Aneks nr 1
do umowy 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

zawarty 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 odpis 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) Strony działając w porozumieniu z Głównym Inspektorem Sanitarnym dokonały analizy ryzyka związanego z przetwarzaniem danych osobowych użytkowników Aplikacji, które wykazały zasadność decentralizacji sposobu działania Aplikacji (rozwoju Aplikacji w modelu, w którym przetwarzanie danych użytkowników aplikacji odbywać będzie się na ich urządzeniach mobilnych) w celu zwiększenia ochrony prywatności użytkowników Aplikacji,
2) Główny Inspektor Sanitarny, działając na podstawie zwartego z Zamawiającym porozumienia oraz w granicach swych kompetencji uznał, że decentralizacja działania Aplikacji nie wpłynie negatywnie na przeciwdziałanie pandemii COVID-19, oraz wskazał na rozwiązania techniczne oraz funkcjonalności, których wdrożenie w Aplikacji działającej w modelu zdecentralizowanym umożliwi efektywne przeciwdziałanie pandemii COVID-19,
3) W związku z konsultacjami, o których mowa powyżej, a także decyzją Zamawiającego o dalszej decentralizacji Aplikacji, Wykonawca na wniosek Zamawiającego rozpoczął analizę Exposure Notification API Google oraz Apple w tym dokumentacji do

przedmiotowego API, o którym mowa tutaj: https://www.google.com/covid19/exposurenotifications/ oraz https://developer.apple.com/documentation/exposurenotification (dalej: Exposure Notification API).

4) Wstępne wyniki analizy Exposure Notification API wykazały, że realizacja i dalszy rozwój Aplikacji, w tym dalsza decentralizacja, powinny zostać oparte o Exposure Notification API, co do czego Strony się zgadzają.
5) Strony oświadczają o pełnej świadomości prac nad Aplikacją, które mają charakter pracy twórczej oraz badawczo-rozwojowej prowadzącej do wytworzenia kwalifikowanego prawa własności intelektualnej w rozumieniu przepisów prawa podatkowego.

Strony postanowiły zawrzeć Aneks o następującej treści:

§ 1

Na podstawie § 15 ust. 6 Umowy Strony wprowadzają do Umowy następujące zmiany:

1) w §2 dodaje ustęp 6 w brzmieniu:

“Wykonawca zobowiązuje się zabezpieczyć stosowne środki, w tym przede wszystkim Personel w zakresie: dwóch programistów Swift (iOS), dwóch programistów Kotlin (Android), dwóch programistów ReactJS / ReactNative, dwóch specjalistów DevSecOps oraz managera projektu, aby świadczyć Zamawiającemu Usługi Utrzymania po zakończeniu niniejszej Umowy.

2) §5 ust. 1 otrzymuje brzmienie:

“Wynagrodzenie za realizację przedmiotu Umowy wynosi 1 884 000 PLN netto [słownie: jeden milion osiemset osiemdziesiąt cztery tysiące złotych 00/100], co wraz z podatkiem VAT w wysokości 433 320 PLN [słownie: czterysta trzydzieści trzy tysiące trzysta dwadzieścia złotych 00/100] stanowi kwotę 2 317 320 PLN [słownie: dwa miliony trzysta siedemnaście tysięcy trzysta dwadzieścia złotych 00/100], w tym za wynagrodzenie za poszczególne Etapy:

Etap 1 Aplikacja 2.0: 290.000,00 zł (słownie dwieście dziewięćdziesiąt tysięcy złotych i 00/100 zł),

Etap 2 Aplikacja 3.0: 280.000,00 zł. (słownie: dwieście osiemdziesiąt tysięcy złotych i 00/100 zł),

Etap 3 Aplikacja 3.1: 90.000,00 zł. (słownie: dziewięćdziesiąt tysięcy złotych i 00/100 zł),

Etap 4 Aplikacja 4.0: 369.000,00 zł. (słownie: trzysta sześćdziesiąt dziewięć tysięcy złotych i 00/100 zł),

Etap 5 Aplikacja 4.1: 365.900,00 zł. (słownie: trzysta sześćdziesiąt pięć tysięcy dziewięćset złotych i 00/100 zł),

Etap 6 Testy manualne i maszynowe: 120.000,00 zł. (słownie: sto dwadzieścia tysięcy złotych i 00/100 zł),

Etap 7 Założenia i testy cyberbezpieczeństwa: 274.100,00 zł. (słownie: dwieście siedemdziesiąt cztery tysiące sto złotych i 00/100 zł)
Etap 8 Komunikacja Aplikacji: 95.000,00 zł. (słownie: dziewięćdziesiąt pięć tysięcy)

3) w § 10 ust. 2 dodaje się pkt 7 w brzmieniu: SECURITUM AUDYTY Sp. z o.o. Sp.K. KRS: 0000636975, NIP: 6793133732.

4) w § 15 ust. 6 otrzymuje brzmienie:
„Zmiany Umowy wymagają zachowania formy pisemnej lub formie elektronicznej".
5) Załącznik nr 2 do Umowy otrzymuje brzmienie określone w Załączniku 1 do niniejszego Aneksu.

§ 2

1. Pozostałe postanowienia Umowy nie ulegają zmianie.

2. Strony zgodnie oświadczają, że z uwagi na okoliczności wskazane w Preambule nie nastąpiła zwłoka w realizacji poszczególnych Etapów Umowy za które odpowiedzialność ponosi którakolwiek ze Stron.

2. Aneks sporządzono w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym.

Załącznik nr 2 do Umowy

Szczegółowy Opis Przedmiotu Zamówienia

Przedmiotem Umowy jest opracowanie i dostarczenie aplikacji na urządzenia mobilne wraz z skonfigurowaniem Infrastruktury Zamawiającego i oprogramowania po stronie serwerowej wspierające aplikacje. Aplikacja przeznaczona jest dla nieograniczonej liczby Użytkowników Końcowych 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 w oparciu o Exposure Notification API. Moduł ten umożliwia tworzenie historii napotkanych urządzeń z zainstalowaną Aplikacją, a historia ta umożliwia poinformowanie Użytkowników Końcowych za pośrednictwem Aplikacji o tym, że mogą znajdować się w grupie wysokiego ryzyka zarażenia COVID-19. Aplikacja zostanie wykonana na Infrastrukturze Zamawiającego. Aplikacja zostanie wykonana zgodne z KEY VISUAL brandingu gov.pl bazując na przykładowych projektach interfejsu aplikacji dostępnym pod linkiem: https://zpl.io/a70ZWnW aktualnych na dzień 20 maja 2020 roku.

Pojęcia pisane wielką literą będą miały znaczenie określone w niniejszej tabeli:

Pojęcie	Definicja pojęcia
API G+A	Exposure Notification API Google oraz Apple, o którym mowa tutaj: https://www.google.com/covid19/exposurenotifications/ oraz https://developer.apple.com/documentation/exposurenotification.
Aplikacja	Aplikacja ProteGO Safe
Centrum Kontaktu	Wskazane przez Zamawiającego call-center dedykowane do przeciwdziałania pandemii COVID-19 oraz informowania Osób Chorych o wynikach testu na COVID-19.
Cloud-Backend	Centralny serwer za pośrednictwem którego przesyłane są Diagnosis Key w celu przekazania informacji do innych Użytkowników Końcowych, którzy mogli mieć kontakt z Osobą Chorą.
CSIOZ	Centrum Systemów Informacyjnych

	Ochrony Zdrowia
Diagnosis Key	Klucz Osoby Chorej lub Użytkownika Końcowego, który może zostać przekazany za pośrednictwem Cloud Backend do innych Użytkowników Końcowych. Generowany lokalnie na urządzeniu użytkownika, przez stosowny moduł dostarczony przez firmy Google i Apple.
EWP	rejestr Osób Chorych prowadzony przez CSIOZ
G+A	Google LLC. oraz Apple Inc.
OP-Backend	Element systemu do podejmowania kontaktu z Osobami Chorymi.
Osoba Chora	Osoba zarażona COVID-19, której choroba została potwierdzona pozytywnym wynikiem testu na obecność SARS-CoV-2 oraz której dane zostały wprowadzone do bazy CSIOZ (zawierającej rejestr Osób Chorych).
Użytkownik Końcowy	Każdy użytkownik Aplikacji.
Triage	Funkcja w Aplikacji umożliwiająca przypisanie grupy ryzyka zarażenia COVID-19.

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 13.5 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.

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
22/05/2020	Etap 3	3.1	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.3
22/05/2020	Etap 4	4.0	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.4
10 dni od opublikowania stosownej dokumentacji API G+A	Etap 5	4.1	Wykonawca	Zgodny z Zakresem funkcjonalności opisanym w punkcie 1.5
22/05/2020	Etap 6	-	Wykonawca	Zgodny z Zakresem opisanym w punkcie 1.6
10 dni od opublikowania stosownej dokumentacji API G+A	Etap 7	-	Wykonawca	Zgodny z Zakresem opisanym w punkcie 1.7

30/06/2020	Etap 8	-	Wykonawca	Zgodny z Zakresem opisanym w punkcie 1.8

1. Opis procesu UX do implementacji w aplikacji:

1.1. Etap 1 - Zakres funkcjonalności dla wersji 2.0

1. Użytkownik Końcowy instaluje Aplikację na telefonie Android,
2. Użytkownik Końcowy otwiera Aplikację i wyświetlają mu się informacje o sposobie jej działania i potrzebnych zgodach/uprawnieniach (akceptacja Regulaminu i Polityki Prywatności).
3. Użytkownik Końcowy uzupełnia metrykę zdrowia.
4. Użytkownik Końcowy wypełnia pierwszy test oceny ryzyka (Triage).
5. Użytkownik Końcowy dostaje pierwszy wynik klasyfikacji swojego stanu zdrowia (Triage).
6. Użytkownik Końcowy odbiera notyfikacje push przypominające o potrzebie wypełnienia testu oceny ryzyka.
7. Aplikacja prowadzi Użytkownika Końcowego przez porady i zachowania związane z jego stanem zdrowia na podstawie oceny ryzyka (Triage).
8. Użytkownik Końcowy może wypełniać dowolną ilość razy dziennie: test oceny ryzyka (Triage) i dziennik zdrowia.
9. Po trzech dniach, w których Użytkownik Końcowy 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 Końcowy musi wyrazić zgodę na “Pozwolenie na wysyłanie notyfikacji”.

Zakres:
- celowy i pożądany brak synchronizacji z Google Analytics,
- brak rejestracji Użytkownika Końcowego 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 Końcowy pobiera aplikację ProteGO Safe 3.0 z modułem OpenTrace i nie ma w niej możliwości (i widoku) podania numeru telefonu (Użytkownik Końcowy 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 (Infrastruktura Zamawiającego) 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 Końcowych w module tracingowym (kontakt Bluetooth w “realu”).
3. Użytkownik Końcowy 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 Końcowych i zapisuje dane: timestamp, msg (TempID), modelC, modelP, rssi, txPower, org. . Dane te są zapisywane w lokalnej pamięci telefonu. Zapewnienie bezpieczeństwa prywatności Użytkownika Końcowego odbywa się poprzez ukrycie go pod TempID zmieniającym się co 15 min.

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

1.3. Etap 3 - Zakres funkcjonalności dla wersji 3.1

Wersja testowa app opartej o OpenTrace [nie produkcyjna]

1. Aplikacja zostaje rozszerzona o funkcjonalność wyświetlania na ekranie aplikacji kodów QR (kod QR jest ustandaryzowany z TempID).
2. Dla każdego statusu Triageu Użytkownika Końcowego jest przypisany kod QR w kolorze Triageu
3. Aplikacja zyskuje funkcjonalność skanowania kodów QR wygenerowanych na innych urządzeniach z aplikacją PS,
4. Użytkownik Końcowy Aplikacji może łatwo zeskanować kod QR drugiego Użytkownika Końcowego; w ten sposób TempID urządzenia zapisuje takie spotkanie jako bezpośrednie; jeżeli zestaw danych ze skanowania Bluetooth wykaże, że urządzenia widziały się przez okres wskazany przez Zamawiającego lub GIS.

1.4. Etap 4 - Zakres funkcjonalności i przepływu danych dla wersji 4.0

Wersja główna aplikacji opartej o API Google + Apple [produkcyjna]

Kontekst: Osoba Chora przekazuje swój numer, lub numery telefonu (kontaktowe) uprawnionemu przedstawicielowi służby zdrowia. Numer telefonu jest przypisywany do próbki (z danymi Osoby Chorej jest przesyłane jego ewp_id co pozwala łączyć telefony tej samej osoby), którą pobiera uprawniony przedstawiciel służby zdrowia - w praktyce ten numer jest dołączony do testu na obecność COVID-19.

Pracownik medyczny/laboratorium dodaje numer telefonu Osoby Chorej do rejestru CSIOZ.

Wypracowane efekty finalne etapu:

Nazwa elementu	Zakres techniczny	Zakres funkcjonalny
OP-BACKEND	Napisany w: Java, Spring.	Narzędzie pracy dla operatorów wyznaczonych przez Health Authority w Centrum Kontaktu w celu nawiązania kontaktu telefonicznego z Osobami Chorymi na COVID-19.
OP-BACKEND / integracja z EWP	Integracja bez API. Możliwość odbierania danych przesyłanych w pliku .xml	OP-BACKEND przyjmuje dane z EWP i wyświetla je w panelu w taki sposób, żeby operator mógł wykonać kontakt telefoniczny z wskazanymi numerami telefonów.
OP-BACKEND / integracja z bramką SMS	- Integracja po API ze wskazanym dostawcą usługi wysyłki SMSów. - Wysyłka SMSów. - Odnotowanie operacji wysłania SMS przy telefonie kontaktowanej osoby	Integracja z API dostawcy SMSów. SMSy z prośba o kontakt telefoniczny będą wysyłane w przypadku braku odbierania telefonu po stronie O soby C horej podczas kontaktu operatora .
OP-BACKEND / rejestracja i logowanie Operatorów	- Dwa rodzaje kont: administrator/Operator - Rejestracja konta przez administratora systemu	Możliwość zakładania kont i pracy wielu operatorów równolegle w panelu.

	- Logowanie Operatorów - Resetowanie hasła operatora - Usuwanie Operatorów przez administratora	
OP-BACKEND / system oznaczania statusu postępu kontaktu	Pole/pola umożliwiające Operatorowi ustawianie statusu kontaktu.	Pole/pola umożliwiające Operatorowi ustawianie statusu kontaktu.
Moduł PIN - funkcjonalność wpisania kodu PIN	Napisany w: ReactJS	Umożliwia wprowadzenie kodu PIN w aplikacji i potwierdzenie chęci wysłania Diagnosis Key aplikacji.

Scenariusz ścieżki użytkownika:

1. Informacja zawierająca numer telefonu (bez innych danych: imienia, nazwiska, płci, wieku, adresu i innych) Osoby Chorej, jest przekazywany po API pomiędzy CSIOZ (EWP) a OP-Backend.
2. Element systemu do podejmowania kontaktu Osobami Chorymi (OP-Backend) odbiera informacje z rejestru EWP o Osobie Chorej (identyfikator pacjenta w EWP, numer telefonu, data diagnozy).
3. Operator Centrum Kontaktu jest zalogowany do kokpitu OP-Backend na komputerze stacjonarnym. Login i hasło otrzymał od administratora, który każdemu operatorowi zakłada takie konto po jego weryfikacji przez uprawnioną osobę. Operator jest zalogowany do systemu, widzi w nim listę numerów kontaktowych Osób Chorych (lista zaciąga się z EWP). Operator wybiera jeden z numerów. Wybranie numeru do obsługi przez danego operatora blokuje numer Osoby Chorej dla innych operatorów (numer jest usuwany z list numerów kontaktowych, widocznej dla innych operatorów), co jest znakiem dla innych operatorów, że dany kontakt jest już obsługiwany. Wykonuje telefon.
4. Centrum Kontaktu podejmuje kontakt telefoniczny Osobą Chorą i pyta, czy osoba ta ma zainstalowaną aplikację ProteGO Safe.
    4.1. Odbiorca nie odbiera - operator może odnotować w systemie taką informację w oparciu, o którą później on, lub inny operator podejmie kolejną próbę kontaktu.
    4.2. Jeśli kontakt jest nieskuteczny i odbiorca cały czas nie odbiera telefonu, operator klika w systemie wiadomość SMS [treść do opracowania] która wysyła się automatycznie na numer telefonu odbiorcy z prośbą o pilny kontakt z Centrum Kontaktu GIS.

4.3. Osoba Chora odbiera telefon i NIE JEST Użytkownikiem Końcowym: Proces kontaktu się kończy.

4.4. Osoba Chora odbiera telefon i JEST Użytkownikiem Końcowym. Operator rozpoczyna scenariusz możliwej wysyłki Diagnosis Key.

5. po upewnieniu się, że Osoba Chora została właściwie poinformowana, Operator pyta czy Osoba Chora ma zainstalowaną aplikację ProteGO Safe.
6. Jeżeli Osoba Chora nie ma zainstalowanej aplikacji, operator proponuje zainstalowanie ProteGO Safe i przedstawia scenariusz zalecany w takiej sytuacji przez GIS.
7. Jeżeli Osoba chora ma zainstalowaną aplikację, operator kontynuuje realizację scenariusza wysyłki Diagnosis Key Chorego.
8. (Opcjonalnie) Operator tłumaczy Osobie Chorej jak działa wysyłanie Diagnosis Key. Cechy:
   8.1. jest anonimowe,
   8.2. narzędzie opiera się na naszej odpowiedzialności społecznej
   8.3. pozwala wysłać ostrzeżenie, do osób, które mogły mieć kontakt z Osobą Chorą.
   8.4. Operator, ani Użytkownik Końcowy, który zostanie poinformowana przez system nie mają możliwości identyfikacji Osoby Chorej, z którą rozmawia operator.
9. Dla kontynuowania scenariusza Osoba Chora musi wyrazić chęć (opt-in) wysłania historii swoich Diagnosis Key.
10. Operator instruuje Osobę Chorą, jak przełączyć rozmowę na głośnik telefonu, jak zminimalizować ono rozmowy na telefonie, następnie pomaga odnaleźć aplikację (nazwa, logo, kolory) i tłumaczy gdzie w aplikacji trzeba klikać żeby dojść do pola wpisania kodu PIN, po wpisaniu, którego aplikacja umożliwi wysłanie historii Diagnosis Key Osoby Chorej z ostatnich 14 dni.
11. Operator w kokpicie OP-Backend klika funkcję “wyświetl dostępny PIN”. OP-Backend w tym momencie odpytuje PS-BACKEND jaki aktualnie dostępny losowo przyznany kod PIN może umożliwić przesłanie zbioru Diagnosis Key z aplikacji Osoby Chorej (przesyłane są tylko Diagnosis Key Osoby Chorej, bez historii napotkanych Diagnosis Key innych osób - to ważne ze względu na zdecentralizowany model metodologii pracy aplikacji).

    Kod PIN zostaje czasowo wyświetlony Operatorowi (bez zapisywania, nawet tymczasowego w jakiejkolwiek bazie danych). Czas wyświetlania zostanie dostosowany do wytycznych Centrum Kontaktu. Czas wyjściowy wyświetlania kodu PIN na ekranie Operatora zostanie ustalony w trybie roboczym między Zamawiającym a Wykonawcą przy uwzględnieniu opinii GIS, jeżeli Operator wcześniej zamknie okno wyświetlanego kodu PIN.
12. Operator kontynuując rozmowę przedyktowuje Osobie Chorej kod PIN. PIN zawsze ma 6 losowych znaków pogrupowanych po 3 znaki. Dyktuje np.: duże d, małe e, trzy, osiem, duże g, dwa. Osoba Chora wpisuje: De3 - 8G2

13. Osoba Chora klika przycisk “Zapisz”
14. Na ekranie aplikacji Osoby Chorej pojawia się okno “Czy chcesz wysłać swoje Diagnosis Key do chmury ProteGO Safe żeby anonimowo ostrzec innych użytkowników aplikacji?”. Jeżeli Osoba Chora chce, żeby dane zostały wysłane dobrowolnie potwierdza to kliknięciem “Tak”.

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

1.5. Etap 5 - Zakres funkcjonalności i przepływu danych dla wersji 4.1

Kontekst: Aplikacja w tej wersji, zyskuje pełną integrację z modułami G+A (Moduł Analityczny, Moduł Bluetooth, Moduł lokalnego generowania kodów Diagnosis Key). Umożliwia wysyłkę historii Diagnosis Key Osoby Chorej na Cloud-Backend, a także dalszą ich dystrybucję przez Cloud-Backend do wszystkich Użytkowników Końcowych.

Wypracowane efekty finalne etapu:

Nazwa elementu	Zakres techniczny	Zakres funkcjonalny
Aplikacja / Moduł Analityczny	Rozwiązanie typu “blackbox” dostarczane przez G+A.	- weryfikuje, czy pobrane z Cloud Backend Diagnosis Key pokrywa się z Diagnosis Key, które w ciągu ostatnich 14 dni widziała aplikacja użytkownika. - Analizuje poziom ryzyka takiego spotkania (jeżeli wystąpiło) i określa poziom ryzyka w skali od 1 do 8.
Aplikacja / Moduł Diagnosis Key	Rozwiązanie typu “blackbox” dostarczane przez G+A.	- Umożliwia generowanie unikatowych Diagnosis Key w Aplikacji na urządzeniu Użytkownika Końcowego.

Aplikacja / Moduł Bluetooth	Rozwiązanie typu “blackbox” dostarczane przez G+A.	- Umożliwia skanowanie otoczenia i rozpoznawanie innych Urządzeń Końcowych - Zapisuje spotkane Diagnosis Key i parametry niezbędne do oceny poziomu ryzyka kontaktu z Osobą Chorą. - Rozgłasza Diagnosis Key urządzenia użytkownika.
CLOUD-BACKEND	Oprogramowanie modułu w języku umożliwiającym wykonanie akcji opisanych w zakresie funkcjonalnym.	- Generowanie kodów PIN - Zarządzanie aktualnie dostępnymi kodami PIN - Walidacja kodu w trakcie wysyłki danych - Invalidowanie użytego kodu - Czasowe zablokowanie kodu po wyświetleniu go w OP-BACKEND - Jeden numer PIN umożliwia jedno wysłanie Diagnosis Key. - Kody PIN są jednorazowe.
CLOUD-BACKEND / potwierdzenie dostarczenia kluczy		- Cloud Backend potwierdza do urządzenia, że Diagnosis key zostały poprawnie wysłane.
Aplikacja / potwierdzenie	Komunikat wyświetlony w	- Aplikacja wyświetla

lub niepowodzenie wysłania kluczy	aplikacji i/lub PUSH.	użytkownikowi komunikat ze statusem powodzenie / niepowodzenie wysłania kluczy. - W przypadku niepowodzenia aplikacja instruuje konieczność ponownego kontaktu z Centrum Kontaktu (komunikat) - Komunikat wymaga potwierdzenia odczytania przez użytkownika.
Aplikacja / walidacja wpisywania PIN	Komunikat wyświetlony w aplikacji.	- po 3 nieudanych próbach wpisania PIN blokada na 1 min - po kolejnej nieudanej próbie blokada na 5 min. - po kolejnej nieudanej próbie blokada na 1h - po każdej kolejnej nieudanej próbie blokada na 24h
Aplikacja / pobieranie Diagnosis Key	Aplikacja Użytkownika Końcowego pobiera Diagnosis Key Osób Ch orych z Cloud Backend.	- Zgodnie z częstotliwością ustaloną przez G+A i/lub Health Authority - Aplikacja rozpoznaje co już pobrała, pobiera tylko nowe zestawy danych. - Po dłuższej nieobecności Aplikacja pobierze wszystkie Diagnosis Key Osób Chorych, których nie posiada,

		z ostatnich 14 dni.
CLOUD-BACKEND	-	- Funkcjonalność Generowanie kodu PIN, który ma określony okres ważności oraz jest jednorazowy - Okresowe usuwanie kodów PIN, które są przeterminowane (nieważne) - Wymiana kodu PIN na token umożliwiający upload Diagnosis Key - Akceptacja wysłanych Diagnosis Key poprzez walidację tokenu oraz ich zapis do tymczasowego storage'a - Okresowe generowanie pliku (paczki odebranych diagnosis keys) podpisanego prywatnym kluczem i udostępnienie go dla Użytkowników Końcowych Okresowe usuwanie przeterminowanych odebranych Diagnosis Key
Aplikacja / Moduł Synchronizacji Informacji Gov.pl	- Stworzenie modułów automatycznej aktualizacji treści w Aplikacji z danymi dostępnymi na stronach rządowych.	- synchronizacja danych z pacjent.gov.pl; - synchronizacja danych z pytań i odpowiedzi z https://www.gov.pl/web/koronawirus/pytania-i-odpowiedzi; - synchronizacja danych

		teleadresowych o szpitalach zakaźnych - synchronizacja i rozwój porad przekazywanych Użytkownikom Końcowym ze stron rządowych https://www.gov.pl/web/koronawirus/porady.

1. Informacja zawierająca numer telefonu (bez innych danych: imienia, nazwiska, płci, wieku, adresu i innych) Osoby Chorej, jest przekazywany po API pomiędzy CSIOZ (EWP) a OP-Backend.
2. Element systemu do podejmowania kontaktu z Osobami Chorymi (OP-Backend) odbiera informacje z rejestru EWP o Osobie Chorej (identyfikator pacjenta w EWP, numer telefonu, data diagnozy).
3. Operator Centrum Kontaktu jest zalogowany do kokpitu OP-Backend na komputerze stacjonarnym. Login i hasło otrzymał od administratora, który każdemu operatorowi zakłada takie konto po jego weryfikacji przez uprawnioną osobę. Operator jest zalogowany do systemu, widzi w nim listę numerów kontaktowych Osób Chorych (lista zaciąga się z EWP). Operator wybiera jeden z numerów. Wybranie numeru do obsługi przez danego operatora blokuje numer Osoby Chorej dla innych operatorów (numer jest usuwany z list numerów kontaktowych, widocznej dla innych operatorów), co jest znakiem dla innych operatorów, że dany kontakt jest już obsługiwany. Wykonuje telefon.
4. Centrum Kontaktu podejmuje kontakt telefoniczny z Osobą Chorą i pyta, czy osoba ta ma zainstalowaną aplikację ProteGO Safe.
   4.1. Odbiorca nie odbiera - operator może odnotować w systemie taką informację w oparciu, o którą później on, lub inny operator podejmie kolejną próbę kontaktu.
   4.2. Jeśli kontakt jest nieskuteczny i odbiorca cały czas nie odbiera telefonu, operator klika w systemie wiadomość SMS [treść do opracowania] która wysyła się automatycznie na numer telefonu odbiorcy z prośbą o pilny kontakt z Centrum Kontaktu GIS.
   4.3. Osoba Chora odbiera telefon i NIE JEST Użytkownikiem Końcowym: Proces kontaktu się kończy.
   4.4. Osoba Chora odbiera telefon i JEST Użytkownikiem Końcowym. Operator rozpoczyna scenariusz możliwej wysyłki Diagnosis Key.
5. po upewnieniu się, że Osoba Chora została właściwie poinformowana, Operator pyta czy Osoba Chora ma zainstalowaną aplikację ProteGO Safe.

6. Jeżeli Osoba Chora nie ma zainstalowanej aplikacji, operator przedstawia scenariusz zalecany w takiej sytuacji przez GIS.
7. Jeżeli Osoba Chora ma zainstalowaną aplikację, operator kontynuuje realizację scenariusza wysyłki Diagnosis Key Osoby Chorej.
8. (Opcjonalnie) Operator tłumaczy Osobie Chorej jak działa wysyłanie Diagnosis Key. Cechy:
   8.1. jest anonimowe,
   8.2. narzędzie opiera się na naszej odpowiedzialności społecznej
   8.3. pozwala wysłać ostrzeżenie, do osób, które mogły mieć kontakt z Osobą Chorą.
   8.4. Operator, ani Użytkownik Końcowy, który zostanie poinformowana przez system nie mają możliwości identyfikacji Osoby Chorej, z którą rozmawia operator.
9. Dla kontynuowania scenariusza Osoba Chora musi wyrazić chęć (opt-in) wysłania historii swoich Diagnosis Key.
10. Operator instruuje Osobę Chorą, jak przełączyć rozmowę na głośnik telefonu, jak zminimalizować rozmowy na telefonie, następnie pomaga odnaleźć aplikację (nazwa, logo, kolory) i tłumaczy gdzie w aplikacji trzeba klikać żeby dojść do pola wpisania kodu PIN, po wpisaniu, którego aplikacja umożliwi wysłanie historii Diagnosis Key Osoby Chorej z ostatnich 14 dni.
11. Operator w kokpicie OP-Backend klika funkcję “wyświetl dostępny PIN”. OP-Backend w tym momencie odpytuje PS-BACKEND jaki aktualnie dostępny losowo przyznany kod PIN może umożliwić przesłanie zbioru Diagnosis Key z aplikacji Osoby Chorej (przesyłane są tylko Diagnosis Key Osoby Chorej, bez historii napotkanych Diagnosis Key innych osób - to ważne ze względu na zdecentralizowany model metodologii pracy aplikacji).

    Kod PIN zostaje czasowo wyświetlony Operatorowi (bez zapisywania, nawet tymczasowego w jakiejkolwiek bazie danych). Czas wyświetlania zostanie dostosowany do wytycznych Centrum Kontaktu. Czas wyjściowy wyświetlania kodu PIN na ekranie Operatora zostanie ustalony w trybie roboczym między Zamawiającym a Wykonawcą przy uwzględnieniu opinii GIS, jeżeli Operator wcześniej zamknie okno wyświetlanego kodu PIN.
12. Operator kontynuując rozmowę przedyktowuje Osobie Chorej kod PIN. PIN zawsze ma 6 losowych znaków pogrupowanych po 3 znaki. Dyktuje np.: duże d, małe e, trzy, osiem, duże g, dwa. Osoba Chora wpisuje: De3 - 8G2
13. Osoba Chora klika przycisk “Zapisz”
    Na ekranie aplikacji Osoby Chorej pojawia się okno „Czy chcesz wysłać swoje Diagnosis Key do chmury ProteGO Safe, żeby anonimowo ostrzec innych użytkowników aplikacji?”. Jeżeli Osoba Chora chce, żeby dane zostały wysłane, dobrowolnie potwierdza to kliknięciem “Tak”.
14. Na ekranie aplikacji Osoby Chorej pojawia się okno “Czy chcesz wysłać swoje Diagnosis Key do chmury ProteGO Safe żeby anonimowo ostrzec innych użytkowników

aplikacji?". Jeżeli Osoba Chora chce, żeby dane zostały wysłane dobrowolnie potwierdza to kliknięciem "Tak".

15. W tym momencie aplikacja generuje historię Diagnosis Key Osoby Chorej z okresu czasu zdefiniowanego przez API G+A i wysyła ją na serwer centralny (do Cloud-Backend).
16. Operator kończy rozmowę z Osobą Chorą.
17. Historia Diagnosis Key zapisuje się tymczasowo na Cloud Backend, skąd będzie pobierana przez każdą aplikację ProteGO Safe Użytkownika Końcowego, która może połączyć się z serwerem centralnym (ma internet, jest włączona itp.)
18. Jeżeli aplikacja ProteGO Safe innego Użytkownika Końcowego widzi, że na serwerze jest nowy zestaw danych od Osoby Chorej i pobiera go.
19. Aplikacja innego Użytkownika Końcowego sprawdza, czy Diagnosis Key które pobrała pokrywa się z jakimiś, z którym się widziała (których historia jest zapisana lokalnie w aplikacji Użytkownika Końcowego).
20. Jeżeli aplikacja określa, że nie miała kontaktu z takim Diagnosis Key - nic się nie dzieje, a dane pobranego Diagnosis Key zostają po 14 dniach usunięte.
21. Jeżeli aplikacja określa, że miała kontakt z takim Diagnosis Key, wtedy sprawdza w swojej historii jaka była siła takiego spotkania i moduł analityczny po API Google & Apple liczy, jakie jest zagrożenie zarażenia. Obowiązuje skala 1-8.
22. W zależności od przyjętego przez GIS oznaczenia (w formie modyfikowanego parametru), TRIAGE aplikacji zmienia się / lub zostaje w jednym z trzech kolorów:
    Niska Grupa Ryzyka (zielone),
    Średnia Grupa Ryzyka (pomarańczowe),
    Wysoka Grupa Ryzyka (czerwone).
23. Aplikacja wysyła Użytkownikowi Końcowemu powiadomienia PUSH z informacją do jakiej grupy TRAGE został zakwalifikowany Użytkownik Końcowy w oparciu o zebrane dane.
24. W zależności od tego jaki kolor i status wyświetlił się Użytkownikowi Końcowemu aplikacji, dostaje on różne porady i numery telefonów przypisane do adekwatnej sytuacji.
25. Użytkownik Końcowy dobrowolnie podejmuje (bądź nie) kontakt z Centrum Kontaktu na podany w aplikacji numer i jest dalej instruowany jak postępować.

Dodatkowe funkcjonalności realizowane w ramach tego etapu:

1. Stworzenie modułów automatycznej aktualizacji treści w Aplikacji z danymi dostępnymi na stronach rządowych.
2. 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 o szpitalach zakaźnych ;

3.4. synchronizacja i rozwój porad przekazywanych Użytkownikom Końcowym 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:
    - konfiguracje o największej krytyczności jak i najpopularniejsze urządzenia (pokrycie rynku) w celu zwiększenia pokrycia urządzeń, na których będzie dokonywana kalibracja aplikacji.
    - testy na fizycznych urządzeniach
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 Końcowych 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, 4.0 i 4.1 w formie przedwydaniowej na urządzeniach fizycznych.
9. Zestaw skryptów weryfikujących poprawność działania podstawowych ścieżek krytycznych w aplikacji PWA, w celu monitorowania ciągłości stabilności wdrożeń na środowisku testowym.
10. Zestaw skryptów weryfikujących poprawność działania podstawowych ścieżek krytycznych w natywnych aplikacjach Android i iOS (z uwzględnieniem modułów dostarczonych przez G+A)
11. Analiza statyczna kodu i architektury (w aplikacji klasy np. Sonaqube)

1.7. Etap 7 - Założenia i testy cyberbezpieczeństwa

Analiza infrastruktury i bezpieczeństwa

1. Testy cyberbezpieczeństwa - przeprowadzone przez podmiot o renomowanej rynkowo opinii z zakresu testów bezpieczeństwa - Securitum Audyty Sp. z o.o. Sp. K., podwykonawca określony w § 10 ust. 2 pkt. 7 Umowy.
2. Testy wydajności i bezpieczeństwa platformy - przeprowadzone przez podmiot o renomowanej rynkowo opinii z zakresu zapewnienia wysokiej wydajności i bezpieczeństwa platform - Webini sp. Z o.o. ., podwykonawca określony w § 10 ust. 2 pkt 2 Umowy.
3. Kod źródłowy Aplikacji chroniony jest w prywatnym repozytorium w Serwisie Github.
4. Jeśli kod Aplikacji trafia do tak zwanego pre-release jest wykonywany automatyczny proces:
   - budowania Aplikacji z ustawieniami dla środowiska dev/stage,
   - wykonuje się podstawowy test potwierdzający, że Aplikacja została poprawnie zbudowana,
   - uruchamia się skaner automatycznie wykrywający znane podatności. Zastosowane rozwiązania: Whitesource for Github z tak zwanego GitHub Marketplace
   - wykonuje się kolejna weryfikacja i opinia drugiego skanera podatności dostarczanego przez firmę Snyk również przez GitHub marketplace.
   - analiza statyczna kodu
5. Jeśli któryś z elementów drzewa zależności Aplikacji wymaga poprawek, 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, w którym jest poddawany społecznemu audytowi.
8. Kod łączony jest z masterem po manualnym potwierdzeniu i review przez min 2 uprawnionych Użytkowników Końcowych jest uruchamiany automatyczny proces przygotowania kolejnej oficjalnej i produkcyjnej wersji Aplikacji:
   - budowania Aplikacji z ustawieniami dla środowiska produkcyjnego,
   - podstawowy test potwierdzający, że Aplikacja się zbudowała,
   - uruchamiany jest skaner automatycznie wykrywający znane podatności. Wybrane zostało do tego celu dostępne w ramach GitHub Marketplace rozwiązanie Whitesource for Github,
   - następuje druga opinia skanera podatności tym razem dostarczanego przez Snyk za pośrednictewm GitHub Marketplace,
   Jeśli któryś z elementów drzewa zależności Aplikacji wymaga poprawek, a są one dostępne, następuje próba usunięcia podatności.
9. Jeśli brak jest zgłoszeń od wewnętrznych testerów, Aplikację jest przekazywana do środowiska produkcyjnego.

Obszary testów cyberbezpieczeństwa

W etapie pierwszym do 22 maja:

1. Testy penetracyjne elementów infrastruktury (m.in. VM) [blackbox]
2. Testy penetracyjne aplikacji PWA (safesafe.app) [blackbox]
3. Testy penetracyjne i analiza bezpieczeństwa aplikacji Android i iOS [blackbox]
4. Podstawowa analiza kodu aplikacji mobilnych [whitebox]
5. Przygotowanie wytycznych do procesu developmentu aplikacji [analysis],

W etapie drugim do 25 maja:

1. Weryfikacja pełnego środowiska (w tym CI/CD) [whitebox]
2. Analiza konfiguracji Google Cloud Platform i Firebase [whitebox]
3. Testy penetracyjne modułu do wysyłki PIN [blackbox],
4. Testy penetracyjne aplikacyjne Operator Backend [blackbox],
5. Testy penetracyjne infrastruktury Operator Backend [blackbox],
6. Testy penetracyjne aplikacyjne Cloud Backend [blackbox],
7. Testy penetracyjne infrastruktury Cloud Backend [blackbox],
8. Testy obciążeniowe DDoS – dla dwóch adresów IP,
9. Hardening konfiguracji GCP VM (1 serwer) [whitebox],
10. OPCJONALNIE – retest obszarów z poprawkami po pierwszym etapie.

Zakres szczegółowy:

Testy penetracyjne aplikacji www

- Rekonesans aktywny i pasywny (w przypadku aplikacji dostępnych w Internecie)
- Próby lokalizacji aplikacji dostępnej pod innym adresem (np. aplikacja deweloperska w infrastrukturze dostawcy, publicznie dostępna aplikacja w wersji testowej)
- Próby lokalizacji ukrytych katalogów i plików
- Próby wywołania błędów / wyjątków w aplikacji
- Poszukiwanie innych domen dostępnych na tym samym adresie IP co domena bazowa
- Poszukiwanie wycieków danych (np. technika Google Hacking, analiza pliku robots.txt).
- Poszukiwanie podatności
- Podatności klasy injection (np. SQL injection, LDAP injection, XPATH injection, NoSQL injection).
- Podatność XXE (użycie zewnętrznych encji XML)
- Podatność XSS (Cross Site Scripting) – błędy typu reflected oraz stored.
- Analiza problemów z uwierzytelnianiem i autoryzacją (np. próby dostępu do zasobów bez uwierzytelnienia, próby dostępu do zasobów administracyjnych przez zwykłego użytkownika, próby przełamania ekranów logowania – w tym próby brute force danych dostępowych).

- Możliwości otrzymania nieautoryzowanego dostępu na poziomie systemu operacyjnego i uzyskanie w ten sposób dostępu do źródeł aplikacji, bazy danych, innych poufnych informacji.
- Analiza błędów logicznych
- Próby wykrycia innych, znanych podatności, np.: Path Traversal, Open Redirection, Cross Site Request Forgery, Server Side Request Forgery, Server Side Template Injection.
- Detekcja ogólnie znanego oprogramowania (aplikacje, biblioteki, systemy wspomagające).
- Po wykryciu nieaktualnych wersji, próby lokalizacji znanych, istotnych podatności w kilku wybranych źródłach

1. **Analiza konfiguracji Google Cloud Platform i Firebase**:
    a. Sprawdzenie modelu uprawnień i tożsamości (IAM),
    b. Analiza sposobu logowania zdarzeń,
    c. Sprawdzenie separacji środowisk,
    d. Sprawdzenie sposobu deploymentu stron w Firebase.

2. **Testy penetracyjne aplikacji na Android i iOS:**
    a. Sprawdzenie sposobu przechowywania danych na pamięci masowej urządzenia mobilnego,
    b. Analiza mechanizmów komunikacji międzyprocesowej (np. możliwość bezpośredniego dostępu do poufnych danych aplikacji przez inną, złośliwą aplikację),
    c. Analiza zastosowanych mechanizmów kryptograficznych,
    d. Analiza integracji z API Exposure Notification,
    e. Analiza konfiguracji WebView,
    f. Sprawdzenie mechanizmu pinningu certyfikatów,
    g. Sprawdzenie logowanych zdarzeń w dzienniku systemowym.

3. **Testy penetracyjne blackbox elementów infrastruktury:**

Dotyczą wystawianych maszyn do Internetu (jedna maszyna: api.safesafe.app).

    a. Skanowanie portów TCP/UDP,
    b. Wykorzystanie skryptów nmap NSE w celu realizacji enumeracji, wykrycia możliwych wycieków danych, czy wskazania podatności,
    c. Próba detekcji typu oraz wersji usług sieciowych działających w systemie.
    d. Próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu.

e. Po udanej detekcji wersji oprogramowania systemowego / usług – próba lokalizacji znanych podatności w danych wersjach oprogramowania.
f. Skanowanie podatności z wykorzystaniem komercyjnej wersji oprogramowania Nessus Vulnerability Scanner (ponad 90.000 pluginów atakujących).

4. Podstawowa analiza whitebox kodu aplikacji mobilnych

Dotyczy obu aplikacji mobilnych i koncentruje się wyłącznie na podstawowych aspektach

a. Dotyczy obu aplikacji mobilnych.
b. Sprawdzenie sposobu przetwarzania danych użytkownika,
c. Sprawdzenie sposobu integracji z innymi systemami (np. bazami danych),
d. Sprawdzenie mechanizmów uwierzytelnienia i autoryzacji,

Hardening konfiguracji GCP VM (1 serwer)

Zakres prac:

- Analiza konfiguracji systemu operacyjnego na maszynie wirtualnej pod kątem:
- Udostępnianych usług sieciowych,
- Działających procesów,
- Wdrożenia dodatkowych metod ochrony (np. SELinux, firewall itp.),
- Uprawnień do plików,
- Sposobu wykonywania aktualizacji,
- Dla kluczowych usług sieciowych działających na serwerze wykonanie sprawdzeń bezpieczeństwa:
- Sprawdzenie szyfrowania komunikacji,
- Sprawdzenie zaleceń hardeningowych dla danego typu usługi,
- Sprawdzenie domyślnych kont użytkowników w usługach,
- Sprawdzenie aktywnych modułów.

Przygotowanie podstawowych wytycznych do procesu developmentu aplikacji

Zakres prac: przygotowanie dokumentu zawierającego rekomendacje dotyczące konfiguracji stacji deweloperskich oraz kont w platformie GitHub, Google Cloud i Firebase, zmniejszające ryzyko zdeployowania niebezpiecznego kodu do repozytorium.

- Analiza odbędzie się poprzez przeprowadzenie wywiadu z Zamawiającym dotyczącym obecnej konfiguracji i przygotowaniu rekomendacji na ich bazie. Aspekty podlegające badaniu to m.in.:
- Konfiguracja kont deweloperskich,
- Włączone dodatkowe mechanizmy uwierzytelniające (np. 2FA),
- Sposób przechowywania kluczy (*secretów*),
- Używane narzędzia do statycznej analizy kodu,
- Sprawdzenie procesu deployu aplikacji na serwer produkcyjny i stagingowy,

- Proces peer-review.

Weryfikacja pełnego środowiska (w tym CI/CD)

Celem prac jest przeprowadzenie analizy pełnego procesu rozwoju aplikacji (od momentu napisania kodu do jego opublikowania w środowisku produkcyjnym/sklepie aplikacji mobilnych), w celu zidentyfikowania miejsc, w których napastnik jest w stanie umieścić w repozytorium własny złośliwy kod.

Prace zostaną podzielone na następujące dwie części:

Część 1 - Przeprowadzenie analizy środowiska wraz z modelowaniem zagrożeń we współpracy z Zamawiającym. W ramach analizy przeprowadzone zostanie zapoznanie Wykonawcy z środowiskiem pracy Zamawiającego oraz zaimplementowanym procesem CI/CD. Celem analizy jest identyfikacja ryzyk oraz ich klasyfikacja.

Prace będą dotyczyć następujących obszarów:

Sposób zabezpieczenia środowiska pracy Zamawiającego (bezpieczeństwo sieci, bezpieczeństwo stacji roboczych, wdrożone polityki bezpieczeństwa),

Analiza wykorzystywanego procesu CI/CD wraz z sposobami zabezpieczania elementów infrastruktury wykorzystywanych w tym procesie,

Analiza sposobu zabezpieczania infrastruktury służącej do dystrybucji wykorzystanego kodu oraz oprogramowania.

Część 2 - Analiza wyniku modelowania zagrożeń – Wykonawca przygotuje zestawienie wykrytych ryzyk oraz potencjalnych zagrożeń. Wynikiem prac będzie dokument (raport) zawierający zidentyfikowane ryzyka oraz propozycje ich niwelacji.

Analiza integracji z Cloudflare

Zakres prac:

- Analiza danych wysyłanych do serwerów Cloudflare,
- Analiza przyjętego sposobu integracji z Cloudflare,
- Analiza możliwości powiązania danych wysyłanych do serwerów,
- Cloudflare z konkretnym użytkownikiem.

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 +4000 zzs) i przesłanie do Zamawiającego.
9. Przygotowanie szablonów edytowalnych grafik ProteGO Safe i przesłanie do Zamawiającego.

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 obsługą nawigacji w aplikacji, obsługa layoutów.	Do 27.04.2020	
Powiadomienia PUSH z wykorzystaniem Firebase Cloud Messaging	Opracowanie powiadomień PUSH	Opracowanie i dokumentacja typów powiadomień PUSH, wykorzystywanych modeli danych i potrzebnych kanałów dystrybucyjnych	Do 27.04.2020	

		(topiców).		
	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 aplikacji iOS.	Implementacja JS bridge'a w aplikacji iOS.	Do 27.04.2020	
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 MVP aplikacji	Przygotowanie logiki do realizacji kolejnych zadań w projekcie	Do 27/04/2020	
	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 "co mam zrobić"	Do 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 na zgodny z brandbook ministerstwa	Do 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 GitHub. Obrandowanie repozytorium.	Do 27/04/2020	
		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 - security - cloud integration	Do 27/04/2020	280 000 PLN
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 Końcowemu 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 ciągły, również po restarcie telefonu. Obsługa stanów aplikacji i telefonu.	Do 27/04/2020	

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	
	Integracja z częścią serwerową systemu w aplikacji iOS.	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 OP- Backend dla Użytkownika Końcowego potwierdzonego zarażeniem.	Do 27/04/2020	
		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 nowego formularza	Do 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 testowa 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 22/05 /2020	90 000 PLN
Funkcjonalność skanowania kodów QR	1. Wykonanie widoku UI. 2. Obsługa wersji Android i iOS	Aplikacja zyskuje możliwość skanowania kodów QR z przypisanym do niego wynikiem Triageu	Do 22/05 /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 przypisanym do niego wynikiem Triageu	Do 22/05 /2020	
Kody QR	Analiza wymagań i opracowanie flow dla funkcjonalności QR code	Przygotowanie sposobu działania funkcjonalności kodów QR po stronie aplikacji mobilnych do zapewnienia dodania odpowiedniego wpisu w historii kontaktów modułu Bluetooth.	Do 22/05 /2020	

	Implementacja skanowania kodów QR w aplikacji Android	Integracja komunikacji PWA <-> native do przekazywania wymaganych danych do wygenerowania kodu QR (przekazanie aktualnego rotującego identyfikatora Użytkownika Końcowego na żądanie oraz przy każdorazowej zmianie) oraz flow związanego ze skanowaniem kodu QR. Analiza dostępnych rozwiązań do skanowania kodów QR i jego wybór w oparciu o wymagania bezpieczeństwa danych i licencje. Implementacja skanowania kodów QR z wykorzystaniem Bardcode API od Firebase.		
	Implementacja skanowania kodów QR w aplikacji Android	Integracja komunikacji PWA <-> native do przekazywania wymaganych danych do wygenerowania kodu QR (przekazanie aktualnego rotującego identyfikatora Użytkownika Końcowego na żądanie oraz przy każdorazowej zmianie) oraz flow związanego ze skanowaniem kodu QR. Implementacja skanowania kodów QR z		

		wykorzystaniem natywnego rozwiązania.		
Przygotowanie wersji produkcyjnej aplikacji z obsługą kodów QR	Przygotowanie wersji produkcyjnej aplikacji Android z obsługą kodów QR	Wystawienie aplikacji oraz kodu źródłowego aplikacji z obsługą kodów QR		
	Przygotowanie wersji produkcyjnej aplikacji iOS z obsługą kodów QR	Wystawienie aplikacji oraz kodu źródłowego aplikacji z obsługą kodów QR		
Zarządzanie repozytorium GitHub		Ustrukturyzowanie i uporządkowanie repozytorium Aplikacji w serwisie GitHub, która umożliwi zapewnienie transparentności prac nad Aplikacją.	Do 22/05 /2020	

Stworzenie dokumentacji		Dokumentacja developerska projektu PWA - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 22/05 /2020	
Wyczyszczenie repozytorium	dodanie pliku licencji	Ustrukturyzowanie i uporządkowanie repozytorium Aplikacji w serwisie GitHub, która umożliwi zapewnienie transparentności prac nad Aplikacją.	Do 22/05 /2020	
Bug bash 3.1	Przeprowadzenie zbiorowych testów eksploracyjnych aplikacji w wersji 3.1		Do 22/05 /2020	
Dostępność przedstawicieli Wykonawcy	Dostępność przedstawicieli Wykonawcy	Przedstawiciele Wykonawcy dedykowani do realizacji Aplikacji, którzy zostaną potwierdzeni przez Strony w trybie roboczym, będą dostępni dla Zamawiającego w Dni Robocze w godzinach 8:00 - 22:00.	Do 22/05 /2020	

Privacy assessment	Wsparcie Zamawiającego w analizie ryzyka przetwarzania danych w Aplikacji oraz konsultacje privacy by design.	Wsparcie Zamawiającego w analizie ryzyka przetwarzania danych w Aplikacji oraz konsultacje privacy by design. Wprowadzanie stosownych zmian w regulaminie oraz polityce prywatności Aplikacji.	Do 22/05 /2020	

2.4 Etap 4 – wersja aplikacji 4.0

Analiza rozwiązania Exposure Notification (Google + Apple)	Przygotowanie do wdrożenia rozwiązania Exposure Notification	Analiza dokumentacji technicznej Analiza przykładowej implementacji dla aplikacji Android Analiza przykładowej implementacji dla aplikacji iOS Opracowanie zmian architektury systemu w oparciu o rozwiązanie Exposure Notification Spotkania uszczegóławiające z Google oraz Apple	Do 22/05 /2020	369 000 PLN
	Zestawienie środowiska umożliwiającego skorzystanie z wersji Beta API Google dla prac programistycznych przy aplikacji Android	Pobranie i instalacja na urządzeniach testowych odpowiednich wersji binarnych wymaganych aktualizacji aplikacji (Google Play Services)	Do 22/05 /2020	

	Zestawienie środowiska umożliwiającego skorzystanie z wersji Beta API Apple dla prac programistycznych przy aplikacji iOS	Pobranie i instalacja na urządzeniach testowych odpowiednich wersji systemu operacyjnego.	Do 22/05 /2020	
Integracja rozwiązania Exposure Notification	Integracja rozwiązania Exposure Notification w aplikacji Android	Usunięcie modułu OpenTrace z kodu źródłowego. Dodanie do kodu źródłowego zależności w postaci odpowiedniej biblioteki pozwalającej na dostęp do API Google dla Exposure Notification. Implementacja zarządzania działaniem Exposure Notification: weryfikacja wsparcia dla rozwiązania w systemie (sprawdzenie czy telefon ma wymaganą aktualizację Google Play Services, która pozwala na skorzystanie z tej funkcjonalności), wyświetlenie próśb o wymagane pozwolenia, startowanie i zatrzymywanie działania modułu, w tym po restarcie telefonu.	Do 22/05 /2020	

	Integracja rozwiązania Exposure Notification w aplikacji iOS	Usunięcie modułu OpenTrace z kodu źródłowego. Dodanie do kodu źródłowego zależności w postaci odpowiedniej biblioteki pozwalającej na dostęp do API Apple dla Exposure Notification. Implementacja zarządzania działaniem Exposure Notification: weryfikacja wsparcia dla rozwiązania w systemie (sprawdzenie czy telefon ma wymaganą wersję systemu iOS, która pozwala na skorzystanie z tej funkcjonalności), wyświetlenie próśb o wymagane pozwolenia, startowanie i zatrzymywanie działania modułu, w tym po restarcie telefonu.	Do 22/05 /2020	
Przesłanie danych Osoby Chorej (będącej Użytkownikiem Końcowym) do Op-Backend	Upload kluczy (Diagnosis Key) z ostatnich X dni po potwierdzeniu zakażenia w aplikacji Android	Dodanie obsługi wywołania przez PWA rozpoczęcia procesu uploadu danych Użytkownika Końcowego (komunikacja PWA -> native). Wywołanie metody pobierającej z API Google odpowiednie dane (klucze) wymagane do przesłania na serwer, włącznie z obsługą pozwolenia Użytkownika Końcowego i możliwymi	Do 22/05 /2020	

		scenariuszami (błędami), w tym komunikację zwrotną do PWA (komunikacja native -> PWA) Przesłanie danych wraz z podanym przez PWA krótkim kodem weryfikującym na serwer.		
Przygotowanie wersji testowej aplikacji	Przygotowanie wersji testowej aplikacji Android z funkcjonalnością Etapu 4.	Przygotowanie pliku instalacyjnego aplikacji Android do osób testujących.	Do 22/05/2020	
	Przygotowanie wersji testowej aplikacji Android z funkcjonalnością Etapu 4.	Przygotowanie pliku instalacyjnego aplikacji iOS do osób testujących.	Do 22/05/2020	
Analiza rozwiązania Exposure Notification (Google + Apple)	Przygotowanie do wdrożenia rozwiązania Exposure Notification	Analiza dokumentacji technicznej Analiza przykładowej implementacji dla aplikacji Android Analiza przykładowej implementacji dla aplikacji iOS Opracowanie zmian architektury systemu w oparciu o rozwiązanie Exposure Notification Spotkania uszczegóławiające z Google oraz Apple	Do 22/05/2020	
	Zestawienie środowiska umożliwiającego skorzystanie z	Pobranie i instalacja na urządzeniach testowych odpowiednich wersji binarnych wymaganych	Do 22/05/2020	

	wersji Beta API Google dla prac programistycznych przy aplikacji Android	aktualizacji aplikacji (Google Play Services)		
	Zestawienie środowiska umożliwiającego skorzystanie z wersji Beta API Apple dla prac programistycznych przy aplikacji iOS	Pobranie i instalacja na urządzeniach testowych odpowiednich wersji systemu operacyjnego.	Do 22/05 /2020	
Integracja rozwiązania Exposure Notification	Integracja rozwiązania Exposure Notification w aplikacji Android	Usunięcie modułu OpenTrace z kodu źródłowego. Dodanie do kodu źródłowego zależności w postaci odpowiedniej biblioteki pozwalającej na dostęp do API Google dla Exposure Notification. Implementacja zarządzania działaniem Exposure Notification: weryfikacja wsparcia dla rozwiązania w systemie (sprawdzenie czy telefon ma wymaganą aktualizację Google Play Services, która pozwala na skorzystanie z tej funkcjonalności), wyświetlenie próśb o wymagane pozwolenia, startowanie i zatrzymywanie działania modułu, w tym po restarcie telefonu.	Do 22/05 /2020	

	Integracja rozwiązania Exposure Notification w aplikacji iOS	Usunięcie modułu OpenTrace z kodu źródłowego. Dodanie do kodu źródłowego zależności w postaci odpowiedniej biblioteki pozwalającej na dostęp do API Apple dla Exposure Notification. Implementacja zarządzania działaniem Exposure Notification: weryfikacja wsparcia dla rozwiązania w systemie (sprawdzenie czy telefon ma wymaganą wersję systemu iOS, która pozwala na skorzystanie z tej funkcjonalności), wyświetlenie próśb o wymagane pozwolenia, startowanie i zatrzymywanie działania modułu, w tym po restarcie telefonu.	Do 22/05 /2020	
Przesłanie danych pozytywnie zdiagnozowanego Użytkownika Końcowego do serwera		Dokumentacja deweloperska projektu PWA - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 22/05 /2020	
Zarządzanie repozytorium GitHub		Ustrukturyzowanie i uporządkowanie repozytorium Aplikacji w serwisie GitHub, która umożliwi zapewnienie transparentności prac nad Aplikacją.	Do 22/05 /2020	

Stworzenie dokumentacji		Dokumentacja deweloperska projektu PWA - uruchomienie, budowanie aplikacji, schemat przepływu danych	Do 22/05 /2020	
Wyczyszczenie repozytorium	dodanie pliku licencji	Ustrukturyzowanie i uporządkowanie repozytorium Aplikacji w serwisie GitHub, która umożliwi zapewnienie transparentności prac nad Aplikacją.	Do 22/05 /2020	
Bug Bash 4.0	Przeprowadzenie zbiorowych testów eksploracyjnych aplikacji w wersji 4.0		Do 22/05 /2020	
Prepare git repository for contact center		Repozytorium kodu dla aplikacji frontendowej op-backend	Do 22/05 /2020	
Prepare app skeleton		Przygotować szkielet aplikacji z bibliotekami, katalogam.	Do 22/05 /2020	
[Backend] Add login view		Dodanie widoku logowania	Do 22/05 /2020	

Add logic for login to the system		Walidacja danych w formularzu; Wysłanie request do backendu; Obsługa błędów i komunikatów z backendu	Do 22/05 /2020	
[Backend] Query for patients list		Pobieranie listy pacjentów;	Do 22/05 /2020	
[Backend] Add list of patients view		Widok listy pacjentów	Do 22/05 /2020	
List of patients from API		Opracowanie logiki do pobierania i paginowania wyników z API;	Do 22/05 /2020	
Add patient modal view		Dodanie widoku modalnego pacjenta; Otwierany po kliknięciu przycisku “kontakt”, “ponów kontakt”, “zmień” na liście pacjentów	Do 22/05 /2020	
Add patient modal logic		Dodanie logiki dot pobierania danych wyświetlanych na modalu	Do 22/05 /2020	

Add logic, command, endpoint for change patient status buttons			Do 22/05 /2020	
Add create user view		Widok dodawania nowego użytkownika: imię, nazwisko, telefon, email, przycisk zapisz, obsługa błędów (czerwone komunikaty pod każdym polem i “globalne” na górze formularza widok zielonego komunikatu u góry formularza, po poprawnym dodaniu użytkownika;	Do 22/05 /2020	
[OP-BACKEND] Add dashboard and sidebar		Przygotowanie widoku dashboard i sidebar z menu	Do 22/05 /2020	
Prepare cloud function for generate pin code		Funkcja służąca do generowania i zapisywania kodu pin	Do 22/05 /2020	
Create logout button in the left menu			Do 22/05 /2020	

Add logic for generate pin code button		Po naciśnięciu przycisku “wygeneruj” na modalu pacjenta: APIl otrzymuje komunikat aby wygenerować nowy kod pin wyświetla się w miejscu gdzie znajduje się przycisk znika po [parametr] sekundach	Do 22/05/ 2020	
Utrzymanie	Świadczenie Usług Utrzymania	Świadczenie Usług Utrzymania zgodnie z pkt. 5 SOPU	Do 22/05 /2020	
Dostępność przedstawicieli Wykonawcy	Dostępność przedstawicieli Wykonawcy	Przedstawiciele Wykonawcy dedykowani do realizacji Aplikacji, którzy zostaną potwierdzeni przez Strony w trybie roboczym, będą dostępni dla Zamawiającego w Dni Robocze w godzinach 8:00 - 22:00.	Do 22/05 /2020	
Privacy assessment	Wsparcie Zamawiającego w analizie ryzyka przetwarzania danych w Aplikacji oraz konsultacje privacy by design.	Wsparcie Zamawiającego w analizie ryzyka przetwarzania danych w Aplikacji oraz konsultacje privacy by design. Wprowadzanie stosownych zmian w regulaminie oraz polityce prywatności Aplikacji.	Do 22/05 /2020	

2.5 Etap 5 – wersja aplikacji 4.1

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Pobieranie danych pozytywnie zdiagnozowanych osób z serwera	Pobieranie danych pozytywnie zdiagnozowanych osób z serwera w aplikacji Android	Zaimplementowanie metody periodycznego pobierania danych z serwera lub na żądanie przekazane poprzez powiadomienie PUSH. Dane pobierane są jedynie dla nowych wpisów, bazując na ostatnio pobranym najstarszym znaczniku czasowym Osoby Chorej j. Dane przekazywane są dalej do modułu odpowiedzialnego za ich analizę, bez zapisywanie w lokalnej pamięci aplikacji. Pobieranie odbywa się w odpowiednim zadaniu wykonywanym w tle. Pobieranie jest uruchamiane na telefonach wszystkich osób korzystających z aplikacji, którzy mają włączony moduł contact tracing.	Do 10 dni od opublikowania stosownej dokumentacji API G+A	365 900 PLN
Zarządzanie repozytorium GitHub	Pobieranie danych pozytywnie zdiagnozowanych osób z serwera w aplikacji iOS	Zaimplementowanie metody periodycznego pobierania danych z serwera lub na żądanie przekazane poprzez powiadomienie PUSH. Dane pobierane są jedynie dla nowych wpisów, bazując na ostatnio pobranym najstarszym znaczniku czasowym Osoby Chorej . Dane przekazywane są dalej do modułu	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

		odpowiedzialnego za ich analizę, bez zapisywanie w lokalnej pamięci aplikacji. Pobieranie odbywa się w odpowiednim zadaniu wykonywanym w tle. Pobieranie jest uruchamiane na telefonach wszystkich osób korzystających z aplikacji, którzy mają włączony moduł contact tracing.		
Analiza danych pozytywnie zdiagnozowanych osób	Uruchomienie i pobranie wyników analizy ryzyka przeprowadzanej przez rozwiązanie Exposure Notification od Google w aplikacji Android	Przeprowadzenie w odpowiednim zadaniu działającym w tle procesu analizy danych przy użyciu Exposure Notification.	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
Obsługa wyników analizy danych pozytywnie zdiagnozowanych osób	Powiadomienie użytkownika o wyniku analizy w aplikacji Android	Dla wyników spełniających kryteria konieczności poinformowania użytkownika o tym fakcie aplikacja wyświetla notyfikację systemową z odpowiednią informacją. Po kliknięciu w notyfikację użytkownik przenoszony jest do aplikacji.	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

	Powiadomienie użytkownika o wyniku analizy w aplikacji iOS	Dla wyników spełniających kryteria konieczności poinformowania użytkownika o tym fakcie aplikacja wyświetla notyfikację systemową z odpowiednią informacją. Po kliknięciu w notyfikację użytkownik przenoszony jest do aplikacji.	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
	Przekazanie wyników analizy do PWA w aplikacji Android	Przekazanie wyników analizy do PWA (komunikacja native -> PWA) w przypadku gdy: - aplikacja jest otwarta w momencie zakończenia analizy - na żądanie PWA kiedy aplikacja zostanie uruchomiona przez użytkownika.	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
	Przekazanie wyników analizy do PWA w aplikacji iOS	Przekazanie wyników analizy do PWA (komunikacja native -> PWA) w przypadku gdy: - aplikacja jest otwarta w momencie zakończenia analizy - na żądanie PWA kiedy aplikacja zostanie uruchomiona przez użytkownika.	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

Przygotowanie do publikacji	Weryfikacja poprawności działania rozwiązania Exposure Notification dla aplikacji Android	Przygotowanie wersji testowej aplikacji z wdrożonym Exposure Notification. Wdrożenie odpowiednich rozwiązań wspomagających testowanie (np. eksport logów do pliku tekstowego) Testy deweloperskie przeprowadzone w kilkudniowym okresie czasowym z uwzględnieniem obserwacji poprawności działania zadań wykonywanych w tle (pobieranie danych, analiza danych, obsługa wyników), w tym podczas niskiej aktywności urządzenia (tryb uśpienia).	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
	Weryfikacja poprawności działania rozwiązania Exposure Notification dla aplikacji iOS	Przygotowanie wersji testowej aplikacji z wdrożonym Exposure Notification. Wdrożenie odpowiednich rozwiązań wspomagających testowanie (np. eksport logów do pliku tekstowego) Testy deweloperskie przeprowadzone w kilkudniowym okresie czasowym z uwzględnieniem obserwacji poprawności działania zadań wykonywanych w tle (pobieranie danych, analiza danych, obsługa wyników), w tym podczas niskiej aktywności urządzenia (tryb uśpienia).	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

Publikacja aplikacji	Publikacja aplikacji Android w sklepie Google Play.	Przygotowanie wersji release aplikacji, wdrożenie wersji produkcyjnej do sklepu, obsługa releasów wersji pośrednich (z poprawkami błędów i nowymi zmianami).	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
	Publikacja aplikacji iOS w sklepie Apple App Store.	Przygotowanie wersji release aplikacji, wdrożenie wersji produkcyjnej do sklepu, obsługa releasów wersji pośrednich (z poprawkami błędów i nowymi zmianami).	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
Periodically pushing notifications		Funkcjonalność potrzebna aby aplikacja się wybudziła i mogła przesłać info do blackbox z nowymi diagnosis key	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

[Backend] Deploy and configure cloud functions on prod env		Konfiguracja i deploy środowiska produkcyjnego	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[Backend] Store uploaded diagnosis keys		Funkcjonalność, która umożliwia sprawdzenie poprawności tokenu JWT i zapis danych w postaci pliku .json na Firebase Storage	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[Bckend] Add readme as short project documentation		Dodać readme w którym będzie krótka dokumentacja jak uruchomić / skonfigurować projekt	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

[Backend] Add license to the cloud backend		Dodać licencję do projektu	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[Backend] Prepare auth for cloud functions		Dodać funkcjonalność autoryzacji za pomocą tokenu albo innej wybranej w r&d metody; aktualnie cloud functions są dostępne dla każdego użytkownika;	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[Backend] Deploy cloud functions on test environment			Do 10 dni od opublikowania stosownej dokumentacji API G+A	

[Backend] Add injecting backend url in the CI/CD		Dodanie zmiennej url backendu podczas budowania albo deploy'u aplikacji;	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[CLOUD-Backend] Add basic validation for https cloud functions		Dodanie walidacji poprawności formatów danych wejściowych;	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[CLOUD-Backend] Additional security for generating pin codes		"Stworzenie zabezpieczenie wpuszczające określone IP; Dodanie konfiguracją jako tablica white IP i wrzucić do konfiguracji aplikacji;"	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

[CLOUD-Backend] Add getAccessToken function		Wykonanie zadania wymiany PIN za JWT który zostanie później wykorzystany do upload danych	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[PWA + BACKEND] Add advices		Wykonanie zmiany: umieścić dane z https://www.gov.pl/web/koronawirus/porady (colapse) w zakladce porady (pod obecnymi poradami)	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[Backend] Prepare repository for cloud backend		Przygotowanie repozytorium do Cloud Backend	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

[Backend] Create logout button in the left menu			Do 10 dni od opublikowania stosownej dokumentacji API G+A	
Move qr codes commits to the other branch		Przeniesienie comitów QR kodowych do nowego brancha 3.1.0-qr-codes	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[Backend] Add exceptions handler		Łapanie wyjątków i ich prezentacja w formie JSON	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

Prepare worker for clearing unused pin codes		Przygotowanie algorytmu, który będzie analizował kody PIN i w określonych odstępach czasu usuwał przedawnione kody	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[CLOUD-BACKEND] Analyze exposure-notifications-server		Wykonanie analizy rozwiązania exposure-notifications-server	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[CLOUD-Backend] Change uploading diagnosis keys logic		Wykonanie zmiany logiki sposobu uploadu diagnosis key	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

[Backend] Add create user functionality		Add create user endpoint, logic and command	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
Bug bash 4.1	Przeprowadzenie zbiorowych testów eksploracyjnych aplikacji w wersji 4.1		Do 10 dni od opublikowania stosownej dokumentacji API G+A	
Utrzymanie	Świadczenie Usług Utrzymania	Świadczenie Usług Utrzymania zgodnie z pkt. 5 SOPU	Do 30/06/2020	

Dostępność przedstawicieli Wykonawcy	Dostępność przedstawicieli Wykonawcy	Przedstawiciele Wykonawcy dedykowani do realizacji Aplikacji, którzy zostaną potwierdzeni przez Strony w trybie roboczym, będą dostępni dla Zamawiającego w Dni Robocze w godzinach 8:00 - 22:00.	Do 30/06/2020	
Privacy assessment	Wsparcie Zamawiającego w analizie ryzyka przetwarzania danych w Aplikacji oraz konsultacje privacy by design.	Wsparcie Zamawiającego w analizie ryzyka przetwarzania danych w Aplikacji oraz konsultacje privacy by design. Wprowadzanie stosownych zmian w regulaminie oraz polityce prywatności Aplikacji.	Do 30/06/2020	
[Backend] Add injecting backend url in the CI/CD		Dodanie zmiennej url backendu podczas budowania albo deploy'u aplikacji;	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

[CLOUD-Backend] Add basic validation for https cloud functions		Dodanie walidacji poprawności formatów danych wejściowych;	Do 10 dni od opublikowania stosownej dokumentacji API G+A	
[CLOUD-Backend] Additional security for generating pin codes		"Stworzenie zabezpieczenie wpuszczające określone IP; Dodanie konfiguracją jako tablica white IP i wrzucić do konfiguracji aplikacji;"	Do 10 dni od opublikowania stosownej dokumentacji API G+A	

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 22/05 /2020	
Wstępna analiza rynku	Zidentyfikowanie urządzeń niezbędnych do pokrycia testami interfejsu Użytkownika Końcowego		Do 22/05 /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 22/05 /2020	
Dokumentacja testowa	Przygotowanie macierzy urządzeń		Do 22/05 /2020	
Testy eksploracyjne i zdrowotne	Testy eksploracyjne i zdrowotne aplikacji PWA, Android i iOS		Do 22/05 /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 22/05 /2020	
Monitoring środowisk	Skonfigurowanie narzędzia do monitorowania stanu środowiska produkcyjnego i przedwdrożeniowego		Do 22/05 /2020	
Automatyczna weryfikacja	Skrypt weryfikujący poprawność działania podstawowej ścieżki w aplikacji PWA		Do 22/05 /2020	
Testowanie zadań	Testowanie zadań wykonanych przez zespół deweloperski		Do 22/05 /2020	
Analiza rynku urządzeń mobilnych	- Analiza dostępnych raportów odnośnie urządzeń mobilnych - Zidentyfikowanie najpopularniejszych		Do 22/05 /2020	120 000 zł

	urządzeń na rynku		
Dokumentacja testowa	Stworzenie planu testów	Do 22/05/2020	
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 22/05/2020	

2.7 Etap 7 – Założenia cyberbezpieczeństwa

Nazwa zadania	Zakres techniczny	Opis funkcjonalny	Data wykonania	Wycena
Etap 1	Testy penetracyjne elementów infrastruktury (m.in. VM) [blackbox] Testy penetracyjne aplikacji PWA (safesafe.app) [blackbox] Testy penetracyjne API wystawianego przez GCP VM (api.safesafe.app) [blackbox] Testy penetracyjne i analiza bezpieczeństwa aplikacji Android i iOS [blackbox] Podstawowa analiza kodu aplikacji mobilnych [whitebox] Przygotowanie wytycznych do procesu developmentu aplikacji [analysis],		do 22.05.2020	62 500 zł
Etap 2	Weryfikacja pełnego środowiska (w tym CI/CD) [whitebox] Analiza konfiguracji Google Cloud Platform i Firebase [whitebox] Testy penetracyjne modułu do wysyłki PIN [blackbox], Testy penetracyjne aplikacyjne Operator Backend [blackbox], Testy penetracyjne infrastruktury Operator Backend [blackbox], Testy penetracyjne aplikacyjne Cloud Backend [blackbox], Testy penetracyjne infrastruktury Cloud Backend [blackbox],		do 25.05.2020	274.100 zł

	Testy obciążeniowe DDoS – dla dwóch adresów IP, Hardening konfiguracji GCP VM (1 serwer) [whitebox], OPCJONALNIE – retest obszarów z poprawkami po pierwszym etapie.		
Infrastruktura i Security	Weryfikacja bezpieczeństwa: - logiki aplikacji - logiki komunikacji aplikacji z pozostałymi rozwiązaniami - rozwiązania infrastrukturalnego - kodu źródłowego aplikacji	Do 10 dni od opublikowania stosownej dokumentacji API G+A	100 000 zł

2.8 Etap 8 – Komunikacja Aplikacji

Etap 8 – Komunikacja Aplikacji

Nazwa zadania	**Zakres techniczny**	**Opis funkcjonalny**	**Data wykonania**	**Wycena**

Stworzenie logo	Warsztat projektowy analizujący komunikacje celem przygotowania brandingu Aplikacji. Stworzenie 3 wersji nowego logotypu w oparciu o wytyczne. Wdrożenie 2 cykli poprawek do wybranej wersji logo. Prezentacja pomysłów graficznych jak rozwinąć propozycje logo (szkic Key Visuala)	Do 22/05 / 2020	20 000 zł
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 Przygotowanie paczki z logotypami w formatach .png .jpg i .pdf, Stworzenie key visual w oparciu o materiały gov.pl	Do 22/05 / 2020	30 000 zł
Stworzenie grafik marketingowych		Do 22 05/2020	10 000 zł
Stworzenie diagramu przepływu danych	Optymalizacja fanpage pod kątem informacji o projekcie ProteGO Safe Zaprojektowanie 3 głównych grafik w 45 formatach (PR,Social Media) wg wytycznych od Zamawiającego w celu komunikacji o projekcie ProteGO Safe Wizualne zobrazowanie przepływu danych na diagramach dla rozwiązań: - HLD OpenTrace - HLD API G+A	Do 22/05 / 2020	20 000 zł

	- Stany aplikacji		
Obsługa komunikacji w sklepach z aplikacjami (Google Play Store oraz Apple App Store)	Zaprojektowanie serii grafik w 2 formatach dla umieszczenia aplikacji w Google Store i Apple Store, Przygotowanie opisów aplikacji dla umieszczenia aplikacji w Google Store i Apple Store (w sumie +4000 zzs) i przesłanie do Zamawiającego. Przygotowanie szablonów edytowalnych grafik ProteGO Safe i przesłanie do Zamawiającego Obsługa komentarzy w sklepach z aplikacjami (Google Play Store oraz Apple App Store).	Do 30/06/2020	15 000 zł

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.

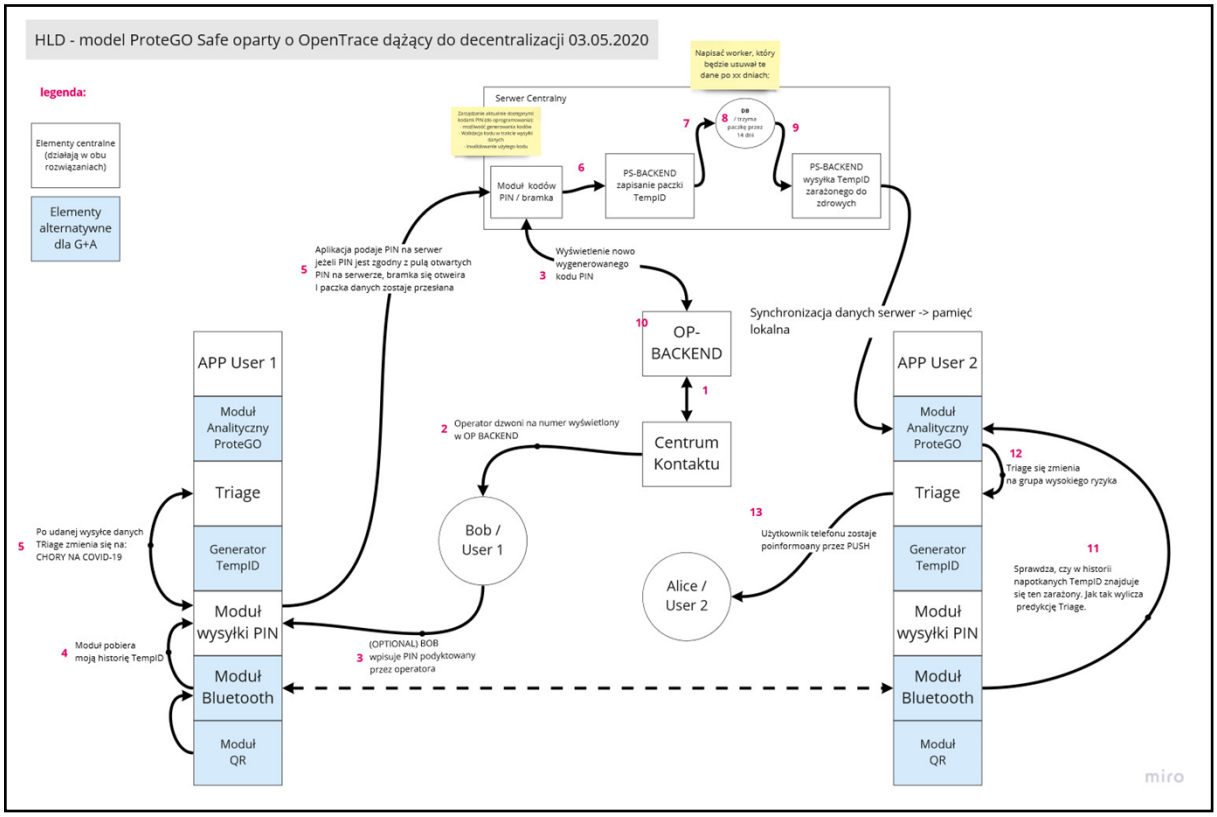
3.1. Testy manualne i maszynowe

Nazwa zadania	**Zakres techniczny**	**Opis funkcjonalny**	**Data wykonania**	**Wycena**
Testowanie zadań	Testowanie zadań wykonanych przez zespół deweloperski		Do 22/05 /2020	
Wstępna analiza rynku	Zidentyfikowanie urządzeń niezbędnych do pokrycia testami interfejsu Użytkownika Końcowego		Do 22/05 /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 22/05 /2020	
Dokumentacja testowa	Przygotowanie macierzy urządzeń		Do 22/05 /202020	
Testy eksploracyjne i zdrowotne	Testy eksploracyjne i zdrowotne aplikacji PWA, Android i iOS		Do 22/05 /2020	120 000 zł

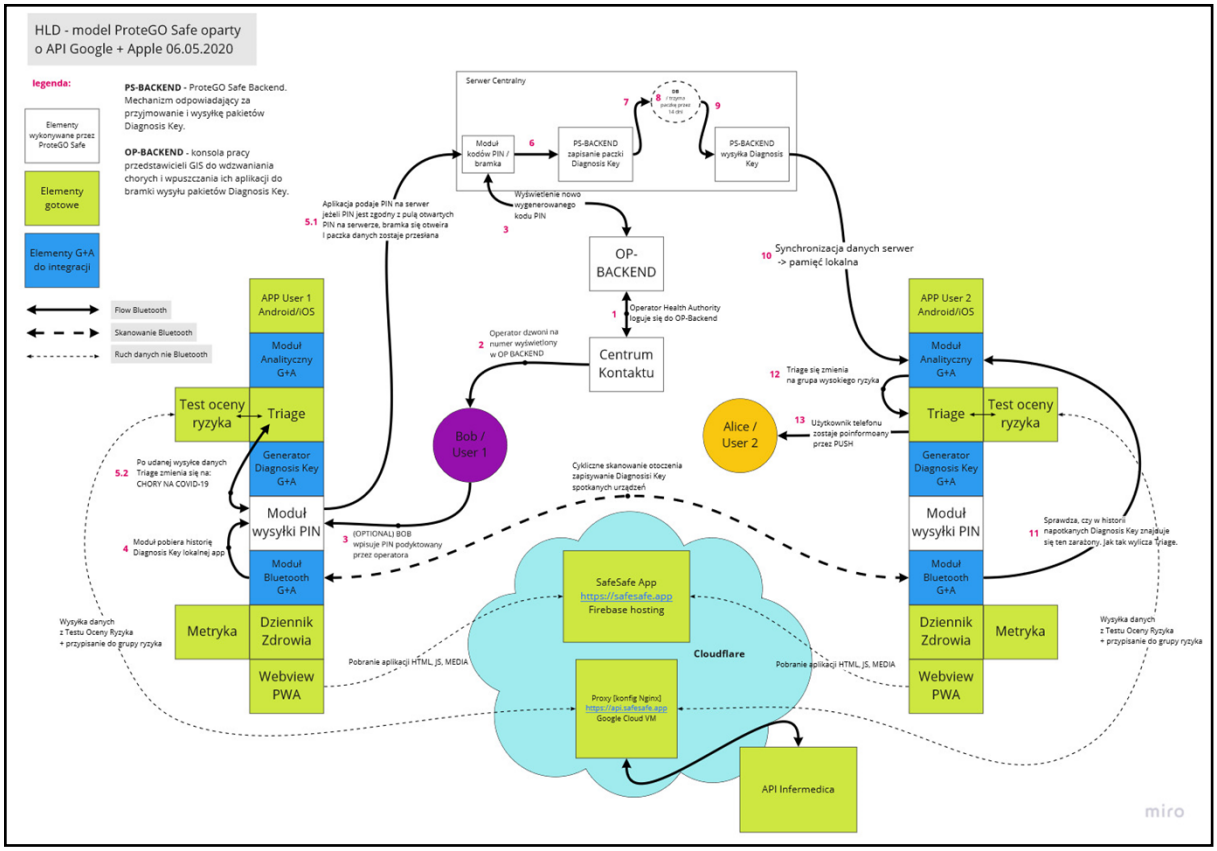
Automatyczna weryfikacja dymna	Przeprowadzenie testów kompatybilności z urządzeniami i wersjami platform o najwyższym priorytecie poprzez uruchomienie testów dymnych z wykorzystaniem narzędzi typu Crawler	Do 22/05 /2020	
Monitoring środowisk	Skonfigurowanie narzędzia do monitorowania stanu środowiska produkcyjnego i przedwdrożeniowego	Do 22/05 /2020	
Automatyczna weryfikacja	Skrypt weryfikujący poprawność działania podstawowej ścieżki w aplikacji PWA	Do 22/05 /2020	
Testowanie zadań	Testowanie zadań wykonanych przez zespół deweloperski	Do 22/05 /2020	
Analiza rynku urządzeń mobilnych	- Analiza dostępnych raportów odnośnie urządzeń mobilnych - Zidentyfikowanie najpopularniejszych urządzeń na rynku	Do 22/05 /2020	
Dokumentacja testowa	Stworzenie planu testów	Do 22/05 /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 22/05 /2020	

4. Architektura rozwiązania

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



Rys. 1 - diagram High Level Design dla modelu OpenTrace



Rys. 2 - Diagram High Level Design dla modelu API Google + Apple

5. Utrzymanie

1. W ramach realizacji Umowy Wykonawca odpowiada za utrzymanie działania Aplikacji (dalej: Usługi Utrzymania).
2. Celem Usług Utrzymania jest zapewnienie Zamawiającemu zgodnego z Umową nieprzerwanego działania Aplikacji.
3. Strony niniejszym wzajemnie potwierdzają, że opisanie w niniejszym pkt. zasady Utrzymania Aplikacji będą miały zastosowanie dla limitu 1.000.000 (słownie: miliona) pobranych aplikacji. W przypadku przekroczenia limitu, o którym mowa w zdaniu poprzedzającym Strony przystąpią w dobrej wierze do renegocjacji warunków Usług Utrzymania Aplikacji. Jeżeli w ciągu 30 dni Strony nie osiągną porozumienia w tym zakresie Wykonawca będzie uprawniony do otrzymania dodatkowego wynagrodzenia w wysokości 500 zł netto za każde 10.000 pobranych aplikacji ponad pierwszy 1 milion
4. Usługi Utrzymania świadczone będą w Dni Robocze z uwzględnieniem czasu reakcji na Błędy Krytyczne (zgodnie z tabelą poniżej) również w dni wolne od pracy.
5. Usługi Utrzymania obejmują:
    5.1. świadczenie usług SLA, w ramach których Wykonawca zobowiązuje się do:
        5.1.1. obsługi zgłoszeń, zgodnie z zasadami opisanymi w niniejszym pkt. 5 SOPU , a w tym do:
            5.1.1.1. reakcji na zgłoszenia błędów w czasie reakcji;
            5.1.1.2. podejmowania działań zmierzających do obejścia dla błędów występujących z przyczyn leżących po stronie Infrastruktury Zamawiającego w czasie naprawy*;*
            5.1.1.3. usuwania Błędów w czasie naprawy;
        5.1.2. udzielania dostępu do nowych wersji Aplikacji / przygotowywania patchy w związku z wykrytymi Błędami.
    5.2. zapewnienia dostępności Aplikacji, zgodnie z zasadami opisanymi w niniejszym pkt. 5 SOPU w trakcie okresu Utrzymania;
    5.3. zapewnienia zgodności Aplikacji z Toolboxem oraz przepisami prawa obowiązującymi w Polsce;
    5.4. tzw. małego rozwoju Aplikacji oznaczającego niewielkie prace rozwojowe inicjowane przez Wykonawcę, które mają na celu zwiększenie efektywności i stabilności Aplikacji, a także komfortu jej używania przez Użytkowników Końcowych.
    5.5. zapewnić tzw. drugą linię wsparcia technicznego realizowaną na rzecz operatorów Centrum Kontaktu w zakresie odpowiadania na uwagi i błędy zgłaszane przez Użytkowników Końcowych. Operatorzy Centrum Kontaktu będą zgłaszali przedmiotowe uwagi i błędy za pośrednictwem systemu do zgłaszania ticketów klasy “Bug Tracker”. W przypadku świadczenia usług drugiej linii wsparcia na rzecz operatorów Centrum Kontaktu stosuje się odpowiednio zasady i terminy określone w niniejszym paragrafie dla Błędów Wydajności.
6. W celu uniknięcia wątpliwości Strony potwierdzają, że Usługami Utrzymania objęte są wszelkie elementy Aplikacji, w tym również w szczególności wszelkie elementy Aplikacji, zapewnione przez Wykonawcę w ramach realizacji Aplikacji.

7. Wszelkie aktualizacje, update'y, poprawki, patche, nowe wersje etc. Aplikacji, dostarczone lub wykonane przez Wykonawcę w ramach Usług Utrzymania (w tym w ramach usuwania Błędów), zawierać będą także kody źródłowe takich aktualizacji, update'ów, poprawek, patchy, nowych wersji etc.
8. Niezależnie od dalej idących postanowień Umowy, w tym regulujących prawa własności intelektualnej, Zamawiający jest uprawniony do samodzielnego wykorzystania lub do przekazania osobie trzeciej, w celu zapewnienia przejęcia Usług Utrzymania, wszelkich dokumentów, prezentacji, rezultatów prac Wykonawcy otrzymanych w ramach realizacji Umowy oraz Dokumentacji.
9. 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 deweloperskiego zaangażowanego w projekt. W ramach podanej kwoty realizacji umowy Wykonawca nie będzie wykonywał nowych funkcjonalności, nie określonych w niniejszym SOPU.
10. Zespół świadczący Usługi Utrzymania będzie składał się z co najmniej dziewięciu osób:
    10.1. dwóch programistów Swift (iOS),
    10.2. dwóch programistów Kotlin (Android),
    10.3. dwóch programistów ReactJS / ReactNative,
    10.4. dwóch specjalistów DevSecOps,
    10.5. managera projektu.
11. W ramach Usług Utrzymania Aplikacji Wykonawca zobowiązuje się do:
    11.1. usuwania błędów Aplikacji;
    11.2. udzielania dostępu do nowych wersji Aplikacji;
    11.3. przyjmowania zgłoszeń za pośrednictwem:
        11.3.1. poczty elektronicznej na adres e-mail: support@tytani24.com;
        11.3.2. systemu do zgłoszeń błędów, o którym mowa w pkt. 4.5.
12. Na potrzeby realizacji Usług Utrzymania wprowadza się następujące klasyfikacje błędów:

Rodzaj problemu	**Opis**	**Czas reakcji od momentu odebrania zgłoszenia**	**Czas na usunięcie błędu (Czas Naprawy)**
Błąd Krytyczny	zdarzenie uniemożliwiające poprawne lub całkowite wykonanie operacji w Aplikacji przez ponad 10% aktywnych Użytkowników Końcowych lub całkowity brak dostępu do lub utrata danych znajdujących się w bazie danych serwera Aplikacji przetwarzania danych lub praca Systemu, niezgodna z dokumentacją. Po udostępnieniu rozwiązania czasowego pozwalającego na realizację błędnie działającej usługi (wdrożeniu obejścia) błąd krytyczny będzie traktowany jak Błędy Wydajności i zostanie usunięty ostatecznie w terminie dla Błędu Wydajności	2h w Dni Robocze, do 4h w pozostałych porach i w dni wolne od pracy	do 8h po w Dni Robocze, do 16h w pozostałych porach i w dni wolne od pracy od momentu zakończenia czasu reakcji.
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 Błędy drobne, błędy ergonomiczne lub konieczność zbędnych „kliknięć” w celu uzyskania pożądanego przez Użytkownika Końcowego rezultatu, itp.).	do 24 godzin	do 5 Dni Roboczych

Błąd wyglądu	zdarzenie pogorszenia estetyki i spójności interfejsu graficznego Aplikacji, kosmetyczne błędy (np. format pól, brak walidacji, literówki, błędne nazwy)	do 24 godzin	do 5 Dni Roboczych
Dni Robocze w rozumieniu niniejszego pkt. 5 SOPU oznaczają dni od poniedziałku do piątku (z wyłączeniem dni ustawowo wolnych od pracy) w godz. 9:00 - 19:00. Jeżeli błąd został zgłoszony w Dniu Roboczym to oznacza, że jest realizowany w ramach ustaleń obsługi błędów Dnia Roboczego.			

13. Zgłoszenie błędu 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.

14. Korespondencja elektroniczna będzie odbierana przez Wykonawcę w Dni Robocze w godzinach 09:00-20:00.
15. Jeżeli usunięcie błędu nie będzie możliwe w założonym czasie, Wykonawca niezwłocznie poinformuje o tym fakcie Zamawiającego.
16. Wykonawca zobowiązuje się do wykonywania zgłoszeń Zamawiającego z należytą starannością oraz z priorytetem pierwszeństwa.
17. Klasyfikacja błędu może zostać zmieniona przez Wykonawcę po konsultacji z Zamawiającym.
18. Zobowiązania Wykonawcy nie obejmują błędów wynikających ze współpracy Aplikacji z innymi połączonymi systemami nie będącymi w utrzymaniu Wykonawcy.
19. Zamawiający zobowiązuje się do współpracy z Wykonawcą przy diagnozowaniu błędów i udzielenia wszelkich niezbędnych informacji, w terminie nie dłuższym niż D zień Roboczy w przypadku Błędów Krytycznych, a w przypadku każdego innego błędu

w terminie nie dłuższym niż 3 Dni Robocze. Czas usunięcia błędów przez Wykonawcę ulega przesunięciu o czas oczekiwania na udzielenie odpowiedzi przez Zamawiającego.

20. 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 Końcowych, 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 Końcowego.
3. Strony ustalają następującą kategorie błędów:
   a) błąd krytyczny - zdarzenie uniemożliwiające poprawne lub całkowite wykonanie operacji w Aplikacji przez ponad 10% aktywnych Użytkowników Końcowych 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.

Signed by /
Podpisano przez:

Mateusz Romanów

Date / Data: 2020-05-21 18:09