 3. funkcjonalność wpięta w OP-BACKEND	Operator OP-Backendu posiada możliwość zdalnego blokowania kodu QR instytucji, która została zawieszona.	Do 08/05/2020	10 000 PLN

2.4 Etap 4 – wersja aplikacji 3.2

Powiadomienia PUSH z wykorzystaniem Firebase Cloud Messaging dla modułu contact tracing	Opracowanie powiadomień PUSH wykorzystanych dla rozwiązania contact tracing.	Opracowanie i dokumentacja typów powiadomień PUSH, wykorzystywanych modeli danych i potrzebnych kanałów dystrybucyjnych (topiców).	Do 13/05/2020	
	Wdrożenie powiadomień PUSH w aplikacji Android	Obsługa kilku typów powiadomień FCM, wyświetlanie odpowiednich notyfikacji (UI), wstrzykiwanie danych z notyfikacji do aplikacji i przekazanie ich do modułu PWA.	Do 13/05/2020	
	Wdrożenie powiadomień PUSH w aplikacji iOS	Obsługa kilku typów powiadomień FCM, wyświetlanie odpowiednich notyfikacji (UI), wstrzykiwanie danych z notyfikacji do aplikacji i przekazanie ich do modułu PWA.	Do 13/05/2020	
Komunikacja PWA i native	Opracowanie komunikacji pomiędzy kodem natywnym i modułem PWA dla modułu contact tracing.	Opracowanie i dokumentacja metod i modeli danych dla JS Bridge'a do komunikacji pomiędzy natywnym kodem aplikacji a modułem PWA dla modułu contact tracing.	Do 13/05/2020	335 000 PLN
	Wdrożenie komunikacji pomiędzy natywnym kodem i modułem PWA dla modułu contact tracing w aplikacji Android.	Implementacja JS bridge'a dla modułu contact tracing w aplikacji Android.	Do 13/05/2020	
	Wdrożenie komunikacji pomiędzy natywnym kodem i modułem PWA	Implementacja JS bridge'a dla modułu contact tracing w aplikacji iOS.	Do 13/05/2020	

	dla modułu contact tracing w aplikacji iOS.		
Publikacja aplikacji	Publikacja aplikacji Android w sklepie Google Play.	Przygotowanie wersji release 3.1 aplikacji, wdrożenie wersji produkcyjnej do sklepu, obsługa releasów wersji pośrednich (z poprawkami błędów i nowymi zmianami).	Do 13/05/2020
Backend	Publikacja aplikacji iOS w sklepie Apple App Store.	Przygotowanie wersji release 3.1 aplikacji, wdrożenie wersji produkcyjnej do sklepu, obsługa releasów wersji pośrednich (z poprawkami błędów i nowymi zmianami).	Do 13/05/2020
		Ukrycie w kroku rejestracji podania numeru telefonu .	Do 13/05/2020
		Dodanie funkcjonalności zmiany danych w metryczce	Do 13/05/2020
		Przerobienie widoku dziennika zdrowia - lista	Do 13/05/2020
		Dodanie ekranu Porady i dodanie ikony w menu	Do 13/05/2020
		Wysłanie informacji do native app po uzupełnionym teście	Do 13/05/2020
		Przerobienie widoku bocznego menu	Do 13/05/2020
		Wysyłka push notifications przez firebase	Do 13/05/2020
Stworzenie dokumentacji		Dokumentacja developerska projektu PWA - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 13/05/2020
Zarządzanie repozytorium		Ustrukturyzowanie i uporządkowanie	Do 13/05/2020

GitHub		repozytorium Aplikacji w serwisie GitHub, która umożliwi zapewnienie transparentności prac nad Aplikacją.		
Usunięcie starych widoków z aplikacji		Usuwamy stare widoki PWA, które powinny być już w aplikacji, np. kroki instalacji PWA.	Do 13/05/2020	
Przerobienie prawego menu		Przeróbka zgodnie z nowymi ikonami i kolorami	Do 13/05/2020	
Stworzenie dokumentacji		Dokumentacja developerska projektu PWA - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 13/05/2020	
Wyczyszczenie repozytorium	dodajemy plik licencji synchronizujemy release/3.1 z masterem	Ustrukturyzowanie i uporządkowanie repozytorium Aplikacji w serwisie GitHub, która umożliwi zapewnienie transparentności prac nad Aplikacją.	Do 13/05/2020	
Bug Bash 3.1	Przeprowadzenie zbiorowych testów eksploracyjnych aplikacji w wersji 3.1		Do 13/05/2020	

2.5 Etap 5 – wersja aplikacji 3.3

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena

Stworzenie dokumentacji		Dokumentacja developerska projektu - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 22/05/2020	
Zarządzanie repozytorium GitHub	dodajemy plik licencji synchronizacja release/3.2.0 z masterem	Ustrukturyzowanie i uporządkowanie repozytorium Aplikacji w serwisie Github, która umożliwi zapewnienie transparentności prac nad Aplikacją.	Do 22/05/2020	
Moduł automatyzacji aktualizacji wybranych treści w Aplikacji		Automatyzacja przepływu części informacji w Aplikacji. Synchronizacja danych z pacjent.gov.pl; synchronizacja danych z pytań i odpowiedzi dot. COVID-19 z portalu gov.pl; synchronizacja szpitali zakaźnych; synchronizacja i rozwój porad dla Użytkowników.	Do 22/05/2020	140 000 PLN

2.6 Etap 6 - testy manualne i maszynowe

Nazwa zadania	**Zakres techniczny**	**Opis funkcjonalny**	**Data wykonania**	**Wycena**
Testowanie zadań	Testowanie zadań wykonanych przez zespół deweloperski		Do 04/05/2020	
Wstępna analiza rynku	Zidentyfikowanie urządzeń niezbędnych do pokrycia testami interfejsu użytkownika		Do 04/05/2020	
Przeprowadzenie bug bash	- Przeprowadzenie zbiorowych testów eksploracyjnych aplikacji w wersji 2.0 - Skonfigurowanie narzędzia do zarządzania		Do 04/05/2020	120 000 PLN

	zgłoszeniami od zewnętrznych testerów z bug bash	
Dokumentacja testowa	Przygotowanie macierzy urządzeń	Do 04/05/2020
Testy eksploracyjne i zdrowotne	Testy eksploracyjne i zdrowotne aplikacji PWA, Android i iOS	Do 04/05/2020
Automatyczna weryfikacja dymna	Przeprowadzenie testów kompatybilności z urządzeniami i wersjami platform o najwyższym priorytecie poprzez uruchomienie testów dymnych z wykorzystaniem narzędzi typu Crawler	Do 04/05/2020
Monitoring środowisk	Skonfigurowanie narzędzia do monitorowania stanu środowiska produkcyjnego i przedwdrożeniowego	Do 04/05/2020
Automatyczna weryfikacja	Skrypt weryfikujący poprawność działania podstawowej ścieżki w aplikacji PWA	Do 04/05/2020
Testowanie zadań	Testowanie zadań wykonanych przez zespół deweloperski	Do 04/05/2020
Analiza rynku urządzeń mobilnych	- Analiza dostępnych raportów odnośnie urządzeń mobilnych - Zidentyfikowanie najpopularniejszych urządzeń na rynku	Do 04/05/2020
Dokumentacja testowa	Stworzenie planu testów	Do 04/05/2020
QA Notes	Stworzenie dokumentacji technicznej procesu testowego, w skład której wchodzą narzędzia, opisy procesów i wszystkie niezbędne informacje dla osób powiązanych z procesem QA	Do 04/05/2020

2.7 Etap 7 – Testy cyberbezpieczeństwa

Etap 7 – Testy cyberbezpieczeństwa

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Infrastruktura i Security	Weryfikacja bezpieczeństwa: - logiki aplikacji - logiki komunikacji aplikacji z pozostałymi rozwiązaniami - rozwiązania infrastrukturalnego - kodu źródłowego aplikacji		Do 25.05.2020	100 000 PLN
Testy bezpieczeństwa – pierwszy podmiot o potwierdzonej, renomowanej rynkowo opinii z zakresu testów bezpieczeństwa	1. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej Android 2. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej iOS 3. Przeprowadzenie testów bezpieczeństwa aplikacji WEB 4. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend Firebase wraz z analizą hostingu. 5. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend OP-BACKEND wraz z analizą hostingu.			
	6. Przeprowadzenie testów bezpieczeństwa komunikacji pomiędzy elementami systemu		Do 25.05.2020	70 000 PLN
Testy bezpieczeństwa – drugi podmiot o potwierdzonej, renomowanej rynkowo opinii z zakresu testów bezpieczeństwa	1. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej Android 2. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej		Do 25.05.2020	70 000 PLN

	iOS 3. Przeprowadzenie testów bezpieczeństwa aplikacji WEB 4. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend Firebase wraz z analizą hostingu. 5. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend OP-BACKEND wraz z analizą hostingu. 6. Przeprowadzenie testów bezpieczeństwa komunikacji pomiędzy elementami systemu		

2.8 Etap 8 – Komunikacja Aplikacji

Etap 8 – Komunikacja Aplikacji

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Stworzenie logo	- 1 propozycje logotypu wraz z uzasadnieniem (dla NZOZ) - 1 propozycje logotypu wraz z uzasadnieniem (dla JO Medical Writing) - Uzasadnienie wyboru - Wybór ostatecznej wersji - 1 cykl poprawek - Przekazanie logo pack z logotypem w krzywych oraz formatach .jpg i .png - księga znaku: wymiarowanie, typografia,		Do 27.04.2020	20 000 PLN

	kolorystyka, zastosowania		
Stworzenie KeyVisual	Zaproponowanie wersji wiodącej Key Visual 1 cykl poprawek do wersji ostatecznej KV Przekazanie elementów składowych/grafik w krzywych oraz formatach .jpg i .png Key Visual to graficzny motyw przewodni nawiązujący do logotypu, możliwy do powielania we wszystkich materiałach wizerunkowych marki. W ramach KV opracujemy: projekt baneru ADS x2 (pion i poziom) projekt grafiki social media x4 projekt baneru Google Ads x6	Do 27.04.2020	30 000 PLN
Stworzenie grafik marketingowych	10 grafik w formatach .png i .jpg	Do 27.04.2020	10 000 PLN
Stworzenie diagramu przepływu danych w module OpenTrace	Export w pliku formatu .jpg	Do 27.04.2020	20 000 PLN
Obsługa komunikacji w sklepach z aplikacjami (Google Play Store oraz Apple App Store)	Obsługa komentarzy w sklepach z aplikacjami Google Play Store oraz Apple App Store, polegająca na analizowaniu i odpowiadaniu na komentarze, a także przekazywaniu komentarzy do zespołu Wykonawcy odpowiadającego za naprawę błędów lub wprowadzanie nowych funkcjonalności.	Do 30.06.2020	15 000 PLN

2.9 Etap 9 – Przygotowanie raportu implementacji API Google w Aplikacji

Etap 9 – Przygotowanie raportu implementacji API Google w Aplikacji

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Analiza dokumentacji API Google contact tracing wraz z przygotowaniem raportu z tej analizy	Wykonawca przeanalizuje dokumentację API Google contact tracing wydane przez Google LLC z siedzibą w 1600 Amphitheatre Parkway, Mountain View, Kalifornia, Stany Zjednoczone Ameryki, a następnie przygotuje raport implementacji API Google contact tracing w Aplikacji. Raport, o którym mowa w zdaniu poprzedzającym zostanie sporządzony w terminie 14 dni od opublikowania przez Google kompletnej dokumentacji dotyczącej API Google contact tracing. Raport, o którym mowa w zdaniu pierwszym niniejszego punktu będzie zawierał w szczególności opis środowiska API Google, możliwości implementacji API Google contact tracing w Aplikacji, a także harmonogram oraz koszt takiej implementacji.		Do 14 dni od opublikowania stosownej dokumentacji przez Google LLC	20 000 PLN

3. Testy

Zamawiający oczekuje przeprowadzenia i dokumentowania testów akceptacyjnych (UAT), bezpieczeństwa oraz wydajności (obciążeniowych) każdej przekazanej wersji Aplikacji od wersji 3.1 włącznie.

Testy akceptacyjne Aplikacji zostaną przeprowadzone w formie weryfikacji zgodności nowych funkcjonalności z Dokumentacją.

Udostępnienie Aplikacji od wersji 3.1 włącznie na środowisku produkcyjnym uwarunkowane jest pozytywnym przebiegiem testów Wykonawcy na środowisku testowym.

Zamawiający zobowiązuje się do udostępnienia rozwiązania do testów na 12 godzin przed planowanym produkcyjnym uruchomieniem Aplikacji.

3.1. Testy manualne i maszynowe

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Testowanie zadań	Testowanie zadań wykonanych przez zespół deweloperski		Do 04/05/2020	
Wstępna analiza rynku	Zidentyfikowanie urządzeń niezbędnych do pokrycia testami interfejsu użytkownika		Do 04/05/2020	
Przeprowadzenie bug bash	- Przeprowadzenie zbiorowych testów eksploracyjnych aplikacji w wersji 2.0 - Skonfigurowanie narzędzia do zarządzania zgłoszeniami od zewnętrznych testerów z bug bash		Do 04/05/2020	
Dokumentacja testowa	Przygotowanie macierzy urządzeń		Do 04/05/2020	
Testy eksploracyjne i zdrowotne	Testy eksploracyjne i zdrowotne aplikacji PWA, Android i iOS		Do 04/05/2020	
Automatyczna weryfikacja dymna	Przeprowadzenie testów kompatybilności z urządzeniami i wersjami platform o najwyższym priorytecie poprzez uruchomienie testów dymnych z wykorzystaniem narzędzi typu Crawler		Do 04/05/2020	
Monitoring środowisk	Skonfigurowanie narzędzia do monitorowania stanu środowiska produkcyjnego i przedwdrożeniowego		Do 04/05/2020	
Automatyczna weryfikacja	Skrypt weryfikujący poprawność działania podstawowej ścieżki w aplikacji PWA		Do 04/05/2020	
Testowanie zadań	Testowanie zadań wykonanych przez zespół deweloperski		Do 04/05/2020	120 000 PLN
Analiza rynku	- Analiza dostępnych raportów odnośnie		Do	

urządzeń mobilnych	urządzeń mobilnych - Zidentyfikowanie najpopularniejszych urządzeń na rynku	04/05/2020	
Dokumentacja testowa	Stworzenie planu testów	Do 04/05/2020	
QA Notes	Stworzenie dokumentacji technicznej procesu testowego, w skład której wchodzą narzędzia, opisy procesów i wszystkie niezbędne informacje dla osób powiązanych z procesem QA	Do 04/05/2020	

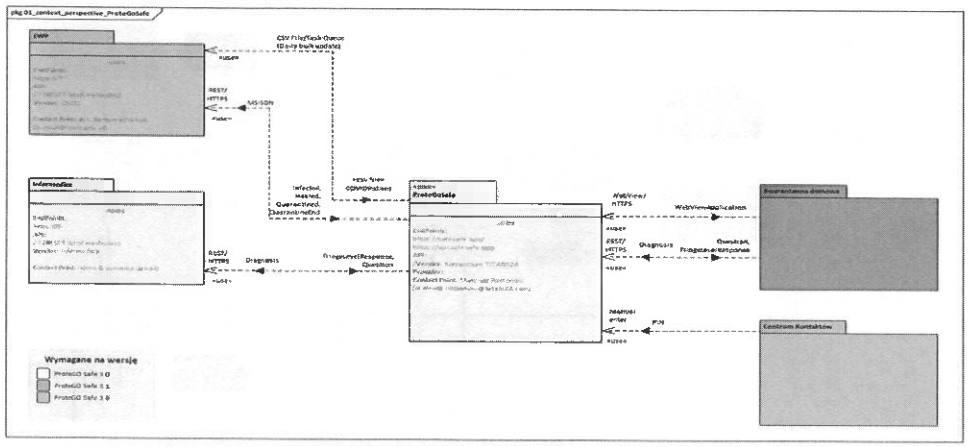
3.2. Testy cyberbezpieczeństwa

Nazwa zadania	**Zakres techniczny**	**Opis funkcjonalny**	**Data wykonania**	**Wycena**
Infrastruktura i Security	Weryfikacja bezpieczeństwa: - logiki aplikacji - logiki komunikacji aplikacji z pozostałymi rozwiązaniami - rozwiązania infrastrukturalnego - kodu źródłowego aplikacji		Do 25.05.2020	100 000 PLN
Testy bezpieczeństwa – pierwszy podmiot o potwierdzonej, renomowanej rynkowo opinii z zakresu testów bezpieczeństwa	1. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej Android 2. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej iOS 3. Przeprowadzenie testów bezpieczeństwa aplikacji WEB 4. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend Firebase wraz z analizą hostingu.		Do 25.05.2020	70 000 PLN

	5. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend OP-BACKEND wraz z analizą hostingu. 6. Przeprowadzenie testów bezpieczeństwa komunikacji pomiędzy elementami systemu		
	1. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej Android 2. Przeprowadzenie testów bezpieczeństwa aplikacji natywnej iOS 3. Przeprowadzenie testów bezpieczeństwa aplikacji WEB 4. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend Firebase wraz z analizą hostingu.		
Testy bezpieczeństwa – drugi podmiot o potwierdzonej, renomowanej rynkowo opinii z zakresu testów bezpieczeństwa	5. Przeprowadzenie testów bezpieczeństwa konfiguracji środowiska backend OP-BACKEND wraz z analizą hostingu. 6. Przeprowadzenie testów bezpieczeństwa komunikacji pomiędzy elementami systemu	Do 25.05.2020	70 000 PLN

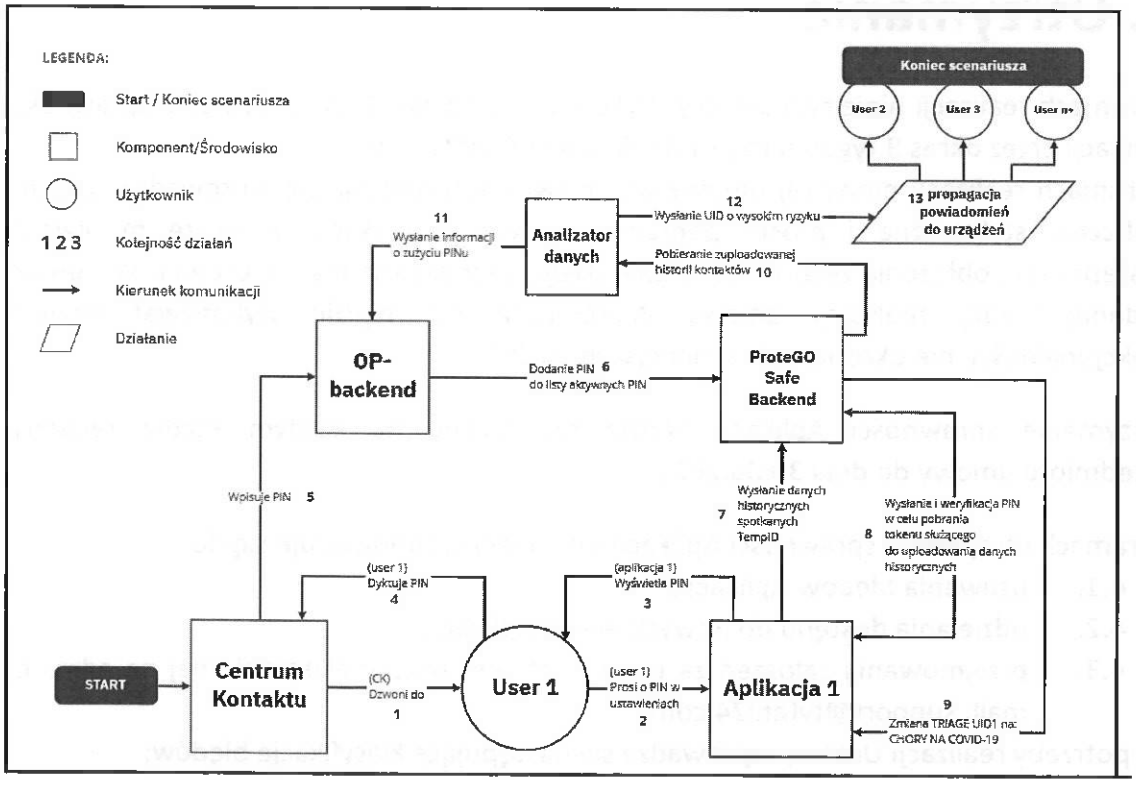
4. Architektura rozwiązania

Poniższy diagram prezentuje najważniejsze obszary z jakimi styka się planowane rozwiązanie (ProteGO Safe).



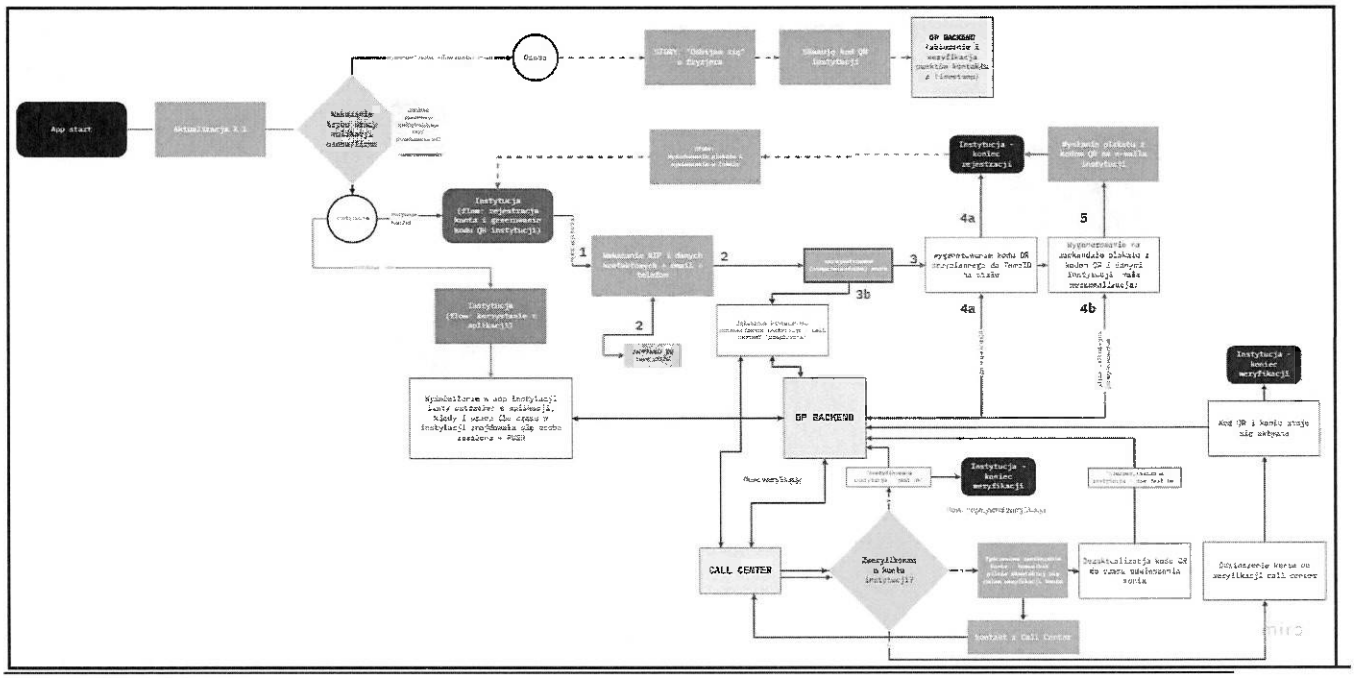
Rysunek 1. Otoczenie rozwiązania, wraz z głównymi przepływami.

Poniższy diagram prezentuje schemat działania modułu Bluetooth opartego o OpenTrace



Rysunek 2. Logika funkcjonowania modułu Bluetooth

Poniższy diagram prezentuje schemat działania modułu kodów QR w rozbiciu na Użytkownika Indywidualnego oraz Instytucje



Rysunek 3. Proces funkcjonalny modułu QR

5. Utrzymanie

1. W ramach realizacji niniejszej umowy Wykonawca odpowiada za utrzymanie sprawności Aplikacji przez okres 9 tygodni to jest do dnia 30.06.2020 roku.
2. W ramach realizacji niniejszej umowy wykonawca zobowiązuje się wprowadzać zmiany graficzne, stylistyczne i proste poprawki w stylach aplikacji, w miarę możliwości dostępności i obłożenia zespołu developerskiego zaangażowanego w projekt. W ramach podanej kwoty realizacji umowy Wykonawca nie będzie wykonywał nowych funkcjonalności, nie określonych w niniejszym SOPU.

3. Utrzymanie sprawności Aplikacji będzie świadczone na każdym etapie realizacji przedmiotu umowy do dnia 30.06.2020 r.

4. W ramach utrzymania sprawności Aplikacji Wykonawca zobowiązuje się do:
   - 4.1. usuwania błędów Aplikacji;
   - 4.2. udzielania dostępu do nowych wersji Aplikacji;
   - 4.3. przyjmowania zgłoszeń za pośrednictwem poczty elektronicznej na adres e-mail: support@tytani24.com.
5. Na potrzeby realizacji Umowy wprowadza się następujące klasyfikacje błędów:
   - 5.1. błąd krytyczny - zdarzenie uniemożliwiające poprawne lub całkowite wykonanie operacji w Aplikacji przez ponad 20% aktywnych użytkowników lub

całkowity brak dostępu do lub utrata danych znajdujących się w bazie danych serwera Aplikacji;

5.2. błąd wydajności - zdarzenie utrudniające wykonanie danej operacji w Aplikacji, tj. operację można wykonać poprawnie, ale w sposób o 30% mniej efektywny niż w trakcie „normalnego działania" Aplikacji;

5.3. błąd wyglądu - zdarzenie pogorszenia estetyki i spójności interfejsu graficznego Aplikacji.

6. Zgłoszenie, o którym mowa powyżej, powinno zawierać takie informacje jak: Szczegółowy opis błędu obejmujący "zachowanie" Aplikacji; Dokładny model urządzenia rodzaj i wersję systemu operacyjnego; rodzaj i wersję przeglądarki; Dokładnie opisane okoliczności wystąpienia błędu; Dokładny czas wykrycia błędu; Dane kontaktowe osoby zgłaszającej Awarię; Informację o potencjalnym naruszeniu ochrony danych osobowych.

7. Wykonawca zobowiązuje się podjąć prace nad rozwiązaniem błędu:

7.1. Czas reakcji na zgłoszenie:

a) Błąd krytyczny – czas reakcji na zgłoszenie od momentu potwierdzenia przyjęcia zgłoszenia: do 2h w Dni Robocze, do 4h w pozostałych porach i w dni wolne od pracy;

b) Każdy inny błąd – czas reakcji na zgłoszenie od momentu potwierdzenia przyjęcia: do 24 h.

7.2 Czas rozwiązania problemu:

a) Błąd krytyczny – czas reakcji na zgłoszenie od momentu przyjęcia do 8h w Dni Robocze, do 16h w pozostałych porach i w dni wolne od pracy;

b) Każdy inny błąd – czas reakcji na zgłoszenie od momentu przyjęcia do 5 ni Roboczych

8. Korespondencja elektroniczna będzie odbierana przez Wykonawcę 24 godziny na dobę przez 7 dni w tygodniu.

9. Jeżeli usunięcie błędu nie będzie możliwe w założonym czasie, Wykonawca niezwłocznie poinformuje o tym fakcie Zamawiającego.

10. Wykonawca zobowiązuje się do wykonywania zgłoszeń Zamawiającego z należytą starannością oraz z priorytetem pierwszeństwa.

11. Zobowiązania Wykonawcy nie obejmują błędów wynikających ze współpracy Aplikacji z innymi połączonymi systemami nie będącymi w utrzymaniu Wykonawcy.

12. Zamawiający zobowiązuje się do współpracy z Wykonawcą przy diagnozowaniu błędów i udzielenia wszelkich niezbędnych informacji, w terminie nie dłuższym niż dzień roboczy w przypadku Błędów Krytycznych, a w przypadku każdego innego błędu w terminie nie dłuższym niż 3 dni robocze.

13. Zgłoszenie błędów dotyczy wyłącznie aktualnej wersji Aplikacji aktualnie udostępnionej przez Wykonawcę.

6. Gwarancja

1. Wykonawca gwarantuje Zamawiającemu, że w okresie 3 miesięcy od dnia podpisania protokołu odbioru bez błędów krytycznych i wydajnościowych , wdrożona przez niego wersja Aplikacji będzie sprawnie i bez zakłóceń wykonywała funkcje określone w niniejszym załączniku do Umowy.
2. Pod pojęciem „błędów" Aplikacji, Strony rozumieją nieprawidłowość, która powoduje, iż cała Aplikacja i/ lub jej część nie działa, lub działa w sposób inny niż wynikający z treści Umowy, lub w sposób nieprawidłowy działa jej podstawowa funkcjonalność (tworzenie i przypisywanie zadań do użytkowników, odbiór i zapis danych z Aplikacji, dostęp do udzielonych odpowiedzi), przy czym nieprawidłowość ta wynika z przyczyn leżących po stronie Aplikacji, a nie z błędów konfiguracyjnych w Aplikacji lub problemów z urządzeniem końcowym użytkownika.
3. Strony ustalają następującą kategorie błędów:
   a) błąd krytyczny - zdarzenie uniemożliwiające poprawne lub całkowite wykonanie operacji w Aplikacji przez ponad 20% aktywnych użytkowników lub całkowity brak dostępu do lub utrata danych znajdujących się w bazie danych serwera Aplikacji;
   b) błąd wydajności - zdarzenie utrudniające wykonanie danej operacji w Aplikacji, tj. operację można wykonać poprawnie, ale w sposób o 30% mniej efektywny niż w trakcie „normalnego działania" Aplikacji;
   c) błąd wyglądu - zdarzenie pogorszenia estetyki i spójności interfejsu graficznego Aplikacji.
4. Zgłoszenia błędów dokonywane są za pomocą poczty elektronicznej na adres e-mail: support@tytani24.com.
5. Zgłoszenie, o którym mowa powyżej, powinno zawierać takie informacje jak:

Szczegółowy opis błędu obejmujący "zachowanie" Aplikacji; Dokładny model urządzenia rodzaj i wersję systemu operacyjnego; rodzaj i wersję przeglądarki; Dokładnie opisane okoliczności wystąpienia błędu; Dokładny czas wykrycia błędu; Dane kontaktowe osoby zgłaszającej Awarię; Informację o potencjalnym naruszeniu ochrony danych osobowych.

6. Korespondencja elektroniczna będzie odbierana przez Wykonawcę 24 godziny na dobę przez 7 dni w tygodniu.
7. Wykonawca zobowiązuje się podjąć prace nad rozwiązaniem błędu:
   7.1 Czas reakcji na zgłoszenie:
   a) Błąd krytyczny – czas reakcji na zgłoszenie od momentu potwierdzenia przyjęcia zgłoszenia: do 2h w Dni Robocze, do 4h w pozostałych porach i w dni wolne od pracy;
   b) Każdy inny błąd – czas reakcji na zgłoszenie od momentu potwierdzenia przyjęcia: do 24 h.
   7.2 Czas rozwiązania problemu:

a) Błąd krytyczny – czas reakcji na zgłoszenie od momentu przyjęcia do 8h w Dni Robocze, do 16h w pozostałych porach i w dni wolne od pracy;

b) Każdy inny błąd – czas reakcji na zgłoszenie od momentu przyjęcia do 5 dni roboczych

8. Jeżeli usunięcie błędu nie będzie możliwe w założonym czasie, Wykonawca niezwłocznie poinformuje o tym fakcie Zamawiającego.
9. Wykonawca zobowiązuje się do wykonywania zgłoszeń Zamawiającego z należytą starannością oraz z priorytetem pierwszeństwa.

Załącznik nr 4 do Umowy

PROCEDURA ODBIORU PRAC

I. ODBIÓR APLIKACJI

1. Wykonawca opracuje i dostarczy Zamawiającemu Aplikację, w formie wskazanej w SOPU do przeprowadzenia testów.
2. Zamawiający przeprowadzi testy wykonanych prac na podstawie uzgodnionych scenariuszy w terminach określonych w SOPU.
3. Zamawiającemu przysługuje prawo zgłoszenia uwag do przedmiotu odbioru.
4. W przypadku zgłoszenia uwag przez Zamawiającego Wykonawca uwzględnia uwagi i zastrzeżenia Zamawiającego. Przekaże Zamawiającemu ostateczną wersję Aplikacji w terminie 1 dnia roboczego. Procedura zgłaszania uwag może być powtarzana do momentu uzyskania najkorzystniejszego rozwiązania jednak nie więcej niż w czterech cyklach poprawek.
5. Po uzgodnieniu lub rozstrzygnięciu uwag Strony podpiszą Protokół Odbioru lub Protokół Odbioru Warunkowego.
6. Strony mogą dokonać odbioru warunkowego prac, w przypadku:
    1) braku możliwości osiągnięcia rezultatów z przyczyn nieleżących po stronie Wykonawcy;
    2) stwierdzenia nieistotnych wad prac wykonanych w ramach SOPU
7. W przypadkach, o których mowa w ust. 6, Strony podpiszą Protokół Odbioru Warunkowego, którego wzór stanowi Załącznik nr 2 do Umowy, sporządzony w formie pisemnej w 4 egzemplarzach, po dwa dla każdej Strony lub w formie elektronicznej.
8. Załącznikiem do Protokołu Odbioru Warunkowego, w przypadku określonym w ust. 7 pkt 2, jest opis wad nieistotnych zidentyfikowanych w ramach procedury odbioru. Usunięcie wad nastąpi w terminie i na zasadach uzgodnionych w Protokole Odbioru Warunkowego. Zamawiający potwierdzi pisemnie usunięcie wad lub wskaże wady, które w ocenie Zamawiającego nie zostały usunięte. Brak stanowiska Zamawiającego w terminie wskazanym w Protokole Odbioru Warunkowego będzie równoznaczny z potwierdzeniem usunięcia wad i ostateczną akceptacją prac wykonanych w ramach SOPU. Na potwierdzenie usunięcia wad Strony podpiszą Protokół Odbioru.

9. Potwierdzeniem wykonania prac lub poszczególnych etapów, jest podpisany przez upoważnionych przedstawicieli Stron Protokół Odbioru, którego wzór stanowi Załącznik nr 1, sporządzony w formie pisemnej w 4 egzemplarzach, po dwa dla każdej Strony lub w formie elektrycznie.
10. W przypadku nieprzystąpienia przez Zamawiającego do odbioru Aplikacji w terminie do 1 dnia roboczego, uznaje się, że Zamawiający nie zgłasza uwag lub zastrzeżeń do Prac, a Wykonawca wystawia jednostronny Protokół Odbioru, który stanowi podstawę do wypłaty wynagrodzenia.
11. Termin realizacji prac przedłuża się o okresy zwłoki po stronie Zamawiającego w dokonywaniu czynności wskazanych w SOPU, w stosunku do terminów określonych w SOPU na ich dokonanie przez Zamawiającego.

Załącznik nr 5 do Umowy

UMOWA O DALSZYM POWIERZENIU PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Warszawie pomiędzy:

Ministrem Cyfryzacji z siedzibą w Warszawie pod adresem ul. Królewska 27, 00-060 Warszawa, zwanym dalej **„Podmiotem powierzający "**, reprezentowanym przez:

Pana Tomasza Napiórkowskiego – Dyrektora Departamentu Rozwoju Usług

a

TYTANI24 Spółka z ograniczoną odpowiedzialnością z siedzibą we Wrocławiu, ul. Ząbkowicka 55, 50 – 511 Wrocław (adres biura: ul. Kościerzyńska 32A, Wrocław, 51 – 410), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000725465, REGON 369879064, NIP 8992843182, o kapitale zakładowym opłaconym w całości w wysokości 20 000,00 zł, reprezentowaną przez:

Pana Mateusza Romanowa - Prezesa zarządu

zwanym dalej: **„Podmiotem przetwarzającym"**,

Podmiot powierzający i Podmiot przetwarzający są zwani dalej łącznie **„Stronami"**, a każdy
z nich z osobna **„Stroną"**,

ZWANE DALEJ: **„UMOWĄ O POWIERZENIU"**.

§ 1

PRZEDMIOT UMOWY O POWIERZENIU

1. **Na podstawie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, s. 1, z późn. zm.), zwanego dalej „RODO", Podmiot powierzający powierza Podmiotowi przetwarzającemu do przetwarzania dane osobowe określone w Załączniku 1 do Umowy o powierzeniu („Dane osobowe"). Podmiot przetwarzający oświadcza, że dysponuje środkami, doświadczeniem, wiedzą i wykwalifikowanym personelem, co umożliwi mu prawidłową realizację postanowień Umowy o powierzeniu, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie Danych osobowych, z zachowaniem odpowiedniego poziomu bezpieczeństwa.**
2. **Umowa o powierzeniu zostaje zawarte w związku i w celu wykonania zawartego pomiędzy Głównym Inspektorem Sanitarnym a Podmiotem powierzającym**

porozumienia z dnia 24 kwietnia 2020 r. zwanej dalej „Umową główną" oraz w celu świadczenia przez Podmiot przetwarzający na rzecz Podmiotu powierzającego usługi utrzymania oraz usługi wsparcia technicznego, tj. obsługi błędów aplikacji mobilnej ProteGO na urządzenia mobilne przeznaczone do przeciwdziałania zakażeniom choroby zakaźnej COVID-19.

3. **Podmiot przetwarzający przetwarza Dane osobowe wyłącznie w celu realizacji Umowy głównej i w zakresie niezbędnym do jej wykonania oraz w czasie jej obowiązywania.**
4. **Przetwarzanie danych osobowych w związku z celami określonymi w ust. 2 podlega przepisom RODO. Podmiot przetwarzający zobowiązany jest przetwarzać dane osobowe zgodnie z RODO, innymi obowiązującymi przepisami prawa oraz Umową o powierzeniu.**
5. **Zakres powierzenia, wskazany w Załączniku nr 1 do Umowy o powierzeniu, może zostać w każdym momencie rozszerzony lub ograniczony przez Podmiot powierzający. Ograniczenie lub rozszerzenie może być dokonane poprzez przesłanie przez Administratora danych do Podmiotu przetwarzającego nowej wersji w Załącznika nr 1 do Umowy o powierzeniu za pośrednictwem poczty elektronicznej (na adres e-mail wskazany w § 4). W przypadku braku reakcji Podmiotu przetwarzającego w ciągu 3 Dni Roboczych (na potrzeby Umowy „Dni Robocze" należy rozumieć dni od poniedziałku do piątku, poza dniami ustawowo wolnymi od pracy w Polsce) od daty wysłania wiadomości przez Administratora danych przyjmuje się, że Podmiot przetwarzający zaakceptował zmianę zakresu powierzenia.**

§ 2
OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO

1. PRZETWARZANIE DANYCH OSOBOWYCH ODBYWAĆ SIĘ BĘDZIE WYŁĄCZNIE W CZASIE OBOWIĄZYWANIA UMOWY GŁÓWNEJ ORAZ WYŁĄCZNIE NA UDOKUMENTOWANE POLECENIE PODMIOTU POWIERZAJĄCEGO, CHYBA ŻE OBOWIĄZEK TAKI NAKŁADAJĄ NA PODMIOT PRZETWARZAJĄCY PRZEPISY PRAWA KRAJOWEGO LUB UNIJNEGO. W SYTUACJI, GDY OBOWIĄZEK PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ PODMIOT PRZETWARZAJĄCY WYNIKA Z PRZEPISÓW PRAWA, INFORMUJE ON O TYM OBOWIĄZKU PRAWNYM ADMINISTRATORA DANYCH, PRZED ROZPOCZĘCIEM PRZETWARZANIA.
2. PODMIOT PRZETWARZAJĄCY BĘDZIE PRZETWARZAŁ POWIERZONE DANE OSOBOWE W MIEJSCU WSKAZANYM W ZAŁĄCZNIKU 1.
3. Podmiot przetwarzający zobowiązuje się do niewykorzystywania powierzonych danych osobowych w celach innych niż określone w Umowie głównej i Umowie o powierzeniu oraz przetwarzania ich wyłącznie w miejscu, o którym mowa w ust. 2.
4. PODMIOT PRZETWARZAJĄCY, NA PODSTAWIE ART. 28 RODO, ZOBOWIĄZUJE SIĘ:
   1) w uzgodnieniu z Podmiotem powierzającym wdrożyć adekwatne środki techniczne i organizacyjne, aby przetwarzanie danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, w tym między innymi środki techniczne i organizacyjne, zapewniające bezpieczeństwo przetwarzania danych, o których mowa w art. 32 RODO;

2) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagać Podmiotowi powierzającemu w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO, w szczególności w zakresie wdrożenia oraz stosowania środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych, dokonywania zgłoszeń naruszeń ochrony danych osobowych, przekazywania informacji o tych naruszeniach oraz wszelkich informacji niezbędnych do przeprowadzenia oceny skutków dla ochrony danych osobowych;
3) wspierać Administratora danych oraz Podmiot powierzający w realizacji obowiązków odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;
4) prowadzić w formie pisemnej, w tym w elektronicznej, rejestr kategorii czynności przetwarzania danych osobowych w zakresie wynikającym z przedmiotu Umowy o przetwarzaniu i udostępniać go na żądanie Administratora danych lub Podmiotu powierzającego;
5) umożliwić Administratorowi danych lub Podmiotu powierzającego; lub ich uprawnionym przedstawicielom przeprowadzenie audytu, kontroli w zakresie prawidłowości przetwarzania powierzonych danych osobowych oraz spełnienia zasad ochrony; w tym udzielać wszelkich informacji niezbędnych do jego przeprowadzenia;
6) stosować się do ewentualnych wskazówek lub zaleceń dotyczących przetwarzania danych osobowych, wydanych przez organ nadzorczy lub unijny organ doradczy zajmujący się ochroną danych osobowych.

5. Podmiot przetwarzający zobowiązuje się do:
   1) ograniczenia dostępu do powierzonych do przetwarzania danych osobowych, wyłącznie do pracowników posiadających imienne upoważnienie do przetwarzania danych osobowych, o których mowa w art. 29 RODO, wydanych przez Podmiot przetwarzający, oraz na żądanie, udostępniania Administratorowi danych aktualnego wykazu wystawionych upoważnień;
   2) stałego nadzorowania pracowników, w zakresie zabezpieczenia powierzonych do przetwarzania danych osobowych;
   3) zobowiązania pracowników do zachowania powierzonych do przetwarzania danych osobowych i sposobów ich zabezpieczenia w tajemnicy, o której mowa w art. 28 ust. 3 pkt b RODO, także po ustaniu zatrudnienia lub ustaniu stosunku cywilnoprawnego albo odwołaniu upoważnienia.
6. Podmiotu powierzającego; na podstawie postanowień Umowy o powierzeniu umocowuje Podmiot przetwarzający do wydawania i odwoływania swoim pracownikom upoważnień do przetwarzania danych osobowych. Upoważnienia do przetwarzania danych osobowych wydawane są na własnych wzorach Podmiotu przetwarzającego.
7. PODMIOT PRZETWARZAJĄCY ZOBOWIĄZANY JEST DO DOKUMENTOWANIA WSZELKICH NARUSZEŃ OCHRONY POWIERZONYCH DANYCH OSOBOWYCH ORAZ PODEJMOWANIA WSZELKICH ROZSĄDNYCH DZIAŁAŃ MAJĄCYCH NA CELU OGRANICZENIE ORAZ USUNIĘCIE SKUTKÓW TYCH NARUSZEŃ.

8. Podmiot przetwarzający zobowiązany jest do niezwłocznego informowania Administratora danych oraz lub Podmiotu powierzającego;:
   1) przypadkach naruszenia ochrony danych osobowych lub o ich niewłaściwym użyciu – na adres e-mail: iod@mc.gov.pl i przedstawienia Podmiotowi powierzającemu następujących informacji:
      a) daty i godziny zaobserwowania zdarzenia po raz pierwszy,
      b) opisu zdarzenia,
      c) miejsca wystąpienia zdarzenia,
      d) liczby zdarzeń (jeżeli zdarzenie miało miejsce wielokrotnie),
      e) jakie działania zostały podjęte do momentu zgłoszenia (co zostało zrobione, komu przekazano informacje i jakie);
   2) czynnościach z własnym udziałem w sprawach dotyczących ochrony danych osobowych prowadzonych w szczególności przed organem nadzorczym, innymi uprawnionymi organami i podmiotami, policją lub przed sądami;
   3) wydanych mu poleceniach pracowników Podmiotu powierzającego, które w jego opinii, stanowią naruszenie przepisów RODO lub innych przepisów dotyczących ochrony danych osobowych.
9. Podmiot przetwarzający w zgłoszeniu naruszeń do Podmiotu powierzającego zobowiązany jest do przekazania wszelkich posiadanych informacji, o których mowa w art. 33 RODO. W przypadku gdy, w momencie zgłoszenia Podmiot przetwarzający nie posiada wszystkich informacji, ma obowiązek udzielać ich na bieżąco bez zbędnej zwłoki.
10. PODMIOT PRZETWARZAJĄCY OŚWIADCZA, IŻ ODPOWIADA ZA WSZELKIE WYRZĄDZONE OSOBOM TRZECIM SZKODY, KTÓRE POWSTAŁY WINY PODMIOTU PRZETWARZAJĄCEGO I W ZWIĄZKU Z NIENALEŻYTYM PRZETWARZANIEM POWIERZONYCH MU DANYCH OSOBOWYCH.
11. BEZ PISEMNEJ ZGODY PODMIOTU POWIERZAJĄCEGO PODMIOT PRZETWARZAJĄCY NIE MOŻE:
   1) ~~powierzać przetwarzania Danych osobowych innym podmiotom;~~
   2) przekazywać (transferować) powierzonych danych osobowych do państw trzecich lub organizacji międzynarodowych, znajdujących się poza Europejskim Obszarem Gospodarczym;
   3) informować osób, których dane dotyczą oraz organu nadzorczego, o naruszeniu ochrony danych osobowych.
12. Dalsze powierzenie przetwarzania powierzonych do przetwarzania Danych osobowych, w imieniu Podmiotu powierzającego, dokonuje się na warunkach określonych w zgodzie, o której mowa w ust. 11 pkt 1.
13. W przypadku dalszego powierzenia przez Podmiot przetwarzający danych osobowych innym podmiotom, zgoda, o której mowa w ust. 11 pkt 1, stanowi jednocześnie umocowanie wskazanego podmiotu do wydawania i odwoływania pracownikom tego podmiotu upoważnień do przetwarzania danych osobowych.
14. Dalsze powierzenie danych osobowych, o którym mowa w ust. 13, odbywa się na podstawie umowy lub innego instrumentu prawnego zawierającego zapisy zawarte w

niniejszym Umowie. W przypadku dalszego powierzenia Podmiot przetwarzający ponosi odpowiedzialność za działania podmiotu, któremu podpowierzył dane osobowe, jak za działania własne.

15. Podmiot przetwarzajacy, w uzgodnieniu z Podmiotem powierzającym, zobowiązany jest do protokolarnego usunięcia/zanonimizowania powierzonych Danych osobowych po zakończeniu realizacji Umów Głównych i Umowy o powierzeniu lub ustaniu celu przetwarzania Danych osobowych.
16. Po zrealizowaniu Umów Głównych i Umowy o podpowierzeniu bądź jego rozwiązaniu, Podmiot przetwarzający, na wezwanie Podmiotu powierzającego, jest zobowiązany do niezwłocznego przekazania Podmiotowi powierzającemu pisemnego oświadczenia, w którym potwierdzi, że nie posiada żadnych Danych osobowych, których przetwarzanie zostało mu powierzone na mocy Umów Głównych i Umowy o powierzeniu lub protokołu usunięcia/zanonimizowania powierzonych Danych osobowych, o którym mowa w ust. 15.
17. Podmiot przetwarzający zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO, a także chroniło prawa osób, których dane dotyczą. Podmiot przetwarzający zobowiązany jest zapewnić, by na dalsze podmioty przetwarzające zostały nałożone co najmniej te same obowiązki co nałożone na Podmiot przetwarzający w Umowie o przetwarzaniu. Podmiot przetwarzający zapewni, by dalsze podmioty przetwarzające zaprzestały przetwarzania powierzonych danych osobowych w każdym wypadku rozwiązania Umowy o powierzeniu, niezależnie od przyczyny.
18. Podmiot przetwarzający oświadcza, że dalszymi podmiotami podprzetwarzającymi będą podmioty, o których mowa w Załączniku 1. Podmiot przetwarzający udostępni Podmiotowi powierzającemu informacje niezbędne do wykonywania jego obowiązków związanych z powierzeniem przetwarzania Danych osobowych. Podmiot przetwarzający umożliwi Administratorowi danych lub Podmiotowi powierzającemu przeprowadzenie audytów, w tym inspekcji, w zakresie dotyczącym dalszego powierzenia przetwarzania Danych osobowych i zapewni współpracę w tym zakresie, co zostanie uprzednio uzgodnione przez odpowiednio zaangażowane Strony.

§ 4
WYMIANA INFORMACJI

1. STRONY WYZNACZAJĄ NASTĘPUJĄCE OSOBY UPOWAŻNIONE DO KONTAKTÓW W SPRAWACH ZWIĄZANYCH Z WYKONANIEM UMOWY O POWIERZENIU:
   1) ZE STRONY PODMIOTU POWIERZJĄCEGO:
   a)
   2) ze strony Podmiotu przetwarzającego:
   a)
   b) Mateusz Romanów, e-mail:

2. ZMIANA OSÓB LUB DANYCH, O KTÓRYCH MOWA W UST. 1, NIE JEST UWAŻANA ZA ZMIANĘ UMOWY O POWIERZENIU I NIE WYMAGA ZAWARCIA ANEKSU, JEDNAKŻE DLA SWEJ SKUTECZNOŚCI WYMAGA ZACHOWANIA FORMY PISEMNEJ.

§ 5
POSTANOWIENIA KOŃCOWE

1. **Podmiot powierzający powierza dane osobowe Podmiotowi przetwarzającemu do czasu wygaśnięcia lub rozwiązania Umów Głównych.**
2. **Umowa o powierzeniu może zostać wypowiedziana przez Podmiot powierzający ze skutkiem natychmiastowym w przypadku rażącego lub powtarzającego się naruszania Umowy o powierzeniu, wymagań RODO lub innych powszechnie obowiązujących przepisów prawa z zakresu ochrony danych osobowych przez Podmiot przetwarzający. Wypowiedzenie Umowy o powierzeniu wymaga formy pisemnej pod rygorem bezskuteczności.**
3. **Zmiany Umowy o powierzeniu są możliwe wyłącznie w formie pisemnej pod rygorem nieważności, z zastrzeżeniem sytuacji, w których Umowa o powierzeniu wprost przewiduje inną formę dokonywania zmian.**
4. Następujące załączniki do Umowy o powierzeniu stanowią jego integralną część:
   1) Załącznik nr 1 – zakres powierzenia danych osobowych;
   2) Załącznik nr 2 - Opis technicznych i organizacyjnych środków bezpieczeństwa.
5. Zmiana treści załączników do Umowy o powierzeniu nie wymaga zmiany Umowy o powierzeniu poprzez jego aneksowanie, jednak dla swej skuteczności wymaga uzyskania akceptacji drugiej Strony w formie pisemnej.
6. **Umowę o powierzeniu sporządzono w czterech jednobrzmiących egzemplarzach, po dwa dla każdej ze Stron.**
7. Traci moc umowa dalszego powierzenia przetwarzania zawarta pomiędzy stronami w dniu 17 kwietnia 2020 r.

Ze strony Podmiotu powierzającego:	Ze strony Podmiotu przetwarzającego:
Tomasz Napiórkowski Dyrektor Departamentu Rozwoju Usług W Ministerstwie Cyfryzacji /podpisano elektronicznie/	Mateusz Romanów Prezes Zarządu TYTANI24 Spółka z ograniczoną odpowiedzialnością /podpisano elektronicznie/

Załącznik nr 1 do Umowy - opis powierzonych czynności przetwarzania i zakres przetwarzanych danych"

I. Zakres przetwarzanych danych:

1. Dane które pozostają anonimowe:

1) **historia napotkanych Urządzeń z zainstalowaną aplikacją proteGO Safe**
2) **ogólne dane dotyczące zdrowia**: (zdiagnozowana przewlekła choroba płuc, zdiagnozowana niewydolność serca, trwająca choroba nowotworowa, choroby lub leki obniżające odporność, zdiagnozowana przewlekła choroba wątroby, zdiagnozowana przewlekła choroba nerek, długoterminowy pobyt w domu opieki,
3) **bieżące dane dotyczące stanu zdrowia:** (temperatura, czy występuje kaszel, czy występują duszności, osłabienie, bóle mięśni, dreszcze, ból głowy, biegunka, mdłości, ból gardła)
4) **dane wynikające z notatnika Aplikacji (Dziennik Zdrowia):** (mieszkam lub opiekowałem się, bez używania maseczki i rękawiczek, osobą z podejrzeniem zakażenia koronawirusem, przebywałem w tym samym pomieszczeniu (np. biuro, klasa, siłownia) lub podróżowałem w bliskiej odległości (1 metra) z osobą z podejrzeniem zakażenia koronawirusem, miałem osobisty kontakt przez dłużej niż 15 minut z osobą podejrzaną o zakażenie koronawirusem, inny rodzaj kontaktu, żadne z powyższych

2. Dane osobowe:

1) dane dotyczące urządzenia: identyfikator urządzenia, wersja systemu operacyjnego android/ios,
2) anonimowe dane statystyczne dostarczane przez serwis FireBase,
3) wersja aplikacji ProteGO Safe,
4) imię (nazwa),
5) płeć,
6) dane kontaktowe (w przypadku rozwiązywania błędów zgłoszonych przez użytkownika).

I. Opis czynności przetwarzania:

Opis czynności przetwarzania w wersji 2.0

1. Użytkownik instaluje aplikację na telefonie Android
2. Użytkownik otwiera aplikację i wyświetlają mu się informacje o sposobie jej działania i potrzebnych zgodach/uprawnieniach (akceptacja Regulaminu i Polityki Prywatności).
3. Użytkownik uzupełnia metrykę zdrowia.
4. Użytkownik wypełnia pierwszy Test Oceny Ryzyka (triaż)
5. Użytkownik dostaje pierwszy wynik klasyfikacji swojego stanu zdrowia (triaż)
6. Użytkownik odbiera 1x przez pierwszy tydzień (tj do 27.04.2020 włącznie - później do decyzji co dalej po stronie MC) notyfikacje push przypominające o potrzebie wypełnienia Testu Oceny Ryzyka.

7. Aplikacja prowadzi użytkownika przez porady i zachowania związane z jego stanem zdrowia na podstawie oceny ryzyka (triażu).
8. Użytkownik może wypełniać dowolną ilość razy dziennie: Test Oceny Ryzyka (triaż) i Dziennik Zdrowia.
9. Po trzech dniach, w których użytkownik przynajmniej raz dziennie wypełnił Test Oceny Ryzyka w aplikacji wyświetla się odznaka "Dbam o siebie i bliskich"

+ iOS

10. dla iOS - użytkownik musi wyrazić zgodę na "Pozwolenie na wysyłanie notyfikacji"

Opis czynności przetwarzania w wersji 3.0

11. Użytkownik pobiera aplikację ProteGO Safe 3.0 z modułem OpenTrace i nie ma w niej możliwości (i widoku) podania numeru telefonu (użytkownik nie podaje numeru telefonu w aplikacji - nie zbieramy tych danych w żaden sposób). Serwer Firebase przyznaje aplikacji (a nie numerowi telefonu) UID czyli zanonimizowany indywidualny numer danej instalacji (aplikacji).
12. Backend Firebase Google Authenticator ProteGO Safe zapisuje UID aplikacji - przez co jest w stanie komunikować się z aplikacją. Do każdego UID backend generuje TempID (zapisuje na urządzeniu tablicę z listą numerów TempID na 2 tygodnie do przodu, które aplikacja będzie cyklicznie, co 15 minut, zmieniała), które służą do anonimizacji użytkowników w module tracingowym (kontakt Bluetooth w "realu").
13. Użytkownik jest proszony o wyrażenie zgody na:
    13.1. Android: Lokalizacja (żeby skanować inne urządzenia w okolicy trzeba mieć zgodę na "Lokalizację". W praktyce jest to możliwość tracingu przez bluetooth; nie ma możliwości ustalania geolokalizacji urządzenia za pośrednictwem GPS).
    13.2. iOS: "Pozwolenie na używanie modułu Bluetooth".
14. Po wyrażeniu zgody, określonej w pkt. 13, aplikacja uruchamia moduł OpenTrace, który działa w tle (tylko w systemie Android, w systemie iOS możliwości działania Bluetooth w aplikacji działającej "w tle" są bardzo ograniczone), również po opuszczeniu aplikacji i zablokowaniu ekranu (na tyle na ile pozwala na to system operacyjny). Moduł bluetooth nie działa przy wyłączonej aplikacji.
15. Moduł OpenTrace rozgłasza się po Bluetooth ze swoim TempID.
16. TempID aplikacji jest rotowane tj. zmieniane co 15 minut zgodnie z bazą zapisaną na telefonie ilość kodów określimy w parametrach(tablica). Częstotliwość pobierania nowej paczki TemID jest również określana jako parametr w konfiguracji.
17. Moduł OpenTrace skanuje otoczenie w celu wykrycia innych użytkowników i zapisuje dane::, timestamp, msg (TempID), modelC, modelP, rssi, txPower, org. . Dane te są zapisywane w lokalnej pamięci telefonu. Zapewnienie bezpieczeństwa prywatności użytkownika odbywa się poprzez ukrycie go pod TempID zmieniającym się co 15 min.

18. Aplikacja zostaje rozszerzona o funkcjonalność generowania kodów QR (kod QR jest ustandaryzowany z TempID).
19. Dla każdego statusu triażu użytkownika jest przypisany kod QR w kolorze triażu
20. Aplikacja zyskuje funkcjonalność skanowania kodów QR wygenerowanych na innych urządzeniach z aplikacją PS,
21. Użytkownik jednej aplikacji może łatwo zeskanować kod QR drugiego użytkownika; w ten sposób TempID urządzenia zapisuje takie spotkanie jako bezpośrednie; jeżeli zestaw danych ze skanowania Bluetooth wykaże, że urządzenia widziały się przez więcej niż 15 min, oznacza to, że był to kontakt bezpośredni trwający więcej niż 15 minut.
22. Aplikacja w tej wersji obejmuje możliwość wyboru pomiędzy korzystaniem z aplikacji w trybie osoby fizycznej oraz instytucji.
23. Dodanie parametru osoba/instytucja do przyznawania UID
24. Tryb Instytucji obsługuje następujące funkcje:
    - 24.1. Rejestracja konta Instytucji
    - 24.2. Oparcie rejestracji Instytucji o wymagalność aktualnego kodu NIP danej Instytucji
    - 24.3. Zapisanie danych kontaktowych Instytucji
    - 24.4. Wygenerowanie kodu QR przypisanego do TempID Instytucji na stałe (w przeciwieństwie do końca osoby fizycznej gdzie TempID są rotowane)
    - 24.5. Wygenerowanie na backendzie akcji stworzenia plakatu z kodem QR instytucji i nazwą instytucji wynikającą z NIP.
    - 24.6. Możliwość wysłania plakatu z kodem QR instytucji na podanego do kontaktu emaila
    - 24.7. Możliwość wyświetlania w koncie Instytucji listy ostrzeżeń aplikacji, związanych z danymi wysyłanymi z OP BACKEND, o zweryfikowanych chorych na COVID-19 którzy potwierdzili swoją obecność w Instytucji poprzez zeskanowanie kodu QR wyświetlonego w trybie Instytucji przez Instytucję. Ostrzeżenia/notyfikacje o których mowa w niniejszym punkcie nie będą zawierały danych umożliwiających bezpośrednią identyfikację osoby fizycznej.
    - 24.8. Możliwość ręcznej weryfikacji podmiotów zakładających konta Instytucji
    - 24.9. Możliwość tymczasowego zawieszenia/odwieszenia konta Instytucji.

Opis czynności przetwarzania w wersji 3.2

Kontekst: Osoba zdiagnozowana medycznie jako chora na chorobę COVID-19 podaje swój numer telefonu do przedstawiciela organu zdrowia - w praktyce ten numer jest dołączony do testu na COVID-19.

Pracownik medyczny/laboratorium dodaje numer telefonu osoby zakażonej do rejestru CSIOZ.

25. Serwer z backend (codename: OP-BACKEND) odbiera informacje z rejestru CSIOZ (codename bazy: EWP) o osobie potwierdzonej zakażeniem COVID-19 (numer telefonu, data diagnozy).
26. Centrum Kontaktu podejmuje kontakt telefoniczny z osobą zarażoną COVID-19 i pyta, czy osoba ta ma zainstalowaną aplikację ProteGO Safe.
27. Jeśli chory jest użytkownikiem aplikacji operator prosi użytkownika o "wygenerowanie" w aplikacji krótkiego kodu PIN (składającego się z cyfr, oraz dużych i małych liter) i podyktowanie mu go. Operator wprowadza kod PIN w OP-BACKEND.
28. OP-BACKEND wykonuje połączenie ID użytkownika z numerem telefonu (autoryzacja i połączenie numeru telefonu z ID aplikacji/użytkownika) - w ten sposób łączy konkretną zainfekowaną osobą z konkretnym urządzeniem, z którego ta osoba korzysta.
29. Po poprawnym wprowadzeniu PIN dane z historią spotkanych TempID innych urządzeń z ostatnich 14-21 dni są wysyłane z urządzenia osoby zakażonej na Serwer z backendem ProteGO Safe.
30. Moduł zapisu danych historycznych (listy spotkanych urządzeń - lista TempID) zapisuje w bazie danych na Serwerze ściągnięte dane (powiązane z danym UID użytkownika i datą ściągnięcia).
31. Gdy dane zostały wysłane z aplikacji aplikacja zmienia status TRIAGE w aplikacji na "Chory na COVID-19". - musimy mieć pewność, że backend odebrał dane.
32. Aplikacja umożliwia zdjęcie statusu „Chory na COVID-19" po wprowadzeniu stosownej notyfikacji ze strony GIS.
33. Moduł przetwarzający i analizujący dane historyczne analizuje dane i określa jakie TempID miały kontakt z osobą zarażoną spełniające kryteria kwalifikacji kontaktu (minimum 15 minut) jako narażający osobę na zarażenie. Moduł ten kojarzy TempID z ID użytkowników w aplikacji.
34. Backend ProteGO Safe wysyła powiadomienia PUSH do osób zakwalifikowanych jako osoby będące w grupie wysokiego ryzyka zarażeniem z zestawem danych: o zmianie grupy ryzyka na wysoką, że miał kontakt z osobą chorą na COVID-19 na podstawie parametrów określonych na backendzie (parametryzowane dane: czas inkubacji choroby, czas kwarantanny, czas zbierania i przechowywania, parametry spotkania tj. czas i odległość w ciągu ostatnich X-dni-parametr dni lub ilości dni od dnia uruchomienia OpenTrace jeżeli ten został uruchomiony w czasie krótszym niż 14 dni.
35. Aplikacja zmienia status grupy ryzyka w TRIAGE (funkcja samooceny ryzyka zarażenia) na WYSOKA GRUPA RYZYKA i wyświetla stosowne dalsze wytyczne.
36. Użytkownik, który został oznaczony jako "grupa wysokiego ryzyka", zostaje poinformowany przez aplikację pod jaki numer Centrum Kontaktu ma dzwonić. Jeżeli użytkownik zadzwoni do Centrum Kontaktu, jest prowadzony i wspierany przez Centrum Kontaktu.

Załącznik nr 2 do Umowy

OPIS TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW BEZPIECZEŃSTWA

Środki techniczne:

1. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
2. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są systemem kontroli dostępu.
3. Dostęp do systemu operacyjnego komputera/serwera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych, przetwarzanych przy użyciu systemów teleinformatycznych.
5. Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.
6. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
7. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
8. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
9. Zastosowano środki ochrony przed oprogramowaniem złośliwym (malware) takim jak, np. robaki, wirusy, konie trojańskie, rootkity.
10. Zastosowano urządzenie Firewall do ochrony dostępu do sieci teleinformatycznej.
11. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
12. Zastosowano mechanizm automatycznej blokady dostępu do systemu teleinformatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Środki organizacyjne:

1. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
2. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu teleinformatycznego.
3. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
4. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.