BARTA LITWIŃSKI
KANCELARIA
RADCÓW PRAWNYCH
I ADWOKATÓW
SPÓŁKA PARTNERSKA

Raport z audytu prywatności aplikacji ProteGO Safe przeprowadzonego na zlecenie Ministerstwa Cyfryzacji

sporządzony w Krakowie dnia 5 sierpnia 2020 roku

PRZEDMIOT RAPORTU

Przedmiotem wykonanego audytu prywatności jest ocena prawna zgodności działania aplikacji ProteGo Safe z obowiązującym prawem ochrony danych osobowych.

Audyt prywatności został przeprowadzony na zlecenie Ministerstwa Cyfryzacji Rzeczpospolitej Polskiej (dalej jako „**Ministerstwo**") przez zespół audytowy z kancelarii Barta Litwiński Kancelaria Radców Prawnych i Adwokatów Spółka Partnerska z siedzibą w Krakowie (dalej jako „**Kancelaria**"). Prace audytowe rozpoczęły się w dniu 3 czerwca 2020 r., a niniejszy raport stanowiący podsumowanie całości prac został sporządzony w dniach 27 lipca do 5 sierpnia 2020 r.

Przy wykonywaniu oceny prawnej, w szczególności w zakresie oceny implementacji rozwiązań dotyczących przejrzystości komunikacji z użytkownikiem, korzystano z aplikacji ProteGo Safe w wersji 4.2.2. W toku przeprowadzonej analizy wykorzystano zarówno urządzenia pracujące w systemie operacyjnym iOS, jak również urządzenia pracujące w systemie Android.

Zlecony audyt prywatności obejmował sprawdzenie zgodności funkcjonowania aplikacji ProteGo Safe z obowiązującym prawem ochrony danych osobowych, w tym w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; dalej jako „**RODO**") oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781), jak również innymi przepisami prawa powszechnie obowiązującego, w tym m.in. przepisami ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t. j. Dz. U. z 2019 r. poz. 2460, z 2020 r. poz. 374, 695, 875). W toku oceny pod uwagę wzięte zostały również wytyczne i zalecenia, w tym:

- EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic — 14/04/2020;
- Mandate on geolocation and other tracing tools in the context of the COVID-19 outbreak — 07/04/2020;

- Statement on the data protection impact of the interoperability of contact tracing apps - 16/06/2020;
- Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data
- Communication from the Commission: Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01);
- eHealth Network: Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States;
- 7 Filarów Zaufania Panoptykonu.

Przedmiotem niniejszego raportu jest przedstawienie wyników przeprowadzonej analizy, w tym wskazanie nieprawidłowości wykrytych w związku z przeprowadzeniem audytu prywatności aplikacji.

METODA SPORZĄDZANIA RAPORTU

Zasadnicza część raportu zawiera tabele, w których przedstawiono wyniki analizy w zakresie przetwarzania danych osobowych, a także sugestie zmian w aplikacji. W tabeli ujęto ponadto schematycznie ocenę ryzyka wystąpienia nieprawidłowości w zakresie przetwarzania danych osobowych z wykorzystaniem aplikacji ProteGo Safe, z założeniem, że nieprawidłowości niosące największe ryzyko powinny być usunięte niezwłocznie, a wszystkie nieprawidłowości, niezależnie od stwierdzonego stopnia ryzyka, winny podlegać usunięciu w najbliższym możliwie terminie.

Przyjęta przez Kancelarię metodyka szacowania ryzyka, zastosowana podczas przeprowadzania audytów oraz sporządzania raportów poaudytowych polega na wyszczególnieniu aktywów, dokonaniu analizy zagrożeń wpływających na poszczególne aktywa, dopasowaniu adekwatnych środków technicznych i/lub organizacyjnych, które mają za zadanie przeciwdziałać zidentyfikowanym zagrożeniom i prawdopodobieństwu ich wystąpienia, a w konsekwencji zabezpieczać realizacje celów i chronić podmioty danych przed negatywnym wpływem czynników wewnętrznych i zewnętrznych na przeprowadzane procesy przetwarzania danych.

W zależności od dotkliwości przewidywanych skutków zidentyfikowanych nieprawidłowości (krytyczności zagrożeń) i w odniesieniu do prawdopodobieństwa wystąpienia tych skutków, uwzględniając poziom uciążliwości związanej z przeprowadzaniem działań naprawczych, których efektem miałoby być wdrożenie zaproponowanych w raporcie rozwiązań, ustalono czterostopniową ocenę ryzyka, o następującej skali:

- wysokie ryzyko (rekomendowane bezzwłoczne usunięcie nieprawidłowości);
- średnie ryzyko (nie jest konieczne natychmiastowe usunięcie nieprawidłowości, jednak zaleca się ich usunięcie w najbliższym możliwym terminie);
- niskie ryzyko (rekomendowane usunięcie);
- BRAK - nie zidentyfikowano występowania ryzyka w ramach analizowanego zagadnienia lub podatności.

Artykuł 32 ust. 1 RODO wskazuje, że wdrażanie jakichkolwiek środków technicznych lub organizacyjnych, mających na celu zapewnienie odpowiedniego stopnia bezpieczeństwa ma się odbywać z uwzględnieniem celów przetwarzania oraz ryzyka wystąpienia naruszeń, zależnego od prawdopodobieństwa wystąpienia oraz wagi zidentyfikowanych zagrożeń. Odpowiedni stopień bezpieczeństwa ustalany jest w oparciu o dokonaną ocenę ryzyka. By działania takie były możliwe, w pierwszej kolejności należy w sposób dokładny i metodyczny dokonać identyfikacji i opisu procesów przetwarzania danych oraz przyporządkować im odpowiednie aktywa, na które wpływ będą miały zagrożenia, które następnie będą podlegać ocenie z punktu widzenia. Dopiero w oparciu o przygotowany opis procesu przetwarzania możliwa będzie identyfikacja i przyporządkowanie do niego konkretnych zagrożeń oraz dokładna ocena prawdopodobieństwa ich wystąpienia i skutków, jakie może ono wywrzeć na osiągnięcie zakładanych celów przetwarzania oraz na ochronę praw i wolności osób, których dane dotyczą.

Uwzględniając powyższe oraz fakt, że holistyczne ujęcie przetwarzania danych jako całości (jednego procesu) nie pozwala na dokonanie skutecznej i właściwej analizy ryzyka dla przetwarzania danych osobowych, przekazany Państwu raport poaudytowy, tj. zestawienie stwierdzonych nieprawidłowości w przetwarzaniu danych osobowych został podzielony na działy, odpowiadające procesom przetwarzania danych, a w niektórych przypadkach nawet na konkretne operacje przetwarzania w ramach istniejących procesów.

PODSUMOWANIE USTALEŃ AUDYTOWYCH I WNIOSKI

Przeprowadzony audyt prywatności ProteGO Safe pozwolił na dokładną weryfikację projektu pod kątem ochrony danych osobowych i bezpieczeństwa informacji. Przy analizie wykorzystano źródła pozaprawne, co pozwoliło na dokonanie oceny ProteGO Safe nie tylko pod kątem zgodności z przepisami powszechnie obowiązującymi, ale również z wymogami stawianymi przez organy publiczne, środowisko i użytkowników aplikacji.

Projekt ProteGO Safe od momentu pierwszego wdrożenia do wydania wersji 4.2.2. uległ dużym zmianom, podyktowanym przede wszystkim chęcią ochrony informacji pozyskiwanych i przetwarzanych przez aplikację oraz podmioty odpowiedzialne oraz koniecznością zapewnienia bezpieczeństwa użytkowników przy jednoczesnym zagwarantowaniu pełnej funkcjonalności i operacyjności oraz powszechności i dostępności rozwiązania.

Dbałość o przejrzystość działań podmiotów odpowiedzialnych, w tym GIS i Ministerstwa Cyfryzacji, widoczna jest przede wszystkim w krokach podjętych na rzecz zapewnienia jawności, w tym: publikacji kodu źródłowego aplikacji, publikacji ustaleń z testów i retestów bezpieczeństwa, publikacji arkusza Oceny skutków dla ochrony danych (DPIA). Ustalone cele operacyjne ProteGO Safe pokrywają się z zadaniami realizowanymi w interesie publicznym przez GIS. Wskazane podstawy prawne przetwarzania danych uznawane są przez organy publiczne, w tym Komisję Europejską, za podstawy stabilne.

Zastosowano szereg rozwiązań technicznych gwarantujących poufność i bezpieczeństwo danych osobowych i informacji nieosobowych przetwarzanych w ramach aplikacji, w tym:

- szyfrowanie i pseudonimizacja, również w zakresie identyfikatorów użytkowników;
- anonimizacja danych i uniemożliwienie dostępu do większości danych organom państwowym oraz podmiotom trzecim, w tym w szczególności rezygnacja z technologii opartych na geolokalizacji (GPS) i transferach danych za pomocą sieci bezprzewodowych WiFi i sieci komórkowych na rzecz technologii zbliżeniowych opartych na komunikacji Bluetooth;

- wykorzystanie Exposure Notification API Google i Apple oraz technologii od Cloudflare dla zapewnienia poufności oraz ochrony przed atakami DDOS;
- hybrydowy model przetwarzania, który w dominującej części korzysta z zalet modelu zdecentralizowanego (w szczególności w zakresie lokalnego przechowywania danych wprowadzonych do aplikacji ProteGO Safe), co w konsekwencji oznacza przekazanie kontroli nad przetwarzanymi danymi osobie, której dane dotyczą (szczególnie w zakresie usuwania danych osobowych).

Istotne jest również wykorzystywanie technologii wspierających powszechny charakter ProteGO Safe, przyjaznych użytkownikowi. W tym zakresie na szczególną uwagę zasługuje:

- fakt przystosowania ProteGO Safe do korzystania z technologii Bluetooth Low Energy (BLE), która ogranicza zużycie energii w urządzeniu;
- dostosowanie aplikacji do funkcjonowania w systemach operacyjnych największych dostawców: Google i Apple;
- oparcie ProteGO Safe na powszechnie wspieranych technologiach i algorytmach;
- ustalenie również minimalnych wymagań sprzętowych;
- maksymalne uproszczenie etapu inicjacji działania aplikacji w urządzeniu końcowym użytkownika, które pozwala na redukcję ryzyka wystąpienia błędów konfiguracyjnych podczas rozpoczynania pracy z aplikacją.

Przy projektowaniu zarówno samego ProteGO Safe jak i ustalaniu kierunków jego rozwoju zaangażowany był krajowy organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych. Zapewniono również dobrowolność korzystania z aplikacji. Przetwarzanie danych osobowych w ProteGO Safe odbywa się zgodnie z naczelnymi zasadami przetwarzania, opisanymi w art. 5 RODO, w szczególności z uwzględnieniem minimalizacji danych oraz zasady ograniczenia celu przetwarzania.

Audyt prywatności przeprowadzony przez Kancelarię pozwolił jednocześnie na identyfikację obszarów i zagadnień problematycznych, które pomimo poczynionych wysiłków wciąż wpływają negatywnie na poziom bezpieczeństwa danych w ProteGO Safe. Przeanalizowano łącznie 146 zagadnień, wśród których

zidentyfikowano 13 zagrożeń o kategorii ryzyka „średnie” oraz 8 zagrożeń o kategorii ryzyka „niskie”.

Wśród najważniejszych zidentyfikowanych problemów wskazać należy przejrzystość informacji przekazywanych użytkownikowi. Zgodnie z najlepszymi praktykami, informacje o przetwarzaniu danych osobowych powinny być przekazywane wprost, nie należy umieszczać ich w formie skróconej (za wyjątkiem przyjętych technik warstwowania informacji) czy też umieszczać pod linkiem. W aplikacji brakuje zwięzłego i jasnego komunikatu o tożsamości administratora danych oraz celach przetwarzania. Kancelaria zwraca uwagę, że dla budowania zaufania i poczucia bezpieczeństwa podmiotów danych konieczne jest zapewnienie przejrzystej i rzetelnej komunikacji z użytkownikami.
Drugim obszarem mogącym, w opinii organów publicznych, w tym Komisji Europejskiej, stanowić zagrożenie dla prywatności, jest brak implementacji rozwiązań pozwalających na zdalną dezaktywację lub usunięcie aplikacji po pandemii i ustaniu zagrożenia. Należy zwrócić uwagę, że działania w kierunku opracowania adekwatnego rozwiązania zostały już podjęte, co oznacza że podmioty odpowiedzialne za ProteGO Safe świadome są zagrożenia i działają na rzecz jego wyeliminowania.

Biorąc pod uwagę kierunek zmian wskazany w oparciu o różnice pomiędzy kolejnymi wersjami ProteGO Safe, podmioty odpowiedzialne, w tym GIS i Minister Cyfryzacji, zdają sobie sprawę z potrzeby ochrony danych osobowych i zapewnienia bezpieczeństwa użytkowników przy jednoczesnym zrównoważeniu tych postulatów z celami operacyjnymi ProteGO Safe. Przy utrzymaniu podjętego kierunku działań, aplikacja może stać się przydatnym, skutecznym narzędziem wsparcia społeczeństwa w walce z rozprzestrzenianiem się zakażenia.

	PODSTAWOWE ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH		
	ZGODNOŚĆ Z PRAWEM, RZETELNOŚĆ I PRZEJRZYSTOŚĆ		
	Zagadnienie	Ryzyko	Proponowane działania
1.	• **podstawy prawne przetwarzania danych** Informacje przetwarzane w ramach Aplikacji nie umożliwiają (nawet pośrednio) identyfikacji osób fizycznych, niemniej podmioty zaangażowane w projekt ProteGO Safe mają świadomość, że na urządzeniach końcowych użytkownika w sposób lokalny przetwarzane są informacje które mogą stanowić dane osobowe. W związku z tym administrator danych ustalił i podał do wiadomości publicznej, w szczególności do wiadomości użytkowników, informację o podstawach prawnych przetwarzania danych osobowych. Zgodnie z przygotowaną przez Głównego Inspektora Sanitarnego (dalej również jako „**GIS**") oraz Ministra Cyfryzacji Rzeczpospolitej Polskiej (dalej jako „**MC**" lub „**Minister**") dokumentacją towarzyszącą aplikacji ProteGO Safe, dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. c) i e) RODO w związku z realizacją zadania w interesie publicznym, wynikającego z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (t. j. Dz. U. z 2019 r. poz. 59), a w zakresie danych szczególnych kategorii, w tym danych dotyczących zdrowia, na podstawie art. 9 ust. 2 lit. i) RODO. W przepisach wyżej wskazanej ustawy nie został doprecyzowany obowiązek prawny, który obligowałby GIS do zarządzania aplikacją typu ProteGO Safe. Zespół audytowy wskazuje, że wskazany art. 8a ust. 1 ustawy o Państwowej Inspekcji Sanitarnej mówi o obowiązku zarządzania „systemem wymiany informacji w ramach systemów wymiany informacji, o których mowa w przepisach wydanych na podstawie ust. 2". Ustęp 2 mówi zaś o tym, że „Minister właściwy do spraw zdrowia określi, w drodze rozporządzenia (...) wykaz systemów wymiany informacji, o których mowa w ust. 1 pkt 2 oraz zasady zarządzania przez Głównego Inspektora Sanitarnego wymianą tych informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej". W konsekwencji powyższego, do obowiązków prawnych GIS należy zarządzanie systemami wymiany informacji wyszczególnionymi w rozporządzeniach wykonawczych do wyżej wskazanej ustawy (na dzień przeprowadzenia audytu prywatności są to systemy opisane w rozporządzeniu Ministra Zdrowia z dnia 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej; ostatnia zmiana wprowadzona rozporządzeniem Ministra Zdrowia z dnia 30 października		Ryzyko jest niezależne od administratora – jego źródłem są przepisy prawa powszechnie obowiązującego. Podstawy prawne legitymujące administratora do przetwarzania danych osobowych zostały ustalone zgodnie z wymogami art. 6 i art. 9 RODO. Należy jednak zwrócić uwagę, że jednoczesne powoływanie się na podstawę legitymującą z art. 6 ust. 1 lit. c) RODO (obowiązek prawny) oraz z art. 6 ust. 1 lit. e) RODO (działanie w interesie publicznym). Podstawy te wzajemnie się wykluczają, zatem konieczne jest podjęcie decyzji, która z podstaw znajduje zastosowanie, a w następnej kolejności podstawę tę należy zakomunikować w dokumentacji towarzyszącej aplikacji ProteGO Safe (w szczególności w Polityce prywatności ProteGO Safe). Przesłanki legitymujące niesamoistne, tj. odwołujące się do przepisów krajowych lub unijnych, zostały uzupełnione o odpowiednie podstawy prawne przewidziane w prawie krajowym Rzeczpospolitej Polskiej, dzięki czemu

	2019 r. zmieniające rozporządzenie w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej).		mogą stanowić ważną podstawę prawną przetwarzania danych.
2.	• **realizacja obowiązku informacyjnego – zagadnienie ogólne** Zgodnie z art. 13 (a w adekwatnych okolicznościach – art. 14) RODO, administrator zobowiązany jest do spełnienia obowiązku informacyjnego wobec osób, których dane dotyczą. W sytuacji, gdy dane osobowe są pozyskiwane bezpośrednio od osoby, której dane dotyczą, obowiązek informacyjny należy spełnić w momencie pozyskiwania danych. Aplikacja w momencie instalacji i inicjowania działania nie wymaga podania danych osobowych. Niemniej jednak przy korzystaniu z dodatkowych funkcji aplikacji, użytkownik może dobrowolnie wprowadzić dane osobowe do aplikacji ProteGO Safe. Niezbędne jest więc zrealizowanie obowiązku informacyjnego. Informacje o przetwarzaniu danych osobowych zostały zawarte w Polityce prywatności ProteGO Safe. Inicjując działanie aplikacji ProteGO Safe, użytkownik potwierdza zapoznanie się z Regulaminem ProteGO Safe oraz z treścią Polityki prywatności ProteGO Safe. Niemniej oba dokumenty są „ukryte" pod linkami zamieszczonymi w klauzuli zgody. Odnośniki pozwalają na otwarcie dokumentów bezpośrednio wewnątrz aplikacji, nie przekierowują na strony internetowe, co umożliwia uniknięcie zbierania ewentualnych danych śledzących, zarówno anonimowych jak i personalizowanych, w tym adresów IP. Spełnienie obowiązku informacyjnego polega na udzieleniu osobie, której dane dotyczą informacji w sposób jasny i zrozumiały tak, by na ich podstawie podmiot danych miał możliwość dokonania oceny sytuacji i podjęcia dobrowolnej decyzji co do udostępnienia swoich danych administratorowi. Należy zauważyć, że zawarcie klauzuli informacyjnej jedynie w treści Polityki prywatności nie jest praktyką prawidłową. Klauzula zawierająca informacje, zgodna z powyżej opisanymi wymogami powinna znaleźć się w formularzu. Niemniej, uwzględniając, że zakres informacji niezbędnych do przekazania jest obszerny, wskazać należy, że istnieje teoretyczna, choć niepoparta normatywnie możliwość skrócenia treści klauzuli stanowiącej realizację obowiązku informacyjnego. Taką możliwość daje pogląd wyrażony w opinii Grupy Roboczej Artykułu 29 (WP29, *Opinion 17/EN on Consent under Regulation 2016/676*, WP259, przyjęta 28.11.2017 r., str. 13) oraz stanowisko Komisji Europejskiej, wyznaczające minimalny zakres klauzuli informacyjnej, który daje podstawy do uznania wyrażonej przez podmiot danych zgody za świadomą. Pogląd taki jest również zbieżny z ogólną teorią warstw informacyjnych.		Zgodnie z najlepszą praktyką, wskazane jest zamieszczenie w ekranie umożliwiającym potwierdzenie zapoznania się i akceptację Regulaminu oraz Polityki prywatności ProteGO Safe skróconej wersji klauzuli informacyjnej, zawierającej minimum informacji niezbędnych do uznania działań podejmowanych przez użytkownika aplikacji ProteGO Safe za świadome. Z informacji uzyskanych od podmiotów odpowiedzialnych za ProteGO Safe wynika, że zmiana w tym zakresie jest obecnie projektowana. W następnych wersjach aplikacji ProteGO Safe zostanie wprowadzony dodatkowy ekran zawierający treść odpowiadającą wymaganemu zakresowi informacji dla pierwszej warstwy klauzuli informacyjnej. Alternatywnie rozważane jest również dodanie takiej treści na ekranie, który umożliwia akceptację Regulaminu i Polityki prywatności podczas inicjowania pracy z aplikacją. Projektowana zmiana doprowadzi do pełnej eliminacji oznaczonego poziomu ryzyka.
3.	• **wskazanie administratora danych** Administratorem danych osobowych w rozumieniu art. 4 pkt 7) RODO, pozyskiwanych i przetwarzanych w ramach aplikacji ProteGo Safe jest Główny Inspektor Sanitarny z siedzibą w Warszawie, ul. Targowa 65, 03–729 Warszawa (dalej jako „**GIS**"). GIS jest centralnym organem administracji rządowej, inicjującym i nadzorującym czynności administracji rządowej zmierzające do zapobiegania i minimalizacji negatywnych skutków zdarzeń dotyczących zdrowia	BRAK	Brak konieczności podejmowania dodatkowych działań. Administrator danych został wskazany jednoznacznie i prawidłowo, uwzględniając cele przetwarzania danych.

	publicznego. Analizując założenia projektu aplikacji ProteGO Safe, cele utworzenia aplikacji pozostają zgodne z zakresem zadań GIS wskazanych w ustawie o Państwowej Inspekcji Sanitarnej.		
4.	• **przejrzyste komunikowanie informacji o administratorze i podmiotach zaangażowanych** W AppStore jak i w Sklepie Google oferentem oprogramowania ProteGO Safe jest Ministerstwo Cyfryzacji. MC kieruje m.in działem administracji rządowej odpowiedzialnym za informatyzację działalności administracji. Zarówno w AppStore jak i w Sklepie Google zamieszczona została informacja, że ProteGO Safe to „[O]ficjalna, polska aplikacja służąca do śledzenia kontaktu z koronawirusem, wydana przez Ministerstwo Cyfryzacji przy współpracy z Głównym Inspektoratem Sanitarnym". MC jest podmiotem odpowiedzialnym za nadzór nad rozwojem i utrzymaniem aplikacji ProteGO Safe. Pełni rolę podmiotu przetwarzającego, działającego w imieniu administratora danych. Informacja taka znajduje się m.in. w Regulaminie ProteGO Safe (v.4.2.), Polityce prywatności ProteGO Safe (v.4.2.) oraz w opublikowanym przez Ministerstwo arkuszu Oceny skutków dla ochrony danych (DPIA). Dodatkowo, arkusz Oceny skutków dla ochrony danych (DPIA) zawiera również informacje o dalszych podmiotach przetwarzających, zaangażowanych w przetwarzanie danych osobowych: 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 - podmiot odpowiedzialny za utrzymanie aplikacji ProteGO Safe, a także wykonywanie zleconych przez MC prac rozwojowych i deweloperskich nad ProteGO Safe; Operator Chmury Krajowej Sp. z o.o. podmiot dostarczający infrastrukturę umożliwiającą pobieranie i aktualizowanie ProteGO Safe oraz utrzymujący Serwer ProteGO Safe. Podmiot ten świadczy także utrzymanie usługi Google Firebase umożliwiającej przekazywanie Użytkownikom powiadomień push - https://firebase.google.com/support/privacy; Cloudflare Inc. 101 Townsend St, San Francisco, CA 94107, USA (usługa zapobiegania atakom DDOS oraz zapewnienia najwyższych standardów bezpieczeństwa Użytkowników).	BRAK	Brak konieczności podejmowania dodatkowych działań. Informacje o podmiotach odpowiedzialnych za dostarczanie oprogramowania ProteGO Safe są łatwo dostępne i przejrzyste.
	ZASADA OGRANICZENIA CELU		
	Zgodnie z treścią wiersza 2 „Opisu operacji przetwarzania" Oceny skutków dla ochrony danych (DPIA) „[C]elem przetwarzania danych w aplikacji ProteGO Safe jest wsparcie społeczeństwa w przeciwdziałaniu rozprzestrzeniania się pandemii COVID-19: działając w szeroko rozumianym interesie publicznym, administrator poprzez dystrybucję i zapewnienie operacyjności aplikacji ProteGO Safe wspiera szybką wymianę informacji pomiędzy osobami fizycznymi w ramach określonej społeczności, działając na rzecz profilaktyki zdrowia publicznego i przeciwdziałania rozprzestrzenianiu się wirusa SARS CoV-2 oraz choroby COVID-2, poprzez wymianę zanonimizowanych informacji dotyczących osób zakażonych oraz oprogramowanie umożliwiające analizę spotkań i kontaktów, jak również poprzez algorytmy umożliwiające ocenę ryzyka zarażenia". Celami przetwarzania danych osobowych, zgodnie z treścią Polityki prywatności ProteGO Safe jest realizacja działań związanych „z zadaniem publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19, wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej (Dz.U.		

	z 2019 r. poz. 59), gdyż przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi na podstawie prawa państwa członkowskiego".		
	Zagadnienie	Ryzyko	Proponowane działania
5.	• **dokładne i jednoznaczne określenie celu przetwarzania danych osobowych** Cele przetwarzania danych osobowych zostały określone jednoznacznie. Cele są zbieżne z zadaniami GIS, sprecyzowanymi w ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej. Cel przetwarzania został dodatkowo dookreślony w taki sposób, by ponad wszelką wątpliwość informować o zamierzonym rezultacie przetwarzania danych osobowych przez GIS jako administratora danych, z wykorzystaniem aplikacji ProteGO Safe.	BRAK	Brak konieczności podejmowania dodatkowych działań.
6.	• **cele akcesoryjne przetwarzania danych, powiązane z pierwotnym celem przetwarzania** Celem przetwarzania danych Użytkownika jest także świadczenie usług drogą elektroniczną, w oparciu o postanowienia Regulaminu ProteGO Safe, przy czym z uwagi na powszechny i bezpłatny charakter aplikacji, cel ten nie wymaga identyfikacji osoby fizycznej korzystającej z aplikacji. Dane przetwarzane w ramach Google Firebase oraz Google Analitycs mają charakter statystyczny, dane nie są jednostkowe (stanowią średnią wszystkich danych) oraz mają na celu efektywne utrzymanie aplikacji, a także planowanie dalszego jej rozwoju w oparciu m.in. o informacje o liczbie użytkowników oraz modelach telefonów. W ramach serwera Google Firebase przetwarzanie ma charakter anonimowy, nie są tam przetwarzane dane osobowe (Google LLC nie uzyskuje danych w formie osobowej za pośrednictwem aplikacji).	BRAK	Brak konieczności podejmowania dodatkowych działań.
7.	• **cele przetwarzania danych osobowych nieustalane przez GIS** Przetwarzanie danych ma na celu dostarczenie obywatelom usługi umożliwiającej ocenę stanu własnego zdrowia oraz uzyskanie informacji o spotkaniach z osobami zarażonymi bez identyfikacji tych osób oraz okoliczności kontaktu z nimi. Aplikacja umożliwia triaż (samoocenę ryzyka infekcji wirusem SARS-CoV-2, stworzoną na podstawie kwestionariusza WHO), prowadzenie dziennika zdrowia Użytkownika, wsparcie w profilaktyce i zapobieganiu zarażeniem, wczesne ostrzeganie Użytkownika potencjalnie zagrożonego zarażeniem, otrzymywanie istotnych informacjach związanych z pandemią wirusa SARS-CoV-2 oraz przypominacz bezpiecznych zachowań i nawyków codziennej higieny. O przetwarzaniu danych osobowych w powyższych celach decyduje użytkownik. GIS i podmioty odpowiedzialne za ProteGO Safe dostarczają wyłącznie oprogramowanie umożliwiające realizację powyższych celów w pewien określony sposób.	BRAK	Brak konieczności podejmowania dodatkowych działań.
8.	• **możliwość wykorzystania danych osobowych w celach innych niż pierwotny cel** Informacje przetwarzane w ramach Aplikacji nie umożliwiają (nawet pośrednio) identyfikacji osób fizycznych. Zastosowanie znajduje art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Z uwagi na brak dostępu do danych osobowych zapisywanych lokalnie w Urządzeniu Użytkownika, wykorzystanie danych w celach innych niż pierwotnie określone, w tym w celach niezwiązanych z pierwotnymi celami przetwarzania danych, nie jest możliwe.		
	ZASADA MINIMALIZACJI DANYCH		
	Aplikacja zbiera dane i informacje wyszczególnione w wierszy 6 „Opisu operacji przetwarzania" arkusza Oceny skutków dla ochrony danych (DPIA). Zakres danych wprowadzanych przez użytkownika do aplikacji został potwierdzony empirycznie, podczas praktycznej pracy z aplikacją ProteGO Safe.		
	Zagadnienie	Ryzyko	Proponowane działania
9.	• **minimalizacja danych w ramach podstawowego działania aplikacji ProteGO Safe (bez funkcjonalności dodatkowych)** W podstawowej wersji aplikacji ProteGO Safe przetwarzany jest minimalny zakres danych - ograniczony do identyfikatora użytkownika oraz klucza diagnostycznego (losowe i okresowo zmieniane anonimowe identyfikatory urządzeń), a także danych statystycznych (w tym danych zanonimizowanych).	BRAK	Brak konieczności podejmowania dodatkowych działań.
10.	• **minimalizacja danych w ramach dodatkowych funkcjonalności aplikacji ProteGO Safe (Moduł Triażu i Moduł Dziennika Zdrowia)** W ramach korzystania z funkcji dodatkowych, aplikacja pozwala na wprowadzenie przez użytkownika wyłącznie danych niezbędnych do wykonania oceny ryzyka zarażenia (w przypadku korzystania z Modułu Triażu) czy też kontroli stanu zdrowia użytkownika celem wczesnego wykrywania niepokojących objawów (w przypadku korzystania z Modułu Dziennika Zdrowia). Dane przetwarzane w aplikacji są wyłącznie danymi niezbędnymi do zapewnienia Użytkownikowi możliwości korzystania z Aplikacji oraz jej funkcjonalności i Modułów.	BRAK	Brak konieczności podejmowania dodatkowych działań.
11.	• **minimalizacja danych w ramach wymiany informacji pomiędzy urządzeniem użytkownika i serwerem ProteGO Safe** Uwierzytelnienie osoby chorej na COVID-19 następuje poprzez wprowadzenie do Aplikacji losowego numeru PIN podanego przez przedstawiciela Centrum Kontaktu, który nie umożliwia identyfikacji. Użytkownicy Aplikacji nie są oznaczani danymi identyfikującymi osobę typu imię i nazwisko, lecz losowo generowanym identyfikatorem Użytkownika. Dla GIS czy Ministra, który zarządza Serwerem ProteGO Safe, dane te są anonimowe w rozumieniu art. 11 RODO. Aplikacja przypomina, by nie wprowadzać do niej nazwiska użytkownika (w każdym miejscu, w którym możliwe jest ustalenie lub zmiana lokalnie przechowywanego identyfikatora użytkownika). Dane osobowe przetwarzane w Aplikacji ProteGO Safe przetwarzane są w formie uniemożliwiającej identyfikację osoby, której dane dotyczą zarówno przez Ministra Cyfryzacji jak i GIS. Dane przekazywane podczas komunikacji z serwerem ProteGO Safe, znane Ministrowi Cyfryzacji jak i GIS podmiotom przetwarzane w Aplikacji ProteGO Safe to dane związane z wykorzystywaniem serwera zapewniającego przekazywanie Użytkownikom komunikatów:	BRAK	Brak konieczności podejmowania dodatkowych działań.

	– UID - losowy identyfikator Urządzenia Użytkownika, – Średni czas korzystania z Aplikacji przez Użytkowników (dane statystyczne, których nie można powiązać z poszczególnymi Użytkownikami).		
12.	• **minimalizacja danych w ramach wymiany informacji pomiędzy urządzeniami użytkowników (zapis kontaktów z wykorzystaniem technologii Bluetooth)** Zakres danych, a w szczególności zakres danych udostępnianych innym podmiotom niż osoba, której dotyczą ograniczony jest do niezbędnego minimum - ogranicza się wyłącznie do danych niezbędnych zakodowanych w kluczu diagnostycznym, umożliwiających wskazanie ryzyka transmisji wirusa SARS CoV-2 od użytkownika, u którego wykryto obecność wirusa lub chorobę COVID-19. Udostępnianiu może podlegać klucz diagnostyczny, zawierający informację o chorym użytkowniku (osobie chorej) oraz kluczach jego urządzenia, przy czym sygnał odbierany przez aplikację jest przez nią interpretowany automatycznie, bez wskazywania użytkownikom, które z zarejestrowanych spotkań stanowi podstawę zagrożenia zakażeniem, zatem nie dochodzi do udostępnienia danych osoby chorej lub innego użytkownika. Dla innych podmiotów, w tym GIS, czy MC, który zarządza serwerem ProteGO Safe poprzez który wysyłane są na urządzenia innych użytkowników klucze urządzeń użytkowników, którzy wyrazili zgodę na anonimowe ostrzeżenie osób, które znalazły się w ich otoczeniu o zidentyfikowaniu u nich choroby i możliwości zakażenia innych osób, dane te są anonimowe w rozumieniu art. 11 RODO.	BRAK	Brak konieczności podejmowania dodatkowych działań.
	ZASADA PRAWIDŁOWOŚCI DANYCH		
	Zagadnienie	Ryzyko	Proponowane działania
13.	• **prawo do sprostowania danych w ProteGO Safe** Zgodnie z informacjami zawartymi w arkuszu Oceny skutków dla ochrony danych (DPIA) „[A]plikacja umożliwia realizację prawa do sprostowania, którą z uwagi na minimalizację danych może wykonać wyłącznie osoba, której dane dotyczą (użytkownik Aplikacji). W aplikacji ProteGO Safe w Polityce Prywatności (do której odsyła Regulamin aplikacji) będą wyświetlane informacje dotyczące możliwości skorzystania z tego uprawnienia. Po usunięciu danych za pośrednictwem aplikacji (w ustawieniach aplikacji), można sprostować dane wprowadzając je od nowa do Aplikacji". Powyższe zostało potwierdzone empirycznie, podczas praktycznej pracy z aplikacją ProteGO Safe.	BRAK	Brak konieczności podejmowania dodatkowych działań.
14.	• **redukcja ryzyka przetwarzania nieprawidłowych danych osobowych w procesie ostrzegania przed kontaktami potencjalnie epidemiologicznymi** By uniemożliwić wprowadzanie nieprawidłowych informacji do aplikacji ProteGO Safe, inicjować dystrybucję klucza diagnostycznego przez osoby niebędące osobami chorymi, GIS i podmioty odpowiedzialne zadecydowały o wprowadzeniu mechanizmu uwierzytelniania osób chorych z wykorzystaniem numeru PIN – jednorazowego, pseudolosowo generowanego kodu, przekazywanego użytkownikowi który posiada	BRAK	Brak konieczności podejmowania dodatkowych działań.

	potwierdzony pozytywny wynik testu diagnostycznego, przez Centrum Kontaktu. W ten sposób zredukowano ryzyko przetwarzania informacji nieprawidłowych w aplikacji.		
	ZASADA OGRANICZENIA PRZECHOWYWANIA		
	Zagadnienie	Ryzyko	Proponowane działania
15.	• **ustalenie relewantnego okresu przetwarzania danych osobowych** Okres retencji został ustalony na 14 dni od dnia wprowadzenia informacji do aplikacji lub do pamięci serwera. Okres tak ustalony zgadza się z okresem inkubacji koronawirusa SARS CoV-2, jak również zgadza się z wytycznymi i zaleceniami niezależnych organów.	BRAK	Brak konieczności podejmowania dodatkowych działań.
16.	• **automatyzacja procesu usuwania danych osobowych z pamięci urządzenia użytkownika (aplikacja ProteGO Safe) oraz z backendu (serwer ProteGO Safe)** Możliwość przechowywania danych ograniczono poprzez wprowadzenie systemowego ograniczenia historii działania Modułu Analitycznego do 14 dni wstecz. Klucze diagnostyczne są przechowywane na serwerze ProteGO Safe przez okres 14 dni, a następnie automatycznie kasowane.	BRAK	Brak konieczności podejmowania dodatkowych działań.
17.	• **powiązanie usunięcia aplikacji z usunięciem danych zapisanych w aplikacji** Użytkownik może zaprzestać korzystania z ProteGO Safe ze skutkiem natychmiastowym i bez wskazywania przyczyn poprzez usunięcie ProteGO Safe ze swojego urządzenia lub manualnego wyczyszczenia danych w aplikacji. Usunięcie aplikacji przez użytkownika z urządzenia skutkuje usunięciem danych przechowywanych w aplikacji. Po zaprzestaniu korzystania z ProteGO Safe dane zostaną usunięte wraz z aplikacją.	BRAK	Brak konieczności podejmowania dodatkowych działań.
	ZASADA INTEGRALNOŚCI I POUFNOŚCI		
	Zagadnienie	Ryzyko	Proponowane działania
18.	• **lokalne przechowywanie danych na urządzeniu końcowym użytkownika** Dane osobowe zbierane przez aplikację ProteGO Safe (dotyczące kontaktów, wprowadzane bezpośrednio przez użytkownika) przechowywane są lokalnie w pamięci wewnętrznej urządzenia końcowego użytkownika aplikacji. Dostęp do danych jest niemożliwy zarówno dla GIS i podmiotów odpowiedzialnych (w tym dla MC jako głównego procesora) jak i dla innych użytkowników aplikacji. Wyjątek stanowi sytuacja, gdy poprzez dobrowolne wprowadzenie kodu PIN osoba zarażona decyduje się na powiadomienie innych użytkowników o kontakcie stwarzającym zagrożenie epidemiologiczne.	BRAK	Brak konieczności podejmowania dodatkowych działań.
19.	• **zabezpieczenie kryptograficzne transmisji danych pomiędzy urządzeniem użytkownika i serwerem ProteGO Safe** • **zabezpieczenie kryptograficzne danych przechowywanych na urządzeniu użytkownika i na serwerze ProteGO Safe** Dane osobowe w aplikacji są szyfrowane przy wykorzystaniu nowoczesnych rozwiązań kryptograficznych. Dostęp do nich możliwy jest jedynie poprzez nieuprawnione i niezgodne z prawem złamanie zabezpieczeń	BRAK	Brak konieczności podejmowania dodatkowych działań.

	telefonu. Takie złamanie zabezpieczeń powoduje, że osoba nieuprawniona otrzymuje dostęp do zasobów jednej instancji aplikacji (jednego urządzenia). Krótkotrwałe ID, generowane losowe i dynamiczne (zmieniające się w czasie, zgodnie z ustalonym harmonogramem), zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Kluczowym jest używanie TLS w kodowaniu danych w transporcie gdy dochodzi do komunikacji poprzez WiFi lub dane komórkowe (przesyłania klucza diagnostycznego po wprowadzeniu przez osobę chorą kodu PIN w aplikacji; aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej).		
20.	• **separacja serwerów** Serwer nadający anonimowe identyfikatory oraz serwer przesyłający klucze diagnostyczne nie są ze sobą połączone. Identyfikacja osób chorych na COVID-19 jest niemożliwa z perspektywy aplikacji ProteGO Safe i serwerów ProteGO Safe.	BRAK	Brak konieczności podejmowania dodatkowych działań.
21.	• **wykorzystanie Exposure Notification API Google i Apple oraz technologii od Cloudflare dla zapewnienia poufności** Exposure Notification API Google i Apple jest specjalnie zaprojektowane w taki sposób, aby uniemożliwić deanonimizację użytkowników oraz wykorzystanie systemu do innego celu. ProteGO Safe technicznie minimalizuje ryzyko działania systemu dalej przez gromadzenie wyłącznie anonimowych danych systemu Exposure Notification. Architektura systemu Exposure Notification API, własne rozwiązania wykorzystujące system Cloudflare do anonimizacji użytkowników, a także okoliczność, że generowanie identyfikatorów oraz analiza spotkań odbywa się na urządzeniu użytkownika sprawia, że niemożliwym staje się niewłaściwie wykorzystanie danych przez MC lub GIS. Jedyną funkcją systemu jest anonimowe powiadamianie osób narażonych. Cloudflare jest usługą chmurową wykorzystywaną w celu zapobiegania atakom DDOS oraz zapewnienia najwyższych standardów bezpieczeństwa Użytkowników. Cloudflare przy połączeniach z aplikacją ProteGO Safe ustawia ciasteczko __cfduid, które może zostać użyte do monitorowania użytkownika pomiędzy różnymi serwerami oraz tworzenie jego profilu. Ciasteczko może zostać wyłączone w edycji Enterprise, co jest sugerowane, niemniej wersja Enterprise jest kosztowna, a ryzyko monitorowania nie jest znaczne. Ponadto wyniki testów bezpieczeństwa nie wykazały, że przedmiotowe ryzyko stanowi podatność aplikacji ProteGO Safe.	BRAK	Brak konieczności podejmowania dodatkowych działań.
22.	• **dostęp do danych przetwarzanych na serwerach wyłącznie przez osoby upoważnione** Zgodnie z dokumentacją towarzyszącą, dostęp do systemu jest ograniczony do uprawnionych pracowników podmiotu utrzymującego i wspierającego aplikację. Ponadto modyfikacja danych nieosobowych jest ograniczona technicznie.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	ZASADA ROZLICZALNOŚCI		
	Zagadnienie	Ryzyko	Proponowane działania
23.	• **przeprowadzenie analizy ryzyka** • **w razie konieczności: przeprowadzenie oceny skutków dla przetwarzania danych osobowych oraz przeprowadzenie uprzednich konsultacji ws. projektu** Analiza ryzyka dla przetwarzania danych osobowych w ProteGO Safe została przeprowadzona i udokumentowana w arkuszu Oceny skutków dla ochrony danych (DPIA). Z uwagi na wykorzystanie modułów Bluetooth (uznawanych za technologie tracingowe) oraz z uwagi na dużą skalę przetwarzania danych osobowych lokalnie w urządzeniu użytkownika, jednak za pomocą dostarczanej aplikacji ProteGO Safe, w tym danych szczególnych kategorii (dotyczących zdrowia), przeprowadzono ocenę skutków dla ochrony danych osobowych zgodnie z wymogami art. 35 RODO. Badanie zostało udokumentowane i opublikowane tak, by zapewnić transparentność funkcjonowania aplikacji ProteGO Safe. Wynik badania DPIA nie wskazuje na konieczność przeprowadzenia uprzednich konsultacji w rozumieniu art. 36 RODO.	**BRAK**	Brak konieczności podejmowania dodatkowych działań.
24.	• **realizacja zasad *privacy by design* i *privacy by default*** Aplikacja w podstawowym zakresie może funkcjonować z powodzeniem bez przetwarzania jakichkolwiek danych osobowych. Dopiero korzystanie z dodatkowych modułów (Moduł Triażu, Moduł Dziennika Zdrowia, Moduł Analityczny) wymaga podania dodatkowych danych osobowych przez użytkowników. Zakres danych osobowych wymagany przez aplikację został ustalony z uwzględnieniem zasady minimalizacji danych. Jednocześnie dane nie podlegają autouzupełnianiu z innych źródeł (m.in. aplikacja ProteGO Safe nie jest powiązana i nie może zostać sparowana z kontami w mediach społecznościowych). Użytkownik ma możliwość wprowadzenia wyłącznie danych relewantnych dla oceny zagrożenia zakażeniem SARS CoV-2 (przy czym w przypadku np. wieku nie jest konieczne podawanie konkretnej wartości, a wyłącznie przedział poniżej lub powyżej 65 roku życia; możliwa jest również rezygnacja z podawania informacji o wieku). Dodatkowo, wszelkie zgody lub oświadczenia w aplikacji zbierane są na zasadzie opt-in, a ewentualne checkboxy (jak np. w przypadku akceptacji Regulaminu ProteGO Safe czy Polityki prywatności ProteGO Safe, czy też zgody na wykorzystanie modułów Bluetooth) pozostają domyślnie odznaczone.	**BRAK**	Brak konieczności podejmowania dodatkowych działań.
25.	• **odnotowanie procesu w rejestrze czynności przetwarzania administratora (GIS)** • **odnotowanie procesu w rejestrze kategorii czynności przetwarzania procesora (MC)** Dla wykazania spełnienia obowiązków, o których mowa w art. 30 ust. 1 i 2 RODO, informacje o procesach przetwarzania danych osobowych związanych z aplikacją ProteGO Safe zostały odnotowane w rejestrze czynności przetwarzania GIS oraz rejestrze kategorii czynności przetwarzania MC.	**BRAK**	Brak konieczności podejmowania dodatkowych działań.

26.	• **ustalone warunki powierzenia przetwarzania danych osobowych MC i dalszego powierzenia przetwarzania danych osobowych subprocesorom, w zakresie treściowym zgodne z wymogami art. 28 RODO** Współpraca pomiędzy GIS, MC a innymi podmiotami zaangażowanymi w budowę i zapewnienie funkcjonowania ProteGO Safe opiera się na postanowieniach zawartego pomiędzy podmiotami porozumienia. Porozumienie zawiera regulacje dotyczące powierzenia przetwarzania danych osobowych, w zakresie treściowym zgodne z wymogami umowy powierzenia przetwarzania danych, wskazanymi w art. 28 ust. 3 RODO.	BRAK	Brak konieczności podejmowania dodatkowych działań.
	PODSTAWOWE ZASADY DOTYCZĄCE WYKORZYSTYWANIA URZĄDZEŃ KOŃCOWYCH GROMADZENIE I DOSTĘP DO INFORMACJI ZGROMADZONYCH W URZĄDZENIACH KOŃCOWYCH		
	WYMOGI WYNIKAJĄCE Z DYREKTYWY O ŁĄCZNOŚCI ELEKTRONICZNEJ I USTAWY PRAWO TELEKOMUNIKACYJNE		
	Zgodnie z art. 173 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t. j. Dz. U. z 2019 r. poz. 2460, z 2020 r. poz. 374, 695, 875; dalej jako: „**PrTelU**"), by przechowywanie i dostęp do informacji przechowywanych w pamięci urządzenia końcowego były zgodne z prawem, należy spełnić szereg wymogów, w tym m.in. poinformować w sposób zrozumiały, łatwy i jednoznaczny użytkownika urządzenia końcowego o celu przechowywania i uzyskiwania dostępu do informacji oraz możliwości modyfikowania uprawnień związanych z dostępem do informacji przechowywanych w urządzeniu końcowym. Należy również uzyskać świadomą zgodę użytkownika na takie przechowywanie (która, zgodnie z brzmieniem art. 174 PrTelU podlega rygorom ważności przewidzianym w przepisach o ochronie danych osobowych). Zgodnie z art. 173 ust. 3 pkt 2) PrTelU powyższe warunki nie mają zastosowania jeżeli przechowywanie lub dostęp do informacji przechowywanych na urządzeniu końcowym są konieczne do „dostarczania usługi telekomunikacyjnej lub usługi świadczonej drogą elektroniczną, żądanej przez abonenta lub użytkownika końcowego".		
	Aplikacja ProteGO Safe przechowuje na urządzeniu końcowym użytkownika informacje, które można podzielić na dwie grupy: – informacje niezbędne dla zapewnienia funkcjonalności Modułów Triażu, Dziennika Zdrowia i Analitycznego; – informacje niezbędne dla zapewnienia bezpieczeństwa aplikacji i danych w niej zapisanych, w szczególności w zakresie plików cookies dostarczanych przez Cloudflare w celu ochrony przed atakami typu DDOS. ProteGO Safe gromadzi informacje niezbędne dla zapewnienia możliwości przeprowadzania analiz dotyczących aplikacji, w celu umożliwienia dalszego rozwoju aplikacji i doskonalenia jej, w oparciu o technologię Google Analytics. Wykorzystywana technologia Google Analytics projekcie ProteGO Safe nie umożliwia analizowania sposobu korzystania z aplikacji, a jedynie daje informacje statystyczne dotyczące liczby pobrań, modelów telefonów (aby efektywniej dobierać zasoby usług utrzymania w zakresie obsługi błędów) i przybliżonej lokalizacji pobrania (chodzi nam głównie o kraj pobrania aplikacji). Ten sposób wykorzystania Google Analytics nie wymaga implementacji ani odczytywania informacji z urządzenia końcowego użytkownika.		
	Zagadnienie	Ryzyko	Proponowane działania
27.	• **przechowywanie i dostęp do informacji przechowywanych na urządzeniu końcowym użytkownika w kontekście wyłączenia z art. 173 ust. 3 pkt 2) ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne** *Technologia ochrony DDOS w oparciu o cookies od Cloudflare* Aplikacja ProteGO Safe w podstawowej wersji korzysta z przechowywania informacji i dostępu do informacji przechowywanej na urządzeniu końcowym użytkownika w zakresie informacji niezbędnych dla zapewnienia	BRAK	Brak konieczności podejmowania dodatkowych działań.

	bezpieczeństwa (technologia ochrony Cloudflare). Zapewnienie stabilności i bezpieczeństwa aplikacji ProteGO Safe jest niezbędne dla dostarczania usługi świadczonej drogą elektroniczną w postaci aplikacji ProteGO Safe, bezpiecznej z punktu widzenia prywatności, a więc takiej, jakiej oczekuje i żąda użytkownik instalując aplikację. W konsekwencji, przechowywanie tych informacji w urządzeniu końcowym wyczerpuje przesłanki wyłączenia obowiązków z art. 173 ust. 1 PrTelU w oparciu o art. 173 ust. 3 pkt 2) PrTelU. *Korzystanie z modułów dodatkowych* Korzystanie z poszczególnych dodatkowych funkcji (Modułów Triażu, Dziennika Zdrowia i Analitycznego) wymaga przechowywania dodatkowych informacji w urządzeniu użytkownika. Aplikacja ProteGO Safe co do zasady nie uzyskuje dostępu do informacji przechowywanych na urządzeniu końcowym użytkownika. Jedynym przypadkiem jest zainicjowany proces ostrzegania użytkownika, gdy aplikacja w wyniku odebrania informacji z serwera o kluczu diagnostycznym osoby chorej, bazując na wbudowanych skryptach analitycznych, porównuje otrzymany klucz diagnostyczny z identyfikatorami kontaktów, które zostały przez nią odnotowane, celem ustalenia ryzyka zakażenia. Z uwagi na lokalny charakter procesu oraz fakt, że w procesie porównywania nie uczestniczy podmiot trzeci oraz że wynik porównania nie jest znany podmiotowi trzeciemu, wątpliwym jest jednak, by takie działanie mogło zostać zakwalifikowane stricte jako dostęp do informacji przechowywanych na urządzeniu końcowym użytkownika ProteGO Safe w rozumieniu art. 173 PrTelU. Informacje zgromadzone w modułach dodatkowych pozostają niezbędne do zapewnia użytkownikowi możliwości korzystania z dodatkowych funkcji, zatem ich przechowywanie w urządzeniu końcowym wyczerpuje przesłanki wyłączenia obowiązków z art. 173 ust. 1 PrTelU w oparciu o art. 173 ust. 3 pkt 2) PrTelU.		
	INNE ZAGADNIENIA		
	ZGODNOŚĆ Z DODATKOWYMI WYMOGAMI WYNIKAJĄCYMI Z ZALECEŃ I WYTYCZNYCH		
	EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic — 14/04/2020 (dalej jako: „**List EROD**")		
	Zagadnienie	**Ryzyko**	**Proponowane działania**
28.	• **zaangażowanie organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych** Zgodnie z zaleceniami wyrażonymi w Liście EROD „w celu zapewnienia przetwarzani danych osobowych zgodnie z prawem" powinny odbyć się konsultacje z organem nadzorczym. Ministerstwo zwracało się do PUODO z prośbą o wzięcie udziału w pracach nad ProteGO Safe. Organ nadzorczy istotnie wystosował swoje uwagi i zalecenia co do funkcjonowania aplikacji ProteGO Safe, zwrócił również uwagę na ważne dla ochrony prywatności zagadnienia (odpowiedź PUODO dostępna pod linkiem: https://pliki.panoptykon.org/DIP/Cyfrowy%20Nadz%C3%B3r%20-%20EOG%20I/Przychodz%C4%85ca%20-	**BRAK**	Brak konieczności podejmowania dodatkowych działań. Prezes Urzędu Ochrony Danych Osobowych został poproszony o opinię na temat projektowanego rozwiązania oraz wyraził swoje stanowisko i przedstawił zalecenia.

	%20odpowiedzi%20na%20wniosek/UODO_dip_obowi%C4%85zkowo%C5%9B%C4%87%20ProteGO/odpowied%C5%BA%20w%20sprawie%20ProteGO_30.04.2020%20%282%29.pdf).		
29.	• **wykonanie oceny skutków dla ochrony danych osobowych** Zgodnie z zaleceniami wynikającymi z Listu EROD „ocena skutków w zakresie ochrony danych powinna obejmować wszystkie wdrożone mechanizmy ochrony prywatności już w fazie projektowania i domyślnej ochrony prywatności". Ocena skutków dla ochrony danych (DPIA) została wykonana, a jej udokumentowana forma (arkusz Oceny skutków dla ochrony danych (DPIA)) został opublikowany, umożliwiając opinii publicznej zapoznanie się z ustaleniami poczynionymi w trakcie badania ryzyka i skutków przetwarzania dla ochrony danych.	BRAK	Brak konieczności podejmowania dodatkowych działań.
30.	• **otwartość kodu źródłowego** Zgodnie z zaleceniami wyrażonymi w Liście EROD „[K]od źródłowy powinien być upubliczniony i poddany jak najszerszym badaniom prowadzonym przez naukowców". Kod źródłowy aplikacji ProteGO Safe został podany do wiadomości publicznej.	BRAK	Brak konieczności podejmowania dodatkowych działań.
31.	• **dobrowolność stosowania aplikacji** Zgodnie ze stanowiskiem wyrażonym w Liście EROD „EROD zdecydowanie popiera wniosek Komisji dotyczący dobrowolnego stosowania takich aplikacji". Stosowanie aplikacji ProteGO Safe jest dobrowolne, zależy od indywidualnego wyboru osoby fizycznej. Brak negatywnych skutków dla osób nieużywających aplikacji. Użytkownik może zaprzestać korzystania z ProteGO Safe ze skutkiem natychmiastowym i bez wskazywania przyczyn poprzez usunięcie ProteGO Safe ze swojego Urządzenia.	BRAK	Brak konieczności podejmowania dodatkowych działań.
32.	• **podstawa przetwarzania danych osobowych: konieczność wykonania zadania w interesie publicznym** Zgodnie z zaleceniami wynikającymi z Listu EROD „najważniejszą podstawą prawną przetwarzania danych jest [...] konieczność wykonania zadania w interesie publicznym". Zgodnie z przygotowaną przez GIS oraz MC dokumentacją towarzyszącą aplikacji ProteGO Safe, dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. e) RODO w związku z realizacją zadania w interesie publicznym. Celem aplikacji ProteGO Safe jest wsparcie społeczeństwa w przeciwdziałaniu rozprzestrzeniania się infekcji wirusem SARS-CoV-2. Zgodnie z treścią Polityki prywatności ProteGO Safe celem przetwarzania danych osobowych w ProteGO Safe jest realizacja działań związanych „z zadaniem publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19, wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej (Dz.U. z 2019 r. poz. 59), gdyż przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi na podstawie prawa państwa członkowskiego".	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Cele są zbieżne z zadaniami GIS, sprecyzowanymi w ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej.		
33.	• **minimalizacja danych – rezygnacja z gromadzenia danych o przemieszczaniu się osób fizycznych** Zgodnie z zaleceniami wynikającymi z Listu EROD „gromadzenie danych o przemieszczaniu się osób fizycznych w ramach aplikacji służących do ustalania kontaktów zakaźnych naruszałoby zasadę minimalizacji danych". Aplikacja ProteGO Safe dla ustalenia kontaktu pomiędzy urządzeniami użytkownika wykorzystuje technologię Bluetooth (BLE). Nie korzysta jednocześnie z technologii geolokalizacyjnych ani z transmisji danych za pomocą sieci komórkowych (wniosek bazowany na doświadczeniach empirycznych uzyskanych podczas korzystania z aplikacji ProteGO Safe). Technologia Bluetooth wykorzystywana przez ProteGO Safe nie wymaga aktywacji żadnych innych technologii lokalizacyjnych, w szczególności wskazanych powyżej.	BRAK	Brak konieczności podejmowania dodatkowych działań.
34.	• **przechowywanie danych o kontaktach (zdarzeniach)** W Liście EROD za dopuszczalne uznaje się dwa warianty przechowywania danych: „lokalne przechowywanie danych w urządzeniach osób fizycznych lub przechowywanie scentralizowane". Warunkiem zapewnienia zgodności z prawem każdego z tych rozwiązań jest wprowadzenie odpowiednich środków bezpieczeństwa oraz określenie podmiotu administracyjnego w zależności od ostatecznego przeznaczenia aplikacji. Zdaniem EROD-u „przechowywanie scentralizowane jest bardziej spójne z zasadą minimalizacji danych". Dane osobowe użytkownika oraz inne informacje wprowadzane do aplikacji ProteGO Safe przez użytkownika są przechowywane lokalnie, na urządzeniu końcowym użytkownika. Podjęto decyzję o decentralizacji dużej części procesu, niemniej dane otrzymane od użytkowników z pozytywnym wynikiem testu na Covid-19 są zaś przetwarzane centralnie (klucz diagnostyczny urządzenia przechowywany jest na serwerze ProteGO Safe przez okres 14 dni). Poprzez zastosowanie odpowiednich środków zabezpieczających, przyjęty model, choć w dominującej części decentralizowany, posiada elementy modelu scentralizowanego. Jest to zatem rozwiązanie hybrydowe, korzystające z zalet rozwiązań scentralizowanych i zdecentralizowanych.	BRAK	Brak konieczności podejmowania dodatkowych działań.
35.	• **szyfrowanie i pseudonimizacja** Zgodnie z zaleceniami wyrażonymi w Liście EROD „powiadomienie danej osoby w aplikacji może się odbywać w taki sposób, aby były przetwarzane jedynie przypadkowo generowane pseudonimy". ProteGO Safe w momencie instalacji i inicjowania działania nie wymaga podania danych osobowych. Użytkownik może wprowadzić swoją nazwę, którą nie powinno być jednak nazwisko. Dane osobowe mogą zostać podane przez użytkownika w wyniku korzystania z dodatkowych funkcji aplikacji. Wszystkie informacje przetwarzane przez ProteGO Safe zbierane i przetwarzane są w taki sposób, aby uniemożliwić identyfikację użytkowników.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Zgodnie z informacjami zamieszczonymi w arkuszu Oceny skutków dla ochrony danych (DPIA) „aplikacja bazuje na losowych i dynamicznych (zmieniających się w czasie, zgodnie z ustalonym harmonogramem) kluczach Urządzenia Użytkownika". Serwer ProteGO Safe (backend) nie umożliwia także przechowywania lub połączenia (porównania) kluczy dziennych z kluczami diagnostycznymi. Krótkotrwałe ID, generowane losowe i dynamiczne (zmieniające się w czasie, zgodnie z ustalonym harmonogramem), zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Kluczowym jest używanie TLS w kodowaniu danych w transporcie gdy dochodzi do komunikacji poprzez WiFi lub dane komórkowe (przesyłania klucza diagnostycznego po wprowadzeniu przez osobę chorą kodu PIN w aplikacji; aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej). Deweloperzy przy tworzeniu aplikacji korzystali z dobrze znanych i rekomendowanych algorytmów i protokołów kryptograficznych.		
36.	• **prawidłowość danych** Zgodnie z zaleceniami wyrażonymi w Liście EROD powinien istnieć mechanizm gwarantujący prawidłowość wprowadzonych informacji, w przypadku stwierdzenia, że jakaś osoba jest zarażona COVID-19. Może być to np. „jednorazowy kod, który skanuje się w momencie odebrania wyniku tekstu". Uwierzytelnienie osoby chorej na COVID-19 następuje poprzez wprowadzenie do Aplikacji losowego numeru PIN podanego przez przedstawiciela Centrum Kontaktu. Inicjacja procesu przekazywania klucza diagnostycznego jest zabezpieczona za pomocą kodu PIN (generowanym w sposób losowy, jednorazowego użytku). Wpisanie kodu PIN w aplikacji ProteGO Safe jest dobrowolne.	BRAK	Brak konieczności podejmowania dodatkowych działań.
37.	• **nadzór nad wykorzystywanymi w aplikacji algorytmami, brak całkowitego zautomatyzowania** Zgodnie z zaleceniami wynikającymi z Listu EROD „algorytmy wykorzystywane w aplikacjach służących do ustalania kontaktów zakaźnych powinny podlegać ścisłemu nadzorowi sprawowanemu przez wykwalifikowany personel […] a zadanie „udzielania informacji o kolejnych etapach" nie może być w żadnym razie całkowicie zautomatyzowane". Zainteresowana osoba powinna mieć możliwość uzyskania dodatkowych informacji o osobie obsługującej np. przez otrzymanie numeru telefonu. Informacje te nie mogą zawierać żadnych potencjalnych elementów identyfikujących inną osobę, której dane dotyczą. Celem aplikacji ProteGO Safe jest wsparcie użytkowników we wczesnej identyfikacji ryzyka zakażenia. Podmioty odpowiedzialne za funkcjonowanie aplikacji zaznaczają, że wskazania aplikacji nie są diagnozą medyczną oraz że powinny być interpretowane z uwzględnieniem odpowiedniego marginesu ostrożności. Wskazania aplikacji dotyczące wysokiego ryzyka zakażenia mogą być sygnałem wskazującym na potrzebę	BRAK	Brak konieczności podejmowania dodatkowych działań.

	skontaktowania się ze służbami sanitarno-epidemiologicznymi, jednak nie zastępują takiego kontaktu, tym bardziej nie zastępują konieczności konsultacji medycznej z lekarzem. W aplikacji ProteGo Safe udzielanie informacji nie jest całkowicie zautomatyzowane - automatyzacja przetwarzania dotyczy podejmowania decyzji w zakresie wskazania użytkownikowi stopnia zagrożenia. Od użytkownika wówczas zależy, czy skontaktuje się ze służbami sanitarno-epidemiologicznymi. W celu umożliwienia takiego kontaktu aplikacja podaje „specjalny numer" do Państwowej Inspekcji Sanitarnej. Serwer nadający anonimowe identyfikatory oraz serwer przesyłający klucze diagnostyczne nie są ze sobą połączone. Identyfikacja osób chorych na COVID-19 jest niemożliwa z perspektywy aplikacji ProteGO Safe i serwerów ProteGO Safe. Aplikacja wskazując na wysokie ryzyko zarażenia nie podaje żadnych informacji umożliwiających identyfikacje zarażonej osobie, z która miało się kontakt. Nie podaje się też informacji o czasie i miejscu kontaktu.		
38.	• **brak przechowywania danych identyfikacyjnych w urządzeniach użytkowników** W Liście EROD zalecane jest „aby nie przechowywać żadnych bezpośrednich danych identyfikacyjnych w urządzeniach użytkowników i aby dane takie były w każdym razie jak najszybciej usuwane". W sytuacji, gdy zarażony użytkownik wprowadza do aplikacji ProteGo Safe kod PIN, identyfikacja urządzenia, który zainicjował proces dystrybucji kluczy diagnostycznych jest teoretycznie możliwa. Sama jednak identyfikacja użytkownika, z uwagi na brak innych danych umożliwiających jednoznaczne wskazanie tożsamości osoby fizycznej, pozostaje niemożliwa gdyż jedyna informacją, jaką dysponuje administrator jest sygnał inicjujący wysyłkę kluczy diagnostycznych.	BRAK	Brak konieczności podejmowania dodatkowych działań.
39.	• **automatyczna dezaktywacja/usuwanie aplikacji po pandemii/ustaniu zagrożenia epidemiologicznego** W Liście EROD „popiera […] koncepcję, aby po zakończeniu obecnego kryzysu nie używać w dalszym ciągu przedmiotowego systemu zarządzania sytuacjami wyjątkowymi, a zebrane dane powinny, co do zasady, być usunięte lub zanonimizowane". Zgodnie z założeniami projektowymi, o których użytkownicy są informowani w dokumentacji towarzyszącej aplikacji (Regulaminie ProteGO Safe (v.4.2.), Polityce prywatności ProteGO Safe (v.4.2.) oraz w opublikowanym przez Ministerstwo arkuszu Oceny skutków dla ochrony danych (DPIA)), aplikacja zostanie wyposażona w możliwość zdalnej dezaktywacji w momencie zakończenia pandemii COVID-19 lub stanu zagrożenia pandemicznego w następnej wersji oprogramowania. Na moment przeprowadzania audytu prywatności oraz opracowywania niniejszego raportu, zalecenie to nie jest spełnione. Zgodnie z uzyskanymi od podmiotów odpowiedzialnych informacjami, z uwagi na obawy o nieproporcjonalną ingerencję w prywatność (pełna realizacja, zakładająca usunięcie aplikacji wraz z danymi w niej przechowywanymi z urządzenia użytkownika wymagałaby technicznych rozwiązań umożliwiających zdalny dostęp podmiotów odpowiedzialnych do urządzenia końcowego użytkownika, co z uwagi na poszanowanie prywatności użytkowników jest niemożliwe do realizacji) oraz możliwe konsekwencje w postaci spadku		Dla pełnej zgodności przetwarzania danych osobowych w aplikacji ProteGO Safe z wytycznymi KE należy uzupełnić możliwość zdalnej dezaktywacji aplikacji w momencie zakończenia pandemii COVID-19 lub stanu zagrożenia pandemicznego. Wstępne założenia projektowe zakładają wprowadzenie rozwiązania, które będzie zapewniać realizację tego wymogu, a prace w tym kierunku zostały podjęte.

	zaufania do podmiotów publicznych oraz tego typu aplikacji i programów, rozwiązania, które choćby w stopniu potencjalnym wymagały ingerencji w urządzenia końcowe użytkownika nie są rozważane. Podmioty odpowiedzialne rozważają alternatywne możliwości dezaktywacji aplikacji, które nie będą wymagać dostępu do urządzenia końcowego użytkownika, w tym wprowadzenie rozwiązań umożliwiających zachowanie danych lub ich eksport po okresie pandemii, ewentualne pozostawienie możliwości korzystania z aplikacji ProteGO Safe po zakończeniu pandemii z jednoczesnym ograniczeniem funkcjonalności aplikacji, np. do funkcji informowania o prawach i obowiązkach, aktualnej sytuacji epidemiologicznej. Podmioty odpowiedzialne podjęły konsultacje z interesariuszami projektu ProteGO Safe, zgodnie z uzyskanymi informacjami planowane jest również przeprowadzenie konsultacji ze społecznością GitHub oraz Komisją Europejską.		
	Mandate on geolocation and other tracing tools in the context of the COVID-19 outbreak — 07/04/2020.		
	Zagadnienie	**Ryzyko**	**Proponowane działania**
40.	• **wykorzystanie zagregowanych /zanonimizowanych danych dotyczących lokalizacji** Po zdalnym posiedzeniu plenarnym w dniu 3 kwietnia 2020 r. EROD zdecydowała się przedstawić wytyczne dotyczące kwestii wykorzystania narzędzi śledzenia i geolokalizacji powstałe w kontekście kryzysu związanego z wybuchem COVID-19, a w szczególności wykorzystywania zagregowanych/ zanonimizowanych danych dotyczących lokalizacji (np. dostarczonych przez operatora sieci telekomunikacyjnej/dostawcy usług społeczeństwa informacyjnego). Aplikacja ProteGo Safe nie zbiera danych o lokalizacji użytkownika, tj. fizycznego położenia geograficznego użytkownika jak również z transmisji danych za pomocą sieci komórkowych (operatorzy sieci telekomunikacyjnych nie przekazują żadnych danych dostawcy aplikacji o lokalizacji użytkowników aplikacji). Dane pozyskiwane są bezpośrednio z otoczenia Użytkownika (przy wykorzystaniu technologii Bluetooth - klucze Urządzeń innych Użytkowników). Aplikacja ProteGO Safe przetwarza wyłącznie dane niezbędne do ustalenia kontaktu potencjalnie zakaźnego, unikając przy tym przechowywania informacji dodatkowych, takich jak geolokalizacja.	BRAK	Brak konieczności podejmowania dodatkowych działań.
41.	• **przestrzeganie zasad legalności, „niezbędności", „proporcjonalności", minimalizacji danych** EROD wskazała na konieczność przestrzegania szeroko pojętych zasad legalności, niezbędności, proporcjonalności, w tym prawidłowości i minimalizacji danych do różnych dostępnych środków gromadzenia danych o lokalizacji lub śledzenia interakcji między osobami, których dane dotyczą. Wytyczne w zakresie przestrzegania powyższych zasad, a w szczególności zasady legalności, która określa, że dane osobowe mogą być przetwarzane przez administratora danych w oparciu o ustawowe przesłanki. GIS jako administrator danych osobowych przetwarza dane w oparciu o przepisy prawa, a dokładniej mówiąc dla realizacji swoich zadań ustawowych wynikających z ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (t. j. Dz. U. z 2019 r. poz. 59). Niestety, przepisy te zawierają zakres zadań, które GIS ma wykonywać,		W zakresie spełnienia przestrzegania zasady legalności, konieczne jest jednoznaczne określenie podstaw prawnych przetwarzania danych, jednak jest to ryzyko niezależne od administratora – jego źródłem są przepisy prawa powszechnie obowiązującego. Powyższe nie zmienia faktu, że administrator danych oraz

	nie zawierają jednak dyspozycji kwalifikowanych jako obowiązki prawne, co jest szczególnie istotne w kontekście aplikacji ProteGo Safe. Brak w przepisach powszechnie obowiązujących szczegółowych regulacji dotyczących wyżej wskazanych zagadnień, wyszczególnionych w wytycznych, w szczególności informacji o wymaganych przepisami prawa, konkretnych zabezpieczeniach. W konsekwencji krajowy system prawny nie pozwala na powołanie się na art. 6 ust. 1 lit. c) RODO jako podstawę prawną przetwarzania w analizowanym przypadku. Właściwszym jest wskazanie art. 6 ust. 1 lit. e) RODO. Możliwa do przyjęcia podstawa prawna przetwarzania, czyli art. 6 ust. 1 lit. e) RODO jest mniej stabilna niż miałoby to miejsce w przypadku istnienia obowiązku prawnego nałożonego na GIS, z drugiej jednak strony jest to podstawa legitymująca o dość stabilnym charakterze. Obszerna dokumentacja towarzysząca (w szczególności publikowaną Ocenę skutków dla ochrony danych (DPIA) oraz raporty z testów bezpieczeństwa przeprowadzonych przez niezależne podmioty) dodatkowo wpływa na dalsze ustabilizowanie warunków przetwarzania i buduje wiarygodność przyjętych rozwiązań. Nie mniej należy wskazać, że administrator danych oraz podmiot przetwarzający legitymują się co najmniej jedną z przesłanek legalizujących przetwarzanie danych osobowych. Z kolei „zasada niezbędności" wskazuje za konieczność przetwarzania jedynie takiego zakresu danych, który jest niezbędny i konieczny do osiągnięcia celu, w tym przypadku celu ustalenia potencjalnego kontaktu z osobą zakażoną. Aplikacja spełnia ww. wymagania. Zasada proporcjonalności, którą można wyinterpretować z zasady minimalizacji danych, nakazuje, aby dane były przetwarzane proporcjonalnie do celów, jakie aplikacja ma spełniać w kontekście pandemii. Z kolei stosowanie zasady minimalizacji danych, a więc ograniczenia zakresu przetwarzanych danych do minimum przejawia się poprzez stosowanie w aplikacji zbliżeniowej technologii wzajemnego odnotowywania osób Urządzeń innych Użytkowników znajdujących się w otoczeniu Użytkownika, które nie pozwala zarówno na identyfikację (tak pośrednią jak i bezpośrednią) innych Użytkowników, jak i geograficzną lokalizację miejsca, w którym doszło do spotkania. Wytyczne w kontekście przestrzegania zasady prawidłowości przez aplikację przejawiają w ten sposób, że aby uniemożliwić wprowadzanie nieprawidłowych informacji do aplikacji ProteGO Safe i uniemożliwić inicjowanie dystrybucji klucza diagnostycznego przez osoby niebędące osobami chorymi, GIS i podmioty odpowiedzialne zadecydowały o wprowadzeniu mechanizmu uwierzytelniania osób chorych z wykorzystaniem numeru PIN – jednorazowego, pseudolosowo generowanego kodu, przekazywanego użytkownikowi który posiada potwierdzony pozytywny wynik testu diagnostycznego, przez Centrum Kontaktu. W ten sposób zredukowano ryzyko przetwarzania informacji nieprawidłowych w aplikacji.		podmiot przetwarzający legitymują się co najmniej jedną z przesłanek legalizujących przetwarzanie danych osobowych. W wytycznych 2020/C 124 I/01 Komisja wspomina o art. 6 ust. 1 lit. e) RODO i choć preferowaną i stabilniejszą podstawą przetwarzania danych osobowych byłby istniejący obowiązek prawny (art. 6 ust. 1 lit. c) RODO), krajowy system prawa nie zawiera odpowiednich przepisów umożliwiających oparcie przetwarzania na tej podstawie legitymującej. W zakresie pozostałych zasad wskazanych w wytycznych EROD – brak konieczności podejmowania dodatkowych działań.
42.	• **ogólna analiza prawna korzystania z aplikacji i gromadzenia danych osobowych** EROD w swoich wytycznych wskazuje na konieczności przeprowadzenia przez dostawcę aplikacji ogólnej analizy prawnej korzystania z aplikacji oraz gromadzenia danych. Taka analiza została przeprowadzona bezpośrednio poprzez opracowanie przez Ministerstwo oraz publiczne udostępnienie arkuszu Oceny skutków dla ochrony danych (DPIA), który zawiera dokładny opis wykonanego badania DPIA. Do wiadomości	BRAK	Brak konieczności podejmowania dodatkowych działań.

	publicznej podawane są również raporty z audytów i analiz dotyczących bezpieczeństwa i prywatności, w tym raport z przeprowadzonego audytu bezpieczeństwa aplikacji (https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport). Ministerstwo wypełnia wytyczne o konieczności przeprowadzania tego rodzaju analiz prawnych.		
43.	• **zabezpieczenia zapewniające przestrzegania zasad ochrony danych, w tym w odniesieniu do czasu przechowywania danych** Informacje o otoczeniu Użytkownika przechowywane są bezpośrednio w pamięci wewnętrznej jego Urządzenia jedynie przez 14 dni od ich wygenerowania. Możliwość przechowywania danych ograniczono poprzez wprowadzenie systemowego ograniczenia historii działania Modułu Analitycznego do 14 dni wstecz. Reszta danych przechowywana jest do czasu usunięcia manualnego lub usunięcia Aplikacji. Usunięcie Aplikacji przez Użytkownika z Urządzenia skutkuje usunięciem danych przechowywanych w aplikacji. Dane będą przechowywane nie dłużej niż trwa korzystanie z ProteGO Safe oraz mogą być przechowywane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Zastosowano środki zabezpieczające zapewniające przestrzeganie zasady ograniczonego czasu przechowywania, w szczególności systemowe usuwanie z Modułu Analitycznego danych starszych niż 14 dni, które pozwalają na pełną realizację zasady ograniczenia czasowego. Istnieje możliwość usunięcia Aplikacji lub manualnego wyczyszczenia danych w Aplikacji. Możliwość przechowywania danych z Modułu Analitycznego ograniczono poprzez wprowadzenie systemowego ograniczenia historii działania Aplikacji do 14 dni wstecz.	BRAK	Brak konieczności podejmowania dodatkowych działań.
44.	• **ramy czasowe podejmowanych środków** Kolejną wytyczną wystosowaną przez EROD jest konieczność zwrócenia uwagi przez dostawców aplikacji na ogólny czas podejmowanych środków w celu reakcji na sytuację epidemiologiczną za pośrednictwem aplikacji. Możliwość korzystania z aplikacja powinna przybrać ramy czasowe adekwatne do czasu trwania pandemii COVID-19. W chwili obecnej okres obowiązywania aplikacji nie jest jednoznacznie określony. Aplikacja będzie umożliwiała zdalne jej zdeaktywowanie z momentem zakończenia pandemii COVID-19 lub stanu zagrożenia epidemiologicznego w kolejnej wersji aplikacji. Zatem Ministerstwo jest świadome konieczności określenia z góry czasu podejmowania środków za pomocą aplikacji w celu przeciwdziałania rozprzestrzenianiu się pandemii. Zgodnie z uzyskanymi od podmiotów odpowiedzialnych informacjami, z uwagi na obawy o nieproporcjonalną ingerencję w prywatność (pełna realizacja, zakładająca usunięcie aplikacji wraz z danymi w niej przechowywanymi z urządzenia użytkownika wymagałaby technicznych rozwiązań umożliwiających zdalny dostęp podmiotów odpowiedzialnych do urządzenia końcowego użytkownika, co z uwagi na poszanowanie prywatności użytkowników jest niemożliwe do realizacji) oraz możliwe konsekwencje w postaci spadku zaufania do podmiotów publicznych oraz tego typu aplikacji i programów, rozwiązania, które choćby w stopniu potencjalnym wymagały ingerencji w urządzenia końcowe użytkownika nie są rozważane. Podmioty odpowiedzialne rozważają alternatywne możliwości dezaktywacji aplikacji, które nie będą		Konieczność umożliwienia zdalnego zdezaktywowania aplikacji z momentem zakończenia pandemii COVID-19 lub stanu zagrożenia epidemiologicznego. Odpowiednie rozwiązanie zostanie wdrożone w kolejnych wersjach aplikacji.

	wymagać dostępu do urządzenia końcowego użytkownika, w tym wprowadzenie rozwiązań umożliwiających zachowanie danych lub ich eksport po okresie pandemii, ewentualne pozostawienie możliwości korzystania z aplikacji ProteGO Safe po zakończeniu pandemii z jednoczesnym ograniczeniem funkcjonalności aplikacji, np. do funkcji informowania o prawach i obowiązkach, aktualnej sytuacji epidemiologicznej. Podmioty odpowiedzialne podjęły konsultacje z interesariuszami projektu ProteGO Safe, zgodnie z uzyskanymi informacjami planowane jest również przeprowadzenie konsultacji ze społecznością GitHub oraz Komisją Europejską.		
	Europejska Rada Ochrony Danych: Oświadczenie w sprawie interoperacyjności aplikacji służących do ustalania kontaktów zakaźnych. Przyjęte w dniu 16 czerwca 2020 r.		
	Zagadnienie	**Ryzyko**	**Proponowane działania**
45.	• **wymiana minimum informacji** EROD przyjęła do wiadomości wytyczne w sprawie interoperacyjności dotyczące zatwierdzonych aplikacji służących do ustalania kontaktów zakaźnych w UE, przyjęte przez sieć e-zdrowie w dniu 13 maja 2020 r., w których opisano interoperacyjność w kontekście aplikacji służącej do ustalania kontaktów zakaźnych jako „*zdolność do wymiany minimum informacji niezbędnych do tego, by poszczególni użytkownicy aplikacji, niezależnie od tego, gdzie się znajdują na terenie UE, zostali ostrzeżeni, jeżeli w danym okresie znajdowali się w pobliżu innego użytkownika, który powiadomił aplikację o pozytywnym wyniku testu na obecność COVID-19*". Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, ProteGo Safe spełnia warunki interoperacyjności sprecyzowane w powyżej wskazanym dokumencie. Wskazane wytyczne w zakresie interoperacyjności zostały wzięte pod uwagę podczas tworzenia ProteGO Safe. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, ProteGo Safe spełnia warunki interoperacyjności sprecyzowane w powyżej wskazanych dokumentach. Aplikacja ProteGO Safe przechowuje informacje o okresie kontaktu urządzeń użytkowników (jak długo urządzenia znajdowały się blisko siebie; wartości w zakresie 5-30 minut) oraz o dacie kontaktu. Celem aplikacji nie jest powiadamianie organów ds. zdrowia, a użytkowników aplikacji o ryzyku epidemiologicznym wynikającym z kontaktu z osobą zakażoną. Powyżej wskazany zakres danych jest niezbędny do ustalenia zwiększenia ryzyka, jednocześnie inne informacje i dane nie będą miały wpływ na ustalenie ryzyka zakażenia, zatem pozostają zbędne i z tego względu zrezygnowano z ich zbierania.	BRAK	Brak konieczności podejmowania dodatkowych działań.
46.	• **działania następcze podejmowane zgodnie z procedurami określonymi przez organy zdrowia publicznego z uwzględnieniem oceny skutków dla ochrony danych** W sytuacji, gdy osoba będzie miała wynik pozytywny testu na COVID-19, skontaktuje się z nim konsultant Centrum Kontaktu, który informuje o pozytywnym wyniku testu. Konsultant zaproponuje powiadomienie innych Użytkowników o tym, że przebywali w pobliżu Urządzenia osoby zakażonej w ciągu ostatnich 14 dni poprzez podanie kodu PIN osoby chorej. Udostępnienie takiej informacji w aplikacja jest dobrowolne. W		W zakresie interoperacyjności działań następczych - należy kontynuować podjęte rozmowy z organami zdrowia publicznego celem wypracowania zasad interoperacyjności.

	każdym z tych przypadków, organ ds. zdrowia w Polsce podejmuje konkretne działania następcze w oparciu o przepisy prawa, a dokładniej mówiąc dla realizacji swoich zadań ustawowych wynikających z ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (t. j. Dz. U. z 2019 r. poz. 59). W zakresie interoperacyjności organy zdrowia publicznego powinny uzgodnić protokoły wymiany informacji o łańcuchach transgranicznych kontaktów, zwłaszcza o zarażonych mających kontakt z osobami z innych państw. GIS i inne organy zdrowia publicznego podjęły dialog celem ustalenia zasad interoperacyjności. Na dzień przeprowadzenia niniejszego audytu prywatności, rozmowy nie zostały zakończone a ustaleń nie podjęto.		
47.	• pseudonimizacja W podstawowej wersji aplikacji ProteGO Safe przetwarzany jest minimalny zakres danych - ograniczony do identyfikatora użytkownika oraz klucza diagnostycznego (losowe i okresowo zmieniane anonimowe identyfikatory urządzeń), a także danych statystycznych (w tym danych zanonimizowanych). Krótkotrwałe ID, generowane losowe i dynamiczne (zmieniające się w czasie, zgodnie z ustalonym harmonogramem), zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne. W ramach korzystania z funkcji dodatkowych, aplikacja pozwala na wprowadzenie przez użytkownika wyłącznie danych niezbędnych do wykonania oceny ryzyka zarażenia (w przypadku korzystania z Modułu Triażu) czy też kontroli stanu zdrowia użytkownika celem wczesnego wykrywania niepokojących objawów (w przypadku korzystania z Modułu Dziennika Zdrowia). W ramach Modułu Analitycznego aplikacja przechowuje informacje o okresie kontaktu urządzeń użytkowników (jak długo urządzenia znajdowały się blisko siebie; wartości w zakresie 5-30 minut) oraz o dacie kontaktu. Dane osobowe użytkownika oraz inne informacje wprowadzane do aplikacji przez użytkownika są przechowywane lokalnie, na urządzeniu końcowym użytkownika. Dane osobowe przetwarzane w Aplikacji ProteGO Safe przetwarzane są w formie uniemożliwiającej identyfikację osoby, której dane dotyczą zarówno przez Ministra Cyfryzacji jak i GIS. Dane przekazywane podczas komunikacji z serwerem ProteGO Safe, znane Ministrowi Cyfryzacji jak i GIS podmiotom przetwarzane w Aplikacji ProteGO Safe to dane związane z wykorzystywaniem serwera zapewniającego przekazywanie Użytkownikom komunikatów. Serwer ProteGO Safe (Backend) nie umożliwia identyfikacji użytkownika ani połączenia (porównania) kluczy diagnostycznych (narażenia) z jakimikolwiek innymi danymi użytkownika. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Kluczowym jest używanie TLS w kodowaniu danych w transporcie gdy dochodzi do komunikacji poprzez WiFi lub dane komórkowe (przesyłania klucza	BRAK	Brak konieczności podejmowania dodatkowych działań.

	diagnostycznego po wprowadzeniu przez osobę chorą kodu PIN w aplikacji; aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej). Zakres danych, a w szczególności zakres danych udostępnianych innym podmiotom niż osoba, której dotyczą ograniczony jest do niezbędnego minimum - ogranicza się wyłącznie do danych niezbędnych zakodowanych w Kluczu Diagnostycznym, umożliwiających wskazanie ryzyka transmisji wirusa SARS CoV-2 od Użytkownika, u którego wykryto obecność wirusa lub chorobę COVID-19. Klucze diagnostyczne (narażenia) są przechowywane na serwerze ProteGO Safe przez okres retencji wynoszący 14 dni, a następnie automatycznie kasowane. Możliwość przechowywania danych przez użytkownika na urządzeniu końcowym, gdzie zainstalowana jest aplikacja ProteGO Safe, ograniczona została poprzez wprowadzenie systemowego ograniczenia historii działania Modułu Analitycznego do 14 dni wstecz.		
48.	• **dobrowolność udostępniania informacji o zakażeniu** Założeniami procedury zdecentralizowanej jest przesyłanie ostrzeżenia „automatycznie za pośrednictwem aplikacji do bliskich kontaktów, gdy użytkownik powiadomi aplikację – za zgodą lub po potwierdzeniu przez organ ds. zdrowia, na przykład za pomocą kodu QR lub kodu TAN – że uzyskał pozytywny wynik testu (proces zdecentralizowany)". W sytuacji, gdy osoba będzie miała wynik pozytywny testu na COVID-19, skontaktuje się z nim konsultant Centrum Kontaktu, który informuje o pozytywnym wyniku testu. Konsultant zadaje pytanie, czy osoba ma zainstalowaną aplikację ProteGo Safe i jeśli tak będzie konsultant zaproponuje powiadomienie innych Użytkowników o tym, że przebywali w pobliżu Urządzenia osoby zakażonej w ciągu ostatnich 14 dni poprzez podanie kodu PIN osoby chorej. Użytkownik samodzielnej podejmuje decyzje czy chce oznaczyć swoje Urządzenie jako Urządzenie Osoby Chorej, co zainicjuje wysłanie anonimowego Klucza Diagnostycznego na Serwer ProteGO Safe, a następnie do innych Użytkowników Aplikacji. Wobec całkowitej dobrowolności podania udostepnienie informacji o zakażeniu warunek dobrowolności podania informacji jest zachowany. Nie ma wymogu informowania o zakażeniu, jak też organ ds. zdrowia (konsultant) nie jest uprawniony do wymagania od zakażonego użytkownika wprowadzenia takiej informacji do aplikacji.	BRAK	Brak konieczności podejmowania dodatkowych działań.
49.	• **przejrzystość** EROD wskazuje, że jak zawsze, osoby, których dane dotyczą, muszą być informowane o każdym dodatkowym przetwarzaniu ich danych osobowych oraz o zaangażowanych stronach. Użytkownicy powinni zawsze mieć jasność co do tego, z czym wiąże się korzystanie z aplikacji, i powinni zachować kontrolę nad swoimi danymi. Najpóźniej w momencie pozyskiwania danych osobowych przez administratora, osoba, której dane dotyczą, musi uzyskać jasne informacje na temat dodatkowego przetwarzania związanego ze stosowaniem interoperacyjności. Na tym etapie użytkownik musi zostać poinformowany o warunkach i zakresie przetwarzania danych. Obowiązują standardowe zasady przejrzystości: informacje te powinny być przekazywane jasnym i prostym językiem. Obejmują one informacje o tym, w jaki sposób dane, które są udostępniane, będą przetwarzane przez otrzymującą interoperacyjną aplikację służącą do ustalania kontaktów zakaźnych.		Zgodnie z najlepszą praktyką, wskazane jest zamieszczenie w ekranie umożliwiającym potwierdzenie zapoznania się i akceptację Regulaminu oraz Polityki prywatności ProteGO Safe skróconej wersji klauzuli informacyjnej, zawierającej minimum informacji niezbędnych do uznania działań podejmowanych przez użytkownika aplikacji ProteGO Safe za świadome.

	Aplikacja w momencie instalacji i inicjowania działania nie wymaga podania danych osobowych. Niemniej jednak przy korzystaniu z dodatkowych funkcji aplikacji, użytkownik może dobrowolnie wprowadzić dane osobowe do aplikacji ProteGO Safe. Niezbędne jest więc zrealizowanie obowiązku informacyjnego. Informacje o przetwarzaniu danych osobowych zostały zawarte w Polityce prywatności ProteGO Safe. Inicjując działanie aplikacji ProteGO Safe, użytkownik potwierdza zapoznanie się z Regulaminem ProteGO Safe oraz z treścią Polityki prywatności ProteGO Safe. Niemniej oba dokumenty są „ukryte" pod linkami zamieszczonymi w klauzuli zgody. Odnośniki pozwalają na otwarcie dokumentów bezpośrednio wewnątrz aplikacji, nie przekierowują na strony internetowe, co umożliwia uniknięcie zbierania ewentualnych danych śledzących, zarówno anonimowych jak i personalizowanych, w tym adresów IP. Przyjęte rozwiązanie należy ocenić częściowo negatywnie. Spełnienie obowiązku informacyjnego polega na udzieleniu osobie, której dane dotyczą informacji w sposób jasny i zrozumiały tak, by na ich podstawie podmiot danych miał możliwość dokonania oceny sytuacji i podjęcia dobrowolnej decyzji co do udostępnienia swoich danych administratorowi. Należy zauważyć, że zawarcie klauzuli informacyjnej jedynie w treści Polityki prywatności nie jest praktyką prawidłową. Klauzula zawierająca informacje, zgodna z powyżej opisanymi wymogami powinna znaleźć się w formularzu. Niemniej, uwzględniając, że zakres informacji niezbędnych do przekazania jest obszerny, wskazać należy, że istnieje teoretyczna, choć niepoparta normatywnie możliwość skrócenia treści klauzuli stanowiącej realizację obowiązku informacyjnego. Taką możliwość daje pogląd wyrażony w opinii Grupy Roboczej Artykułu 29 (WP29, *Opinion 17/EN on Consent under Regulation 2016/676*, WP259, przyjęta 28.11.2017 r., str. 13) oraz stanowisko Komisji Europejskiej, wyznaczające minimalny zakres klauzuli informacyjnej, który daje podstawy do uznania wyrażonej przez podmiot danych zgody za świadomą. Pogląd taki jest również zbieżny z ogólną teorią warstw informacyjnych.		Z informacji uzyskanych od podmiotów odpowiedzialnych za ProteGO Safe wynika, że zmiana w tym zakresie jest obecnie projektowana. W następnych wersjach aplikacji ProteGO Safe zostanie wprowadzony dodatkowy ekran zawierający treść odpowiadającą wymaganemu zakresowi informacji dla pierwszej warstwy klauzuli informacyjnej. Alternatywnie rozważane jest również dodanie takiej treści na ekranie, który umożliwia akceptację Regulaminu i Polityki prywatności podczas inicjowania pracy z aplikacją. Projektowana zmiana doprowadzi do pełnej eliminacji oznaczonego poziomu ryzyka.
50.	• **podstawa prawna** EROD w oświadczeniu w sprawie interoperacyjności aplikacji służących do ustalania kontaktów zakaźnych odwołuje się podstaw prawnych, o których mowa w wytycznych 04/2020. Zgodnie z zaleceniami wynikającymi z Listu EROD „najważniejszą podstawą prawną przetwarzania danych jest [...] konieczność wykonania zadania w interesie publicznym". Zgodnie z przygotowaną przez GIS oraz MC dokumentacją towarzyszącą aplikacji ProteGO Safe, dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. e) RODO w związku z realizacją zadania w interesie publicznym. Celem aplikacji ProteGO Safe jest wsparcie społeczeństwa w przeciwdziałaniu rozprzestrzeniania się infekcji wirusem SARS-CoV-2. Zgodnie z treścią Polityki prywatności ProteGO Safe celem przetwarzania danych osobowych w ProteGO Safe jest realizacja działań związanych „z zadaniem publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19, wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej (Dz.U. z 2019 r. poz. 59), gdyż przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak	BRAK	Brak konieczności podejmowania dodatkowych działań.

	ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi na podstawie prawa państwa członkowskiego". Cele są zbieżne z zadaniami GIS, sprecyzowanymi w ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej.		
51.	• **sprawowanie kontroli** EROD zaleca jednoznaczne ustalenie oraz określenie ról poszczególnych podmiotów zaangażowanych w proces przetwarzania danych oraz sprawowanie przez nich kontroli. Aplikacja ProteGO Safe jest administrowana przez GIS. Podmiotem przetwarzającym jest Ministerstwo Cyfryzacji. Role w procesie przetwarzania zostały jednoznacznie określone.	BRAK	Brak konieczności podejmowania dodatkowych działań.
52.	• **korzystanie z praw przez osoby, których dane dotyczą** Wszelkie rozwiązania interoperacyjne muszą ułatwiać osobom, których dane dotyczą, korzystanie z przysługujących im praw. Jeżeli korzystanie z praw jest możliwe, nie powinno ono stać się bardziej uciążliwe dla osób, których dane dotyczą, i powinno być jasne, do kogo osoby, których dane dotyczą, powinny zwrócić się o możliwość skorzystania ze swoich praw. Ograniczenia w korzystaniu z praw przysługujących osobom, których dane dotyczą, są możliwe na mocy wyjątków określonych w art. 11 i art. 23 RODO. Wskazane powyżej wytyczne zostały wzięte pod uwagę podczas tworzenia ProteGO Safe. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, ProteGo Safe spełnia warunki interoperacyjności sprecyzowane w powyżej wskazanych dokumentach. Zgodnie z zasadami opisanymi w arkuszu Oceny skutków dla ochrony danych (DPIA) „[I]dentyfikacja Urządzenia Użytkownika, który wprowadził Kod PIN a tym samym zainicjował dystrybucję Kluczy Diagnostycznych jest teoretycznie możliwa, niemniej identyfikacja Użytkownika, z uwagi na brak innych danych umożliwiających jednoznaczne wskazanie tożsamości osoby fizycznej, pozostaje niemożliwa (jedyną informacją, jaką dysponuje administrator, jest sygnał inicjujący wysyłkę Kluczy Diagnostycznych przez Serwer ProteGO Safe - istnieje możliwość, że Sewer odnotuje logi komunikacyjne, niemniej ich interpretacja i powiązanie z identyfikowalną osobą fizyczną pozostają niemożliwe)". Informacje przetwarzane w ramach ProteGO Safe nie umożliwiają (nawet pośrednio) identyfikacji osób fizycznych. Dane osobowe przetwarzane są zgodnie z zasadami wskazanymi w art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji.	BRAK	Brak konieczności podejmowania dodatkowych działań.
53.	• **zatrzymanie i minimalizacja danych** EROD wskazuje, że różnice w ustalonym okresie zatrzymywania danych nie powinny prowadzić do przechowywania danych dłużej niż jest to konieczne. Aby propagować skuteczne stosowanie zasad ochrony danych, należy rozważyć wspólny poziom minimalizacji danych i wspólny okres zatrzymywania danych. Jak wspomniano wcześniej, interoperacyjność nie powinna prowadzić do zwiększonego gromadzenia informacji z powodu braku skoordynowanego podejścia. Użytkownik musi być o tym wyraźnie poinformowany przed udostępnieniem danych.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Aplikacja ProteGo Safe stosuje się do wytycznych WHO i ECDC na temat czasu przez jaki dane o kontaktach powinny być przechowywane. Wskazane powyżej wytyczne WHO i ECDC zostały wzięte pod uwagę podczas tworzenia ProteGO Safe. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, ProteGo Safe spełnia warunki interoperacyjności sprecyzowane w powyżej wskazanych dokumentach.		
54.	• **bezpieczeństwo informacji** Interoperacyjność nie powinna prowadzić do zmniejszenia bezpieczeństwa danych i ochrony danych osobowych. EROD zaleca, aby dostawcy aplikacji służących do ustalania kontaktów zakaźnych brali pod uwagę każdy wzrost ryzyka związanego z bezpieczeństwem informacji spowodowany dodatkowym przetwarzaniem i zaangażowaniem dodatkowych podmiotów. Dotyczy to w szczególności bezpieczeństwa danych w tranzycie w celu ewentualnego wzajemnego połączenia serwerów końcowych. W ocenie skutków dla ochrony danych należy w szczególności uwzględnić środki dotyczące zagrożeń dla bezpieczeństwa związanych z interoperacyjnością, które mają wpływ na prawa i wolności osób fizycznych. Ocena skutków dla ochrony danych (DPIA) została wykonana (również w zakresie określonym w wytycznych), a jej udokumentowana forma (arkusz Oceny skutków dla ochrony danych (DPIA) został opublikowany, umożliwiając opinii publicznej zapoznanie się z ustaleniami poczynionymi w trakcie badania ryzyka i skutków przetwarzania dla ochrony danych. Kompleksowa ocena ryzyka z punktu widzenia ochrony danych osobowych i informacji przetwarzanych przez ProteGO Safe została przeprowadzona i udokumentowana w skoroszycie „Ocena i zarządzanie ryzykiem" arkusza Oceny skutków dla ochrony danych (DPIA).	BRAK	Brak konieczności podejmowania dodatkowych działań.
55.	• **Prawidłowość danych** EROD wskazuje, że w przypadku gdy dostawcy rozważają, w jaki sposób zapewnić interoperacyjność swoich aplikacji służących do ustalania kontaktów zakaźnych, powinni w miarę możliwości zagwarantować, że nie doprowadzi to do obniżenia poziomu jakości lub dokładności danych. Interoperacyjność, w przypadku dużych rozbieżności, może prowadzić do utraty jakości danych (np. nieprawidłowe wnioski z oceny, niski przydział ryzyka), co może prowadzić do wzrostu wyników fałszywie pozytywnych. Osoby, których dane dotyczą, będą musiały być wyraźnie informowane o tych dodatkowych zagrożeniach dla dokładności danych. Środki wprowadzone w celu zapewnienia dokładności danych należy utrzymać w systemie interoperacyjnym. Uwierzytelnienie osoby chorej na COVID-19 następuje poprzez wprowadzenie do Aplikacji losowego numeru PIN podanego przez przedstawiciela Centrum Kontaktu, co minimalizuje ryzyko wyniku fałszywie pozytywnego. Inicjacja procesu przekazywania klucza diagnostycznego jest zabezpieczona za pomocą kodu PIN (generowanym w sposób losowy, jednorazowego użytku). Wpisanie kodu PIN w aplikacji ProteGO Safe jest dobrowolne.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Zalecenie Komisji (UE) 2020/518 z dnia 8 kwietnia 2020 r. w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności (dalej jako „zalecenia 2020/518").		
	Zagadnienie	Ryzyko	Proponowane działania
56.	• odpowiedni poziom zabezpieczeń Komisja UE w swoich zaleceniach 2020/518 wskazuje, że czynnikiem ważnym przy korzystaniu z aplikacji jest zapewnienie „że dane będą chronione z wykorzystaniem odpowiednich zabezpieczeń" Zgodnie z arkuszem Oceny skutków dla ochrony danych (DPIA) „ProteGO Safe zaprojektowano w taki sposób, aby minimalizować zagrożenia dla prywatności i bezpieczeństwa osób i społeczności oraz zagwarantować najwyższy poziom ochrony danych". Dane przechowywane są na urządzeniach końcowych użytkowników; wprowadzane do pamięci urządzenia dane umożliwiają zachowanie anonimowości użytkowników; tylko osoby zweryfikowane medycznie jako chore na COVID-19 mogą zainicjować proces wysłania kluczy diagnostycznych.	BRAK	Brak konieczności podejmowania dodatkowych działań.
57.	• cel przetwarzania danych osobowych Zgodnie z zaleceniami 2020/518 pozyskiwane dane powinny być „stosowane wyłącznie w celu ostrzegania osób, które mogły być narażone na kontakt z wirusem". Zgodnie z przygotowaną przez GIS oraz Ministerstwo dokumentacją towarzyszącą aplikacji ProteGO Safe, dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. c) i e) RODO w związku z realizacją zadania w interesie publicznym. Celem aplikacji ProteGO Safe jest wsparcie społeczeństwa w przeciwdziałaniu rozprzestrzeniania się infekcji wirusem COVID-19. Dane otrzymane od użytkowników z pozytywnym wynikiem testu na Covid-19 są przetwarzane centralnie, pozostałe zaś dane są przechowywane lokalnie na urządzeniach użytkowników. Zgodnie z §3 pkt 1 Polityki prywatności aplikacja ProteGO Safe przetwarza informacje niebędące danymi osobowymi wyłącznie w celach: przeciwdziałania pandemii COVID-19; zanonimizowanego profilowania w ramach Modułu Analitycznego w celu przeciwdziałania pandemii COVID-19; korzystania przez użytkownika z aplikacji zgodnie z Regulaminem; analiza, organizowanie i ulepszanie ProteGO Safe w oparciu o dane statystyczne.	BRAK	Brak konieczności podejmowania dodatkowych działań.
58.	• zakaz udostępniania danych stronom trzecim Zgodnie z zaleceniami 2020/518 „wykluczone jest udostępnianie danych stronom trzecim". Aplikacja ProteGO Safe nie informuje użytkownika o tożsamości czy kluczach urządzeń innych użytkowników, w szczególności tych, które potwierdziły kontakt epidemiologiczny i w konsekwencji jego zaistnienia zwiększyły ryzyko. Aplikacja nie przekazuje również użytkownikom odbierającym klucz diagnostyczny informacji o dacie czy czasie kontaktu z osobą zidentyfikowaną jako zakażona, przez co redukuje ryzyko identyfikacji osoby zakażonej przez użytkownika..	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Z uwagi na brak dostępu do danych osobowych zapisywanych lokalnie w urządzeniu użytkownika, wykorzystanie danych w celach innych niż pierwotnie określone, w tym w celach niezwiązanych z pierwotnymi celami przetwarzania danych, nie jest możliwe. Dane osobowe w aplikacji są szyfrowane przy wykorzystaniu nowoczesnych rozwiązań kryptograficznych. Dostęp do nich możliwy jest jedynie poprzez nieuprawnione i niezgodne z prawem złamanie zabezpieczeń telefonu.		
59.	• **zatwierdzanie przez organ ds. zdrowia** Zgodnie z zaleceniami 2020/518 jednym z warunków skuteczności aplikacji mobilnych jest zatwierdzenie jej przez organ ds. zdrowia. Aplikacja ProteGo Safe powstała przy udziale i za aprobatą Ministra Zdrowia. Zgodnie z Polityka prywatności Minister Zdrowia może być także odbiorcą zanonimizowanych danych i informacji z ProteGO Safe.	BRAK	Brak konieczności podejmowania dodatkowych działań.
60.	• **zintegrowany system zarządzania – współpraca pomiędzy organami administracji publicznej** Komisja UE w swoich zaleceniach 2020/518 wskazuje, że „instrumentem przydatnym w procesie przygotowania i wdrożenia środków (aplikacji) jest system zintegrowanego zarządzania, obejmujący nie tylko organy ds. zdrowia, ale również inne organy (w tym organy ochrony danych), a także sektor prywatny, ekspertów, pracowników naukowych i zainteresowane strony, takie jak grupy pacjentów". Ministerstwo zwracało się do PUODO z prośbą o wzięcie udziału w pracach nad ProteGO Safe. Organ nadzorczy istotnie wystosował swoje uwagi i zalecenia co do funkcjonowania aplikacji ProteGO Safe, zwrócił również uwagę na ważne dla ochrony prywatności zagadnienia (odpowiedź PUODO dostępna pod linkiem: https://pliki.panoptykon.org/DIP/Cyfrowy%20Nadz%C3%B3r%20-%20EOG%20I/Przychodz%C4%85ca%20-%20odpowiedzi%20na%20wniosek/UODO_dip_obowi%C4%85zkowo%C5%9B%C4%87%20ProteGO/odpowied%C5%BA%20w%20sprawie%20ProteGO_30.04.2020%20%282%29.pdf). ProteGO Safe było również poddawane testom bezpieczeństwa realizowanym przez trzy niezależne podmioty zewnętrzne (w tym testy Securitum, z których raport został opublikowany i dostępny jest pod adresem: https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport)	BRAK	Brak konieczności podejmowania dodatkowych działań.
61.	• **realizacja zasady minimalizacji danych** Komisja UE w swoich zaleceniach 2020/518 wskazała, że „zgodnie z zasadą minimalizacji danych organy ds. zdrowia publicznego i instytucje badawcze powinny przetwarzać dane osobowe jedynie w przypadku, gdy jest to odpowiednie, stosowne i ograniczone do tego, co jest konieczne". ProteGO Safe działa w związku z realizacją przez GIS zadań w interesie publicznym, wynikających z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej. Zadaniem aplikacji ProteGO Safe jest dostarczenie narzędzia asystującego i chroniącego użytkownika i jego bliskich przed rozprzestrzenianiem się COVID-19. W tym celu aplikacja przechowuje informacje o okresie kontaktu urządzeń użytkowników oraz o dacie kontaktu. Informacje o miejscu i czasie kontaktu nie są przechowywane.	BRAK	Brak konieczności podejmowania dodatkowych działań.

62.	• szyfrowanie i pseudonimizacja Komisja UE w swoich zaleceniach 2020/518 wskazuje, że w celu realizacji zasady minimalizacji danych konieczne jest stosowanie „odpowiednich zabezpieczeń, takich jak pseudonimizacja, agregacja, szyfrowanie i decentralizacja". ProteGO Safe w momencie instalacji i inicjowania działania nie wymaga podania danych osobowych. Użytkownik może wprowadzić swoją nazwę, która nie powinno być jednak nazwisko. Dane osobowe mogą zostać podane przez użytkownika wyniku korzystania z dodatkowych funkcji aplikacji. Wszystkie informacje przetwarzane przez ProteGO Safe zbierane i przetwarzane są w taki sposób, aby uniemożliwić identyfikację użytkowników. Serwer ProteGO Safe nie umożliwia także przechowywania lub połączenia (porównania) kluczy dziennych z kluczami diagnostycznymi. Cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu rekomendowanych bibliotek kryptograficznych. W momencie przesyłania klucza diagnostycznego po wprowadzeniu przez osobę chorą kodu PIN w aplikacji, dane w transporcie są kodowane przy użyciu standardu TLS (aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej).	BRAK	Brak konieczności podejmowania dodatkowych działań.
63.	• anonimizacja i agregacja danych Komisja UE w swoich zaleceniach 2020/518 wskazuje na konieczność „wykorzystywania w miarę możliwości zanonimizowanych i zagregowanych danych". Dane wprowadzane do Aplikacji ProteGO Safe umożliwiają zachowanie anonimowości użytkowników. Nie jest konieczna rejestracja, ani podawanie jakichkolwiek danych identyfikujących. Po instalacji aplikacji użytkownik może podać swoją nazwę, która może być dowolna. Aplikacja informuje Użytkownika, że nazwą nie powinno być jego nazwisko. Wszelkie identyfikatory są generowane w sposób uniemożliwiający ich powiązanie z konkretnym urządzeniem lub użytkownikiem. Co więcej zgodnie z arkuszem Oceny skutków dla ochrony danych (DPIA) „serwer nadający anonimowe identyfikatory oraz serwer przesyłający klucze diagnostyczne nie są ze sobą połączone. Identyfikacja osób chorych na COVID-19 jest niemożliwa z perspektywy aplikacji ProteGO Safe i serwerów ProteGO Safe".	BRAK	Brak konieczności podejmowania dodatkowych działań.
64.	• decentralizacja procesu Komisja UE w swoich zaleceniach 2020/518 za jeden z instrumentów służących zapewnieniu bezpieczeństwa danych uznaje decentralizację. Systemy zdecentralizowane eliminują potrzebę centralnego serwera i polegają na wielu serwerach lub użytkownikach końcowych w celu zrealizowania zadania. W aplikacji ProteGO Safe dane przechowywane są na urządzeniach końcowych użytkowników. Wszystkie informacje (w tym w szczególności wpisy w Dzienniku Zdrowia), a także historia spotykanych urządzeń są przechowywane na urządzeniach końcowych użytkowników i tam analizowane.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Na serwer mogą zostać przesłane jedynie dane zgromadzone przez osoby zweryfikowane przez Centrum Kontaktu jako osoby chore. Jest to tymczasowe Temp ID aplikacji oraz analogicznie tymczasowe Temp ID aplikacji innych użytkowników, modele urządzeń i siła ich sygnału. Tylko osoby zweryfikowane medycznie jako chore na COVID-19 mogą zainicjować proces wysłania swoich kluczy diagnostycznych (warunkiem niezbędnym jest wcześniejszy dobrowolny kontakt osoby chorej z Centrum Kontaktu), aby można było wysłać ostrzeżenie dla innych użytkowników. Serwer backend jest utrzymywany przez Ministerstwo Cyfryzacji.		
65.	• **brak gromadzenia danych o przemieszczaniu się osób fizycznych** Komisja UE w swoich zaleceniach 2020/518 za jedną z zasad korzystania z aplikacji mobilnych uznaje: „preferowanie najmniej inwazyjnych, ale skutecznych środków (...) oraz unikanie przetwarzania danych o lokalizacji lub przemieszczaniu się poszczególnych osób". Aplikacja ProteGO Safe dla ustalenia kontaktu pomiędzy urządzeniami końcowymi użytkowników wykorzystuje technologię Bluetooth (BLE). Nie korzysta z technologii geolokalizacyjnych. Aplikacja przechowuje informacje o okresie kontaktu urządzeń użytkowników oraz o dacie kontaktu. Informacje o miejscu i czasie kontaktu nie są przechowywane.	BRAK	Brak konieczności podejmowania dodatkowych działań.
66.	• **konsultacje z organami ochrony danych** Komisja UE w swoich zaleceniach 2020/518 wskazuje, że „konsultacje z organami ochrony danych, zgodnie z wymogami określonymi w unijnych przepisach dotyczących ochrony danych osobowych, są konieczne, aby zapewnić zgodne z prawem przetwarzanie danych osobowych oraz przestrzeganie praw zainteresowanych osób". W ramach prac nad aplikacja ProteGO Safe odbyły się konsultacje z organem nadzorczym. Prezes Urzędu Ochrony Danych Osobowych wystosował swoje uwagi i zalecenia co do funkcjonowania aplikacji ProteGO Safe, zwrócił również uwagę na ważne dla ochrony prywatności zagadnienia.	BRAK	Brak konieczności podejmowania dodatkowych działań.
67.	• **interoperacyjność aplikacji** Komisja UE w swoich zaleceniach 2020/518 wskazuje na istotę „wspieranie wymogów (...) dotyczących interoperacyjności i wspierania wspólnych rozwiązań". Aplikacja ProteGO Safe, zgodnie z zapowiedziami Ministra Cyfryzacji, będzie współdziałała z innymi europejskimi aplikacjami służącymi do powiadamiania o kontakcie z wirusem SARS CoV-2. Obecnie państwa UE, pod przewodnictwem Komisji Europejskiej, pracują nad współdziałaniem oficjalnych, krajowych aplikacji tego typu. Pierwszym porozumieniem w tym zakresie jest porozumienie krajów członkowskich współpracujących z Komisją Europejską w ramach sieci eHealth Network dotyczące bezpiecznej wymiany informacji między krajowymi aplikacjami. GIS i inne organy zdrowia publicznego podjęły dialog celem ustalenia zasad interoperacyjności. Na dzień przeprowadzenia niniejszego audytu prywatności, rozmowy nie zostały zakończone a ustaleń nie podjęto.		Należy kontynuować podjęte rozmowy z organami zdrowia publicznego celem wypracowania zasad interoperacyjności.
68.	• **poszanowanie przepisów dotyczących ochrony danych osobowych i poufności**	BRAK	

	Komisja UE w swoich zaleceniach 2020/518 wskazuje na potrzebę istnienia „zabezpieczeń zapewniających poszanowanie praw podstawowych i zapobieganie stygmatyzacji, w szczególności mających zastosowanie przepisów dotyczących ochrony danych osobowych i poufności komunikacji". W przeprowadzonej ocenie skutków dla ochrony danych (DPIA) została zawarta ocena niezbędności i proporcjonalności środków ochrony, która nie wykazała uchybień w zakresie stosowanych zabezpieczeń. Korzystanie z Aplikacji ProteGO jest dobrowolne, a zachowane standardy bezpieczeństwa zapobiegają stygmatyzacji osób z niej korzystających. Dane wprowadzane do ProteGO Safe umożliwiają zachowanie anonimowości użytkowników. Nie jest konieczna rejestracja, ani podawanie jakichkolwiek danych identyfikujących. Wszelkie identyfikatory są generowane w sposób uniemożliwiający ich powiązanie z konkretnym urządzeniem lub użytkownikiem. Co więcej zgodnie z arkuszem Oceny skutków dla ochrony danych (DPIA) „serwer nadający anonimowe identyfikatory oraz serwer przesyłający klucze diagnostyczne nie są ze sobą połączone. Identyfikacja osób chorych na COVID-19 jest niemożliwa z perspektywy aplikacji ProteGO Safe i serwerów ProteGO Safe".		Brak konieczności podejmowania dodatkowych działań.
69.	• **istnienie wymogów technicznych dotyczących odpowiednich technologii** Komisja UE w swoich zaleceniach 2020/518 wskazuje na konieczność istnienia „wymogów technicznych dotyczących odpowiednich technologii służących ustaleniu bliskości urządzenia, szyfrowania, ochrony danych, przechowywania danych na urządzeniu przenośnym, możliwego dostępu organów ds. zdrowia oraz przechowywania danych". Aplikacja ProteGO Safe wykorzystuje powszechnie znane technologie i algorytmy, w tym technologię Bluetooth Low Energy (BLE), czyli technologię komunikacji bezprzewodowej urządzeń końcowych, pozwalającą na ochronę zużycia baterii. Aplikacja wymaga użycia WiFi lub danych komórkowych jedynie w momencie przesyłania kluczy diagnostycznych po wprowadzeniu przez osobę chorą kodu PIN w aplikacji. Dane osobowe w aplikacji są szyfrowane przy wykorzystaniu nowoczesnych rozwiązań kryptograficznych. Dostęp do nich możliwy jest jedynie poprzez nieuprawnione i niezgodne z prawem złamanie zabezpieczeń telefonu. ProteGO Safe nie korzysta z technologii geolokalizacyjnych. Wszystkie informacje (w szczególności wpisy w Dzienniku Zdrowia), a także historia spotykanych urządzeń są przechowywane na urządzeniach końcowych użytkowników i tam analizowane. Aplikacja przechowuje informacje o okresie kontaktu urządzeń końcowych użytkowników oraz o dacie kontaktu. Informacje o miejscu i czasie kontaktu nie są przechowywane. Na serwer mogą zostać przesłane jedynie dane zgromadzone przez osoby zweryfikowane przez Centrum Kontaktu. Tylko osoby zweryfikowane medycznie jako chore na COVID-19 mogą zainicjować proces wysłania swoich kluczy diagnostycznych.	BRAK	Brak konieczności podejmowania dodatkowych działań.
70.	• **cyberbezpieczeństwo**		

	Komisja UE w swoich zaleceniach 2020/518 wskazuje na konieczność „istnienia skutecznych wymogów w zakresie cyberbezpieczeństwa w celu ochrony dostępności, autentyczności, integralności i poufności danych". Kompleksowa ocena ryzyka z punktu widzenia ochrony danych osobowych i informacji przetwarzanych przez ProteGO Safe została przeprowadzona i udokumentowana w skoroszycie 3 „Ocena i zarządzanie ryzykiem" arkusza Oceny skutków dla ochrony danych (DPIA). Ustalony poziom ryzyka znajduje swoje potwierdzenie w testach bezpieczeństwa, m.in. przeprowadzonych przez Securitum (raport z przeprowadzonego testu bezpieczeństwa dostępny tutaj: https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport). Ministerstwo regularnie zleca retesty aplikacji, w tym również przed wprowadzeniem kolejnej wersji oprogramowania lub innych znaczących zmian. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, stosowne procedury w zakresie kooperacji i udostępniania informacji oraz stosowne procedury reagowania na incydenty, zawierające m.in. procedury powiadamiania oraz zarządzania incydentami i podatnościami zostały wdrożone i obowiązują. Kod źródłowy aplikacji ProteGO Safe został podany do wiadomości publicznej i jest dostępny do zapoznania się. Każdy może przeanalizować kod. MC oraz inne podmioty odpowiedzialne wyznaczyły kanały raportowania błędów i zidentyfikowanych podatności. Użytkownik aplikacji, który napotkał błąd, może bez problemu zgłosić go bezpośrednio z poziomu aplikacji, może również ocenić produkt i wskazać istnienie błędów np. w formie komentarzy w Sklepie Google (zapoznając się z treścią sekcji „Oceny i opinie" w Sklepie Google zauważyć można, że Ministerstwo odpowiada na większość feedbacków dociekając szczegółów błędu). Zastosowano rozwiązania pozwalające na zachowanie minimalizacji danych; ograniczenie przechowywania danych; szyfrowanie, pseudonimizację i anonimizację. Podczas pracy z aplikacją wielokrotnie weryfikowano, o przyznanie jakich uprawnień aplikacja prosi użytkownika. Pomijając prośbę o wyrażenie zgody na korzystanie z modułów Bluetooth, aplikacja nie wskazuje na konieczność przyznania innych, dodatkowych uprawnień. Zauważyć należy również, że o uprawnienia te aplikacja prosi w toku działania użytkownika (system nie przyznaje aplikacji uprawnień automatycznie, co dotyczy również korzystania z modułu Bluetooth – użytkownik musi podjąć działanie, by aplikacja mogła korzystać z technologii Bluetooth), tak wiec zastosowano prawidłowy model opt-in, zgodny z zasadą privacy by default. Przy ProteGO Safe co do zasady zrezygnowano z komunikacji przez sieć bezprzewodową WiFi oraz sieci komórkowe. Niemniej do transmisji takiej dochodzić będzie w przypadku komunikowania aplikacji użytkownika będącego osobą chorą, który zainicjował dystrybucję klucza diagnostycznego, z serwerem ProteGO Safe. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, rozwiązania zapewniające realizację powyższych zaleceń zostały wdrożone i obowiązują. Deweloperzy przy tworzeniu aplikacji korzystali z dobrze		ProteGO Safe nie jest aplikacją antywirusową. Użytkownik musi mieć na względzie bezpieczeństwo swojego urządzenia nie tylko podczas lub w związku z korzystaniem z aplikacji ProteGO Safe, ale na co dzień. Ryzyko jest niezależne od podmiotów odpowiedzialnych za operacyjność ProteGO Safe, niemniej jednak dostrzegalne, a w konsekwencji konieczne do wskazania w ramach ryzyk. Przy analizie ryzyka wzięto pod uwagę możliwe konsekwencje związane z korzystaniem z aplikacji ProteGO Safe z wykorzystaniem urządzeń końcowych zainfekowanych złośliwym oprogramowaniem lub rootowanych. Dla dalszego podniesienia bezpieczeństwa danych przechowywanych w aplikacji ProteGO Safe można rozważyć rozwiązanie polegające na zabezpieczeniu aplikacji hasłem lub kodem PIN (w momencie uruchamiania aplikacji, by wejść do niej, użytkownik musiałby wpisywać samodzielnie ustalony, dodatkowy kod zabezpieczający aplikację przed dostępem osób przypadkowych, np. korzystających z telefonu użytkownika aplikacji).

	znanych i rekomendowanych algorytmów i protokołów kryptograficznych. Szczególną uwagę poświęcono wymaganiom dla zapewnienia odpowiedniego wykorzystania każdego algorytmu i protokołu (np. random initialization vectors or nonces). Zaimplementowano także mechanizmy bezpieczeństwa przed przekazaniem/odtworzeniem identyfikatora (Identifier relay/replay prevention). Aplikacja ProteGO Safe zaprojektowana została w taki sposób, by każdy mógł jej używać (co osiągnięto poprzez ustalenie minimalnych wymagań sprzętowych, wykorzystanie powszechnie wspieranych technologii i algorytmów, rozwiązania pozwalające na ochronę zużycia baterii tj. korzystanie z technologii Bluetooth Low Energy (BLE) w urządzeniach wspierających tę technologię, zapewnienie dostępności aplikacji u największych dostawców systemów operacyjnych urządzeń mobilnych: w Sklepie Google i AppStore od Apple). Aplikacja nie wymaga skomplikowanej konfiguracji, przez co zredukowano ryzyko wystąpienia błędów konfiguracyjnych. Z uwagi na lokalny charakter działania ProteGO Safe, podmioty odpowiedzialne mają mniejszą możliwość lub brak możliwości ingerowania w system i stan bezpieczeństwa urządzenia użytkownika. Aplikacja nie jest przystosowana do przeprowadzania testów „onboarding security", w tym zakresie użytkownik musi samodzielnie zadbać o stan swojego urządzenia. ProteGO Safe jako aplikacja działająca lokalnie nie posiada dodatkowych zabezpieczeń uwierzytelniających użytkownika. Niemniej inicjacja transmisji danych (dystrybucji klucza diagnostycznego) jest zabezpieczona dodatkowym uwierzytelnieniem. Podmioty odpowiedzialne i zespoły projektowe zdają sobie sprawę z zagrożenia, jakie niesie ze sobą korzystanie ze starszych wersji systemów operacyjnych i starszych technologii na urządzeniach, na których instalowana jest aplikacja ProteGO Safe. Ryzyka związane z korzystaniem z niezabezpieczonych urządzeń mobilnych zostały wzięte pod uwagę podczas przeprowadzania analizy ryzyka i zrównoważone z wykorzystaniem adekwatnych środków zabezpieczających.		
71.	• **dezaktywacja aplikacji po okresie pandemii** Komisja UE w swoich zaleceniach 2020/518 podkreśla, że „wygaśnięcie zastosowanych środków i usunięcie danych osobowych uzyskanych za pomocą tych środków [powinno nastąpić] najpóźniej w momencie, w którym ogłoszone zostanie opanowanie pandemii" Niezbędny jest „regularny przegląd dalszej konieczności przetwarzania danych osobowych do celów walki z kryzysem wywołanym przez COVID-19 oraz ustanowienie odpowiednich klauzul wygaśnięcia". Zgodnie z założeniami projektowymi, o których użytkownicy są informowani w dokumentacji towarzyszącej aplikacji (Regulaminie ProteGO Safe (v.4.2.), Polityce prywatności ProteGO Safe (v.4.2.) oraz w opublikowanym przez Ministerstwo arkuszu Oceny skutków dla ochrony danych (DPIA)), aplikacja zostanie wyposażona w możliwość zdalnej dezaktywacji w momencie zakończenia pandemii COVID-19 lub stanu zagrożenia pandemicznego w następnej wersji oprogramowania. Na moment przeprowadzania audytu prywatności oraz opracowywania niniejszego raportu, zalecenie to nie jest spełnione.		Dla pełnej zgodności przetwarzania danych osobowych w aplikacji ProteGO Safe z wytycznymi KE należy uzupełnić możliwość zdalnej dezaktywacji aplikacji w momencie zakończenia pandemii COVID-19 lub stanu zagrożenia pandemicznego. Wstępne założenia projektowe zakładają już wprowadzenie takiego rozwiązania, a prace w tym kierunku zostały podjęte.

	Zgodnie z uzyskanymi od podmiotów odpowiedzialnych informacjami, z uwagi na obawy o nieproporcjonalną ingerencję w prywatność (pełna realizacja, zakładająca usunięcie aplikacji wraz z danymi w niej przechowywanymi z urządzenia użytkownika wymagałaby technicznych rozwiązań umożliwiających zdalny dostęp podmiotów odpowiedzialnych do urządzenia końcowego użytkownika, co z uwagi na poszanowanie prywatności użytkowników jest niemożliwe do realizacji) oraz możliwe konsekwencje w postaci spadku zaufania do podmiotów publicznych oraz tego typu aplikacji i programów, rozwiązania, które choćby w stopniu potencjalnym wymagały ingerencji w urządzenia końcowe użytkownika nie są rozważane. Podmioty odpowiedzialne rozważają alternatywne możliwości dezaktywacji aplikacji, które nie będą wymagać dostępu do urządzenia końcowego użytkownika, w tym wprowadzenie rozwiązań umożliwiających zachowanie danych lub ich eksport po okresie pandemii, ewentualne pozostawienie możliwości korzystania z aplikacji ProteGO Safe po zakończeniu pandemii z jednoczesnym ograniczeniem funkcjonalności aplikacji, np. do funkcji informowania o prawach i obowiązkach, aktualnej sytuacji epidemiologicznej. Podmioty odpowiedzialne podjęły konsultacje z interesariuszami projektu ProteGO Safe, zgodnie z uzyskanymi informacjami planowane jest również przeprowadzenie konsultacji ze społecznością GitHub oraz Komisją Europejską.		
72.	• **metoda ostrzegania** Komisja UE w swoich zaleceniach 2020/518 jako zasadę statuuje „wysyłanie danych dotyczących bliskości fizycznej w przypadku potwierdzonego zakażenia i stosowanie odpowiednich metod ostrzegania osób, które pozostawały w bliskim kontakcie z osobą zakażoną – która pozostaje anonimowa". W aplikacji ProteGo Safe tylko osoby zweryfikowane medycznie jako chore na COVID-19 mogą zainicjować proces wysłania swoich kluczy diagnostycznych (warunkiem niezbędnym jest wcześniejszy kontakt osoby chorej z Centrum Kontaktu) aby można było wysłać ostrzeżenie dla innych użytkowników. Przekazanie informacji w przypadku zidentyfikowania u użytkownika choroby COVID-19 jest w pełni dobrowolne. W przypadku wysłania klucza diagnostycznego podmiot dostarczający i operujący aplikacją wciąż nie ma dostępu do danych osobowych użytkownika zapisanych w aplikacji. Identyfikacja użytkownika, z uwagi na brak innych danych umożliwiających jednoznaczne wskazanie tożsamości osoby fizycznej, pozostaje niemożliwa.	BRAK	Brak konieczności podejmowania dodatkowych działań.
73.	• **przejrzystość ustawień prywatności** Komisja UE w swoich zaleceniach 2020/518 wymaga „istnienia wymogów przejrzystości dotyczących ustawień prywatności w celu zapewnienia zaufania do aplikacji" oraz „regularnego przekazywanie jasnych informacji". Informacje o podmiotach odpowiedzialnych za dostarczanie oprogramowania ProteGO Safe są łatwo dostępne - przy instalowaniu aplikacji, zarówno w AppStore jak i w Sklepie Google, wyświetla się informacja, że oferentem oprogramowania ProteGO Safe jest Ministerstwo Cyfryzacji. Cele przetwarzania danych i zakres		Zgodnie z najlepszą praktyką, wskazane jest zamieszczenie w ekranie umożliwiającym potwierdzenie zapoznania się i akceptację Regulaminu oraz Polityki prywatności ProteGO Safe skróconej wersji klauzuli informacyjnej, zawierającej minimum informacji niezbędnych do uznania działań podejmowanych przez

	zbieranych danych wskazane są w Polityce prywatności, z która należy zapoznać się przed rozpoczęciem użytkowania aplikacji. Klauzula informacyjna została zawarta jedynie w treści Polityki prywatności. Należy ocenić, że klauzula ta powinna znaleźć się w formularzu (patrz: rubryka 2).		użytkownika aplikacji ProteGO Safe za świadome. Z informacji uzyskanych od podmiotów odpowiedzialnych za ProteGO Safe wynika, że zmiana w tym zakresie jest obecnie projektowana. W następnych wersjach aplikacji ProteGO Safe zostanie wprowadzony dodatkowy ekran zawierający treść odpowiadającą wymaganemu zakresowi informacji dla pierwszej warstwy klauzuli informacyjnej. Alternatywnie rozważane jest również dodanie takiej treści na ekranie, który umożliwia akceptację Regulaminu i Polityki prywatności podczas inicjowania pracy z aplikacją. Projektowana zmiana doprowadzi do pełnej eliminacji oznaczonego poziomu ryzyka.
74.	• **ograniczenie czasu przechowywania** Zgodnie z zaleceniami 2020/518 „usuwanie danych [powinno następować] zasadniczo po upływie 90 dni lub w każdym razie najpóźniej w momencie, w którym ogłoszone zostanie opanowanie pandemii". Zgodnie z tym założeniem z aplikacji ProteGO Safe po 14 dniach usuwane są następujące dane gromadzone lokalnie na urządzeniu: historia wyników analiz Modułu Analitycznego z ostatnich 14 dni, okres kontaktu urządzeń użytkowników, wartości w zakresie 5-30 minut oraz data kontaktu urządzeń użytkowników. Użytkownik może tez samodzielnie usunąć te dane. Usunięcie aplikacji przez użytkownika z telefonu skutkuje usunięciem danych przechowywanych w aplikacji. Klucze diagnostyczne są przechowywane na serwerze ProteGO Safe przez okres retencji wynoszący 14 dni w postaci zaszyfrowanej. Zgodnie z Polityką prywatności ProteGO Safe ma być aktywne jedynie przez okres pandemii COVID-19.	BRAK	Brak konieczności podejmowania dodatkowych działań.
	Wytyczne dotyczące aplikacji pomocniczych w walce z pandemią COVID-19 w odniesieniu do ochrony danych zawartych w komunikacie Komisji Europejskiej (KE) z dnia 17 kwietnia 2020 r. (2020/C 124 I/01) (dalej jako „**Wytyczne 2020/C 124 I/01**").		
	Zagadnienie	**Ryzyko**	**Proponowane działania**
75.	• **wiarygodność administratora zgodnie z wytycznymi KE (2020/C 124 I/01)** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[Z]e względu na wrażliwy charakter (...) danych osobowych oraz cele ich przetwarzania (...) aplikacje należy zaprojektować w taki sposób, by administratorem danych były krajowe organy ds. zdrowia (lub podmioty realizujące zadania w dziedzinie zdrowia w interesie publicznym)".	BRAK	Brak konieczności podejmowania dodatkowych działań. GIS spełnia kryteria wskazane w wytycznych KE, dotyczące ustalenia wiarygodnego

	GIS jest centralnym organem administracji rządowej, ustalającym kierunki działania organów Państwowej Inspekcji Sanitarnej oraz koordynującym i nadzorującym działalność tych organów, jak również inicjującym i nadzorującym czynności administracji rządowej zmierzające do zapobiegania i minimalizacji negatywnych skutków zdarzeń dotyczących zdrowia publicznego. GIS podlega ministrowi właściwemu do spraw zdrowia.		i odpowiedzialnego administratora dla danych przetwarzanych w aplikacjach pomocniczych w walce z pandemią COVID-19.
76.	• **kontrola użytkownika nad danymi osobowymi i prywatnością** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[D]ecydującym czynnikiem zaufania obywateli do aplikacji jest pokazanie, że mają kontrolę nad swoimi danymi osobowymi". Funkcjonowanie ProteGO Safe opiera się na następujących założeniach: – pobranie aplikacji i korzystanie z niej jest dobrowolne, podmioty zaangażowane promują korzystanie z oprogramowania i zachęcają do jego instalacji, jednak poza korzyściami związanymi z samymi funkcjami dostępnymi w aplikacji, nieużywanie jej nie generuje negatywnych konsekwencji dla osoby fizycznej; – pobranie aplikacji nie wymaga podawania żadnych danych osobowych użytkownika. Aplikacja w podstawowej wersji jest w stanie funkcjonować bez podawania przez Użytkownika danych osobowych. Korzystanie z dodatkowych funkcjonalności Modułu Analitycznego - wymaga wyrażenia stosownych zgód/nadania Aplikacji uprawnień. Korzystanie z Modułu Triażu oraz Modułu Dziennik Zdrowia wymaga podania danych osobowych. Pobranie Aplikacji oraz podanie innych danych jest dobrowolne, bez podania danych Aplikacja może spełniać podstawowe funkcje (Moduł Analityczny), ale korzystanie z dodatkowych modułów może być utrudnione; – dane dotyczące kontaktów i spotkań odnotowywane są lokalnie w urządzeniu użytkownika i nie podlegają transmisji zewnętrznej, z zastrzeżeniem sytuacji, gdy użytkownik zdiagnozowany jako nosiciel SARS CoV-2 lub osoba chora na COVID-19 dobrowolnie zdecyduje o wprowadzeniu numeru PIN i przesłaniu informacji do serwera ProteGO Safe w celu powiadomienia innych użytkowników, którzy mogli mieć kontakt z nim w ostatnim okresie; – użytkownik jest informowany o warunkach przetwarzania jego danych osobowych (za pomocą Regulaminu ProteGO Safe (v.4.2.) oraz Polityki prywatności ProteGO Safe (v.4.2.). Dostęp do tych dokumentów możliwy jest zarówno bezpośrednio z aplikacji (w trakcie inicjowania pracy aplikacji po jej pobraniu, w ustawieniach aplikacji – dokumenty otwierają się wewnątrz aplikacji, nie przekierowują na strony internetowe, co umożliwia uniknięcie zbierania ewentualnych danych śledzących, zarówno anonimowych jak i personalizowanych, w tym adresów IP). Ministerstwo, w imieniu podmiotów zaangażowanych w obsługę aplikacji, udostępniło również do wiadomości publicznej arkusz Oceny skutków dla ochrony danych (DPIA), który zawiera dokładny opis wykonanego badania DPIA. Do wiadomości publicznej podawane są również raporty z audytów i analiz dotyczących bezpieczeństwa i prywatności, w tym raport z przeprowadzonego audytu bezpieczeństwa aplikacji (https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport);		Przyjęte rozwiązania i środki bezpieczeństwa, w szczególności lokalny charakter przechowywania danych osobowych zgromadzonych za pośrednictwem aplikacji, pozostawiają pełną kontrolę nad przetwarzanymi danymi osobowymi użytkownikowi, a więc osobie, której dane dotyczą. Z informacji uzyskanych od podmiotów odpowiedzialnych za ProteGO Safe wynika, że zmiana w zakresie informacji dotyczących przetwarzania danych osobowych użytkownika jest obecnie projektowana. W następnych wersjach aplikacji ProteGO Safe zostanie wprowadzony dodatkowy ekran zawierający treść odpowiadającą wymaganemu zakresowi informacji dla pierwszej warstwy klauzuli informacyjnej, co efektywnie zwiększy poziom wiedzy użytkownika na temat przetwarzania jego danych osobowych, a tym samym kontrolę nad tymi danymi. Alternatywnie rozważane jest również dodanie takiej treści na ekranie, który umożliwia akceptację Regulaminu i Polityki prywatności podczas inicjowania pracy z aplikacją. Projektowana zmiana doprowadzi do pełnej eliminacji oznaczonego poziomu ryzyka Dla pełnej zgodności przetwarzania danych osobowych w aplikacji ProteGO Safe z wytycznymi KE należy uzupełnić możliwość zdalnej dezaktywacji aplikacji w momencie

	– z uwagi na lokalny charakter przechowywania danych, użytkownik w czasie rzeczywistym ma dostęp do wszystkich dotyczących go danych osobowych zarejestrowanych w aplikacji (poprzez odpowiedni moduł ustawień), w dowolnym momencie może również samodzielnie usunąć wszystkie dane przechowywane w aplikacji. Funkcjonowanie aplikacji umożliwia użytkownikowi realizację wszelkich praw podmiotowych przysługujących osobie, której dane dotyczą, samodzielnie i bezpośrednio za pomocą aplikacji (prawo dostępu do danych, uzyskania ich kopii, prawo do sprostowania danych, usunięcia danych). Wszelkie przypadku ograniczenia praw podmiotowych wynikających z przepisów prawa powszechnie obowiązującego zostały opisane w arkuszu Oceny skutków dla ochrony danych (DPIA); – zgodnie z założeniami projektowymi, o których użytkownicy są informowani w dokumentacji towarzyszącej aplikacji (Regulaminie ProteGO Safe (v.4.2.), Polityce prywatności ProteGO Safe (v.4.2.) oraz w opublikowanym przez Ministerstwo arkuszu Oceny skutków dla ochrony danych (DPIA)), aplikacja zostanie wyposażona w możliwość zdalnej dezaktywacji w momencie zakończenia pandemii COVID-19 lub stanu zagrożenia pandemicznego w następnej wersji oprogramowania.		zakończenia pandemii COVID-19 lub stanu zagrożenia pandemicznego.
77.	• **podstawy prawne przetwarzania danych osobowych osadzone w przepisach prawa** Zgodnie z treścią wytycznych 2020/C 124 I/01 „oparcie się na prawie jako podstawie prawnej przyczyniłby się do pewności prawnej, ponieważ prawo to (i) przewidywałoby szczegółowo przetwarzanie konkretnych danych dotyczących zdrowia i jasno określałoby cele przetwarzania; (ii) wyraźnie wskazywałoby, kto jest administratorem danych, tj. podmiotem przetwarzającym dane, i kto oprócz administratora może mieć dostęp do takich danych; (iii) wykluczałoby możliwość przetwarzania takich danych w celach innych niż te wymienione w prawodawstwie oraz (iv) przewidywałoby konkretne zabezpieczenia". Wysuwając takie twierdzenie KE kieruje się stanowiskiem, że „[W]szelkie przepisy krajowe muszą przewidywać konkretne i odpowiednie środki ochrony praw i wolności osób, których dane dotyczą. Zasadniczo im większy wpływ danego środka na swobody osób fizycznych, tym silniejsze zabezpieczenia należy przewidzieć w odpowiednich przepisach". GIS jako administrator danych osobowych przetwarza dane w oparciu o przepisy prawa, a dokładniej mówiąc dla realizacji swoich zadań ustawowych wynikających z ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (t. j. Dz. U. z 2019 r. poz. 59). Niestety, przepisy te zawierają zakres zadań, które GIS ma wykonywać, nie zawierają jednak dyspozycji kwalifikowanych jako obowiązki prawne. Brak w przepisach powszechnie obowiązujących szczegółowych regulacji dotyczących wyżej wskazanych zagadnień, wyszczególnionych w wytycznych, w szczególności informacji o wymaganych przepisami prawa, konkretnych zabezpieczeniach. W konsekwencji krajowy system prawny nie pozwala na powołanie się na art. 6 ust. 1 lit. c) RODO jako podstawę prawną przetwarzania w analizowanym przypadku. Właściwszym jest wskazanie art. 6 ust. 1 lit. e) RODO. Możliwa do przyjęcia podstawa prawna przetwarzania jest mniej stabilna niż miałoby to miejsce w przypadku istnienia obowiązku prawnego nałożonego na GIS, z drugiej jednak strony jest to podstawa legitymująca o dość stabilnym charakterze. Obszerna dokumentacja towarzysząca (w szczególności publikowaną Ocenę		Ryzyko jest niezależne od administratora – jego źródłem są przepisy prawa powszechnie obowiązującego. Komisja wspomina o art. 6 ust. 1 lit. e) RODO i choć preferowaną i stabilniejszą podstawą przetwarzania danych osobowych byłby istniejący obowiązek prawny (art. 6 ust. 1 lit. c) RODO), krajowy system prawa nie zawiera odpowiednich przepisów umożliwiających oparcie przetwarzania na tej podstawie legitymującej.

	skutków dla ochrony danych (DPIA) oraz raporty z testów bezpieczeństwa przeprowadzonych przez niezależne podmioty) dodatkowo wpływa na dalsze ustabilizowanie warunków przetwarzania i buduje wiarygodność przyjętych rozwiązań.		
78.	• **zakaz podejmowania decyzji wobec użytkownika opartej wyłącznie na zautomatyzowanym przetwarzaniu** W wytycznych 2020/C 124 I/01, „Komisja zwraca uwagę na zakaz poddawania osób fizycznych decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, która wywołuje skutek prawny lub w podobny sposób istotnie na te osoby wpływa (art. 22 RODO)". Celem aplikacji ProteGO Safe jest wsparcie użytkowników we wczesnej identyfikacji ryzyka zakażenia. Podmioty odpowiedzialne za funkcjonowanie aplikacji zaznaczają, że wskazania aplikacji nie są diagnozą medyczną oraz że powinny być interpretowane z uwzględnieniem odpowiedniego marginesu ostrożności. Wskazania aplikacji dotyczące wysokiego ryzyka zakażenia mogą być sygnałem wskazującym na potrzebę skontaktowania się ze służbami sanitarno-epidemiologicznymi, jednak nie zastępują takiego kontaktu, tym bardziej nie zastępują konieczności konsultacji medycznej z lekarzem. Automatyzacja przetwarzania występująca w ProteGO Safe dotyczy podejmowania decyzji w zakresie wskazania użytkownikowi stopnia zagrożenia. Informacja ta podawana jest jednak wyłącznie użytkownikowi, nie jest podstawą wnioskowania podmiotów zewnętrznych.	BRAK	Brak konieczności podejmowania dodatkowych działań. Aplikacja ani podmioty odpowiedzialne za jej funkcjonowanie nie podejmują decyzji wyłącznie w sposób zautomatyzowany. Automatyzm przetwarzania dotyczy pewnego ograniczonego zakresu, a wynikiem zautomatyzowanego przetwarzania jest wyłącznie wskazanie użytkownikowi, że znalazł się w grupie podwyższonego ryzyka zakażeniem SARS CoV-2.
79.	• **minimalizacja danych – rezygnacja z przechowywania informacji o czasie i miejscu kontaktu** Zgodnie z treścią wytycznych 2020/C 124 I/01 „nie wydaje się konieczne przechowywanie dokładnego czasu lub miejsca kontaktu (jeżeli informacje te są dostępne)". W innym miejscu KE zaznacza, że „dane dotyczące czasu i miejsca takich kontaktów nie powinny być przechowywane". Aplikacja ProteGO Safe nie przechowuje informacji o miejscu, w którym nastąpił kontakt pomiędzy dwoma użytkownikami aplikacji. Nie przechowuje również danych o czasie kontaktu (godzina kontaktu). Aplikacja przechowuje informacje o okresie kontaktu urządzeń użytkowników (jak długo urządzenia znajdowały się blisko siebie; wartości w zakresie 5-30 minut) oraz o dacie kontaktu.	BRAK	Brak konieczności podejmowania dodatkowych działań. Aplikacja ProteGO Safe przetwarza wyłącznie dane niezbędne do ustalenia kontaktu potencjalnie zakaźnego, unikając przy tym przechowywania informacji dodatkowych, tj. jak geolokalizacja kontaktu i godzina kontaktu.
80.	• **wykorzystanie standardów Bluetooth zamiast instrumentów geolokalizacji dla ustalania kontaktów** Zgodnie z treścią wytycznych 2020/C 124 I/01 „łączność między urządzeniami za pośrednictwem standardu Bluetooth Low Energy (BLE) do celów pomiarów bliskości fizycznej i bliskich kontaktów jest bardziej precyzyjna, a co za tym idzie odpowiedniejsza, niż wykorzystanie danych geolokalizacyjnych (GNSS/GPS lub dane dotyczące lokalizacji telefonów komórkowych). Standard BLE pozwala uniknąć możliwości śledzenia (w przeciwieństwie do danych geolokalizacyjnych). W związku z tym Komisja zaleca stosowanie danych pochodzących z łączności BLE (lub danych generowanych przez równoważną technologię) do celów ustalania bliskości fizycznej. Dane dotyczące lokalizacji nie są konieczne do celów funkcji ustalania kontaktów	BRAK	Brak konieczności podejmowania dodatkowych działań.

	zakaźnych, ponieważ ich zadaniem nie jest śledzenie przepływu osób lub egzekwowanie zaleceń". Co więcej, „należy zapewnić możliwość aktywacji Bluetooth bez konieczności aktywacji innych usług lokalizacji". Aplikacja ProteGO Safe dla ustalenia kontaktu pomiędzy urządzeniami użytkownika wykorzystuje technologię Bluetooth (BLE). Nie korzysta jednocześnie z technologii geolokalizacyjnych ani z transmisji danych za pomocą sieci komórkowych (wniosek bazowany na doświadczeniach empirycznych uzyskanych podczas korzystania z aplikacji ProteGO Safe). Technologia Bluetooth wykorzystywana przez ProteGO Safe nie wymaga aktywacji żadnych innych technologii lokalizacyjnych, w szczególności wskazanych powyżej.		
81.	• **technologia Bluetooth jako środek dbałości o rzetelność i poprawność danych dotyczących kontaktów** W wytycznych 2020/C 124 I/01, KE zaleca „korzystać z technologii, które umożliwiają bardziej precyzyjną ocenę, czy doszło do kontaktu (takich jak Bluetooth)". Aplikacja ProteGO Safe dla ustalenia kontaktu pomiędzy urządzeniami użytkownika wykorzystuje technologię Bluetooth (BLE).	BRAK	Brak konieczności podejmowania dodatkowych działań.
82.	• **decentralizacja procesu powiadamiania innych użytkowników o kontakcie z zarażoną osobą** W wytycznych 2020/C 124 I/01 KE wskazuje na istnienie dwóch alternatywnych sposobów przekazywania ostrzeżenia o kontakcie epidemiologicznym użytkownikom aplikacji. KE wskazuje za bardziej prawidłowe tzw. procedurę zdecentralizowaną. Założeniami procedury zdecentralizowanej jest przesyłanie ostrzeżenia „automatycznie za pośrednictwem aplikacji do bliskich kontaktów, gdy użytkownik powiadomi aplikację – za zgodą lub po potwierdzeniu przez organ ds. zdrowia, na przykład za pomocą kodu QR lub kodu TAN – że uzyskał pozytywny wynik testu (proces zdecentralizowany)". Należy zwrócić uwagę na parę ważnych zasad funkcjonowania ProteGO Safe, opisanych w arkuszu Oceny skutków dla ochrony danych (DPIA): – „informacje o otoczeniu użytkownika przechowywane są bezpośrednio w pamięci wewnętrznej jego Urządzenia. Przekazanie informacji w przypadku zidentyfikowania u Użytkownika choroby COVID-19 jest w pełni dobrowolne"; – „Moduł Analityczny inicjuje proces wysłania Klucza Diagnostycznego na Serwer ProteGO Safe, który następnie przekazuje Klucz Diagnostyczny do Urządzeń Użytkowników Aplikacji. W takim wypadku podmiot dostarczający i operujący Aplikacją wciąż nie ma dostępu do danych osobowych Użytkownika zapisanych w aplikacji, niemniej następuje komunikacja z Serwerem ProteGO Safe w zakresie Kluczy Diagnostycznych. Ich interpretacja jest możliwa wyłącznie przez Urządzenie Użytkownika, który odbiera Klucz Diagnostyczny, z uwagi na brak informacji dotyczących historii i analizy spotkań zapisanych na Serwerze ProteGO Safe. Identyfikacja Urządzenia Użytkownika, który wprowadził Kod PIN a tym samym zainicjował dystrybucję Kluczy Diagnostycznych jest teoretycznie możliwa, niemniej identyfikacja Użytkownika, z uwagi na brak innych danych umożliwiających jednoznaczne wskazanie tożsamości osoby	BRAK	Brak konieczności podejmowania dodatkowych działań. Zgodnie z zaleceniami KE, proces powiadamiania o kontaktach niosących potencjalne zagrożenie epidemiologiczne został zdecentralizowany. Serwer ProteGO Safe stanowi wyłącznie środek pośredniczący w wymianie kluczy diagnostycznych pomiędzy aplikacjami końcowymi zainstalowanymi na urządzeniach końcowych użytkowników. Interpretacja informacji zawartych w kluczu diagnostycznym odbywa się w urządzeniu końcowym użytkownika-odbiorcy informacji z serwera ProteGO Safe. Inicjacja procesu przekazywania klucza diagnostycznego jest zabezpieczona za pomocą kodu PIN (generowanym w sposób losowy, jednorazowego użytku). Wpisanie kodu PIN w aplikacji ProteGO Safe jest dobrowolne.

	fizycznej, pozostaje niemożliwa (jedyną informacją, jaką dysponuje administrator, jest sygnał inicjujący wysyłkę Kluczy Diagnostycznych przez Serwer ProteGO Safe - istnieje możliwość, że Sewer odnotuje logi komunikacyjne, niemniej ich interpretacja i powiązanie z identyfikowalną osobą fizyczną pozostają niemożliwe)".		Dodatkowo zastosowano mechanizmy dynamicznych i losowych identyfikatorów użytkowników.
83.	• **tymczasowe i dynamiczne identyfikatory użytkowników** KE w wytycznych 2020/C 124 I/01 wskazuje, że działanie aplikacji typu ProteGO Safe powinno opierać się o „tworzenie i przechowywanie tymczasowych identyfikatorów użytkownika, które regularnie zmieniają się, a nie przechowywanie samego identyfikatora urządzenia". KE wskazuje, że tego typu „[A]plikacje generują pseudolosowo tymczasowe i okresowo zmieniające się identyfikatory telefonów, które pozostają w kontakcie z użytkownikiem". Zgodnie z informacjami zamieszczonymi w arkuszu Oceny skutków dla ochrony danych (DPIA) „aplikacja bazuje na losowych i dynamicznych (zmieniających się w czasie, zgodnie z ustalonym harmonogramem) kluczach Urządzenia Użytkownika". Krótkotrwałe ID zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne.	BRAK	Brak konieczności podejmowania dodatkowych działań.
84.	• **sposób generowania i przetwarzania danych na temat kontaktu** • **sposób przekazywania danych dotyczących kontaktu administratorowi i podmiotom odpowiedzialnym** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[D]ane na temat bliskości fizycznej powinny być generowane i przetwarzane wyłącznie wtedy, gdy istnieje rzeczywiste ryzyko zakażenia (w zależności od bliskości i czasu trwania kontaktu)". Aplikacja ProteGO Safe przechowuje identyfikatory urządzeń innych użytkowników, którzy weszli w kontakt z użytkownikiem wyłącznie lokalnie, z zastrzeżeniem aktywnego działania podejmowanego przez użytkownika będącego osobą chorą lub zakażoną SARS CoV-2. Dopiero w sytuacji zdiagnozowania użytkownika jako chorego lub jako nosiciela, użytkownik w sposób dobrowolny może zadecydować o powiadomieniu innych użytkowników o potencjalnych konsekwencjach epidemiologicznych zarejestrowanego kontaktu z nim.	BRAK	Brak konieczności podejmowania dodatkowych działań.
85.	• **minimalizacja danych transmitowanych administratorowi i podmiotom odpowiedzialnym** KE w wytycznych 2020/C 124 I/01 wskazuje, że „na serwer dostępny dla organów ds. zdrowia powinny trafiać jedynie te dane, które zostały przekazane przez użytkowników i które są niezbędne do osiągnięcia danego celu, o ile taka opcja jest przewidziana (tj. na serwer ładowane są wyłącznie dane dotyczące bliskich kontaktów osoby, u której badanie potwierdziło zakażenie COVID-19)". Dane przekazywane podczas komunikacji z serwerem ProteGO Safe, znane Ministrowi Cyfryzacji jak i GIS podmiotom przetwarzane w aplikacji ProteGO Safe to dane związane z wykorzystywaniem serwera zapewniającego przekazywanie Użytkownikom komunikatów:	BRAK	Brak konieczności podejmowania dodatkowych działań. Zakres danych przekazywanych do serwera ProteGO Safe jest minimalny, są to wyłącznie dane niezbędne do ustalenia przez urządzenie końcowe użytkownika odbierającego klucz

	– UID - losowy identyfikator Urządzenia Użytkownika, – Średni czas korzystania z Aplikacji przez Użytkowników (dane statystyczne, których nie można powiązać z poszczególnymi Użytkownikami). Serwer ProteGO Safe (Backend) nie umożliwia identyfikacji użytkownika ani połączenia (porównania) kluczy diagnostycznych (narażenia) z jakimikolwiek innymi danymi użytkownika.		diagnostyczny, czy wystąpił kontakt potencjalnie epidemiologiczny.
86.	• **szyfrowanie i pseudonimizacja** Zgodnie z treścią wytycznych 2020/C 124 I/01 należy zadbać o to, by „dane przechowywane były na urządzeniu końcowym użytkownika w zaszyfrowanej formie, przy zastosowaniu najnowocześniejszych technik kryptograficznych". KE zwraca również uwagę, że „[D]ane dotyczące bliskości fizycznej powinny być generowane i przechowywane na urządzeniu końcowym wyłącznie w zaszyfrowanej i spseudonimizowanej formie". Co więcej, zdaniem KE „[K]ażdy przekaz z urządzenia osobistego do krajowych organów ds. zdrowia powinien być szyfrowany". Krótkotrwałe ID, generowane losowe i dynamiczne (zmieniające się w czasie, zgodnie z ustalonym harmonogramem), zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Kluczowym jest używanie TLS w kodowaniu danych w transporcie gdy dochodzi do komunikacji poprzez WiFi lub dane komórkowe (przesyłania klucza diagnostycznego po wprowadzeniu przez osobę chorą kodu PIN w aplikacji, aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej). Deweloperzy przy tworzeniu aplikacji korzystali z dobrze znanych i rekomendowanych algorytmów i protokołów kryptograficznych. Szczególną uwagę poświęcono wymaganiom dla zapewnienia odpowiedniego wykorzystania każdego algorytmu i protokołu (np. random initialization vectors or nonces). Zaimplementowano mechanizmy bezpieczeństwa przed przekazaniem/odtworzeniem identyfikatora (Identifier relay/replay prevention).	BRAK	Brak konieczności podejmowania dodatkowych działań.
87.	• **ujawnianie informacji o tożsamości kontaktów z innymi użytkownikami, w tym kontaktów potencjalnie zakaźnych** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[O]soba zakażona nie powinna być informowana o tożsamości osób, z którymi miała kontakt prowadzący potencjalnie do konsekwencji epidemiologicznych, i które zostaną o tym powiadomione" oraz „[T]ożsamości osoby zakażonej nie należy ujawniać osobom, z którymi miała kontakt epidemiologiczny". ProteGO Safe, w przypadku zidentyfikowania osoby zakażonej, umożliwia anonimowe przesłanie informacji za pośrednictwem serwera ProteGO Safe do urządzeń końcowych (aplikacji) innych użytkowników, które to następnie dokonują interpretacji, czy kontakt epidemiologiczny zaistniał czy nie oraz dokonują niezbędnej korekty ustalonego ryzyka zakażenia użytkownika odbierającego klucz diagnostyczny. Aplikacja nie informuje	BRAK	Brak konieczności podejmowania dodatkowych działań. Informacja o kontakcie z osobą zakażoną jest komunikowana użytkownikowi wyłącznie poprzez powiadomienie o zaistnieniu kontaktu oraz o zwiększeniu ryzyka zagrożenia. Użytkownicy nie posiadają dostępu do danych, które mogłyby nawet pośrednio zidentyfikować

	użytkownika będącego osobą chorą o tożsamości czy kluczach urządzeń użytkowników, które potwierdziły kontakt epidemiologiczny i w konsekwencji jego zaistnienia zwiększyły ryzyko dla użytkowników. Aplikacja nie przekazuje również użytkownikom odbierającym klucz diagnostyczny informacji o dacie czy czasie kontaktu z osobą zidentyfikowaną jako zakażona.		miejsce kontaktu, a w konsekwencji umożliwić identyfikację osoby zakażonej.
88.	• **jednoznaczne określenie celów przetwarzania danych** W wytycznych 2020/C 124 I/01 KE wskazuje, że „[P]odstawa prawna (prawo Unii lub prawo państwa członkowskiego) powinna określać cel przetwarzania. Cel powinien być szczegółowo określony, tak aby nie było wątpliwości, jakiego rodzaju dane osobowe muszą zostać przetworzone w celu osiągnięcia pożądanego celu oraz jednoznaczny", jednocześnie jednak KE „zaleca dokładniejsze określenie celu (celów)". Zgodnie z treścią wiersza 2 „Opisu operacji przetwarzania" Oceny skutków dla ochrony danych (DPIA) „[C]elem przetwarzania danych w aplikacji ProteGO Safe jest wsparcie społeczeństwa w przeciwdziałaniu rozprzestrzeniania się pandemii COVID-19: działając w szeroko rozumianym interesie publicznym, administrator poprzez dystrybucję i zapewnienie operacyjności aplikacji ProteGO Safe wspiera szybką wymianę informacji pomiędzy osobami fizycznymi w ramach określonej społeczności, działając na rzecz profilaktyki zdrowia publicznego i przeciwdziałania rozprzestrzenianiu się wirusa SARS CoV-2 oraz choroby COVID-2, poprzez wymianę zanonimizowanych informacji dotyczących osób zakażonych oraz oprogramowanie umożliwiające analizę spotkań i kontaktów, jak również poprzez algorytmy umożliwiające ocenę ryzyka zarażenia".	BRAK	Brak konieczności podejmowania dodatkowych działań. Cel został określony w sposób tożsamy z zadaniami GIS wyszczególnionymi w przywoływanych przepisach ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej. Cel został uszczegółowiony, jest jednoznaczny i wskazuje na pożądany rezultat przetwarzania w sposób niebudzący wątpliwości.
89.	• **określenie czasu przechowywania danych** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[O]kres przechowywania danych powinien zależeć od istotności tych danych z medycznego punktu widzenia (zgodnie z celem aplikacji: okres inkubacji itd.) oraz uwzględniać realistyczny termin realizacji czynności administracyjnych, które być może będzie należało wykonać", a „[D]ane dotyczące bliskości fizycznej powinny być usuwane, jak tylko przestają być potrzebne do celów ostrzegania. Powinno to mieć miejsce najpóźniej po miesiącu (okres inkubacji plus margines) lub po tym, jak dana osoba została zbadana, a wynik okazał się negatywny". Dane użytkowników aplikacji są przechowywane wewnątrz aplikacji do czasu ich manualnego usunięcia przez użytkownika, do czasu usunięcia aplikacji ProteGO Safe z urządzenia końcowego lub usuwane automatycznie po upływie 14 dni od dnia ich wprowadzenia (w zależności od tego, które zdarzenie nastąpi wcześniej). Klucze diagnostyczne są przechowywane na serwerze ProteGO Safe przez okres 14 dni, a następnie automatycznie kasowane.	BRAK	Brak konieczności podejmowania dodatkowych działań. Okres retencji został ustalony na 14 dni od dnia wprowadzenia informacji do aplikacji lub do pamięci serwera.
90.	• **automatyzacja ograniczenia czasu przechowywania danych (instrumenty zapewniające automatyczne usuwanie danych)** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[M]ożna przewidzieć dodatkowe środki mające na celu zabezpieczenie przetwarzanych danych, w szczególności automatyczne usunięcie lub anonimizację danych po pewnym czasie".	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Klucze diagnostyczne (narażenia) są przechowywane na serwerze ProteGO Safe przez okres retencji wynoszący 14 dni, a następnie automatycznie kasowane. Możliwość przechowywania danych przez użytkownika na urządzeniu końcowym, gdzie zainstalowana jest aplikacja ProteGO Safe, ograniczona została poprzez wprowadzenie systemowego ograniczenia historii działania Modułu Analitycznego do 14 dni wstecz.		Wprowadzono automatyczne mechanizmy usuwania danych, gwarantujące, że dane nie będą przechowywane dłużej niż ustalony okres retencji.
91.	• **przechowywanie danych lokalnie (urządzenie końcowe użytkownika)** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[D]ane powinny być przechowywane na urządzeniu użytkownika". Dane osobowe użytkownika oraz inne informacje wprowadzane do aplikacji przez użytkownika są przechowywane lokalnie, na urządzeniu końcowym użytkownika. Urządzenie komunikując się bezpośrednio z innym urządzeniem na którym zainstalowana jest aplikacja ProteGO Safe przesyła bezpośrednio do tego urządzenia informację umożliwiającą ustalenie, że nastąpił kontakt (za pomocą technologii Bluetooth; w procesie nie uczestniczy zewnętrzny serwer lub inne urządzenie, nie wykorzystuje się technologii opartych na transmisjach danych sieciami bezprzewodowymi WiFi lub komórkowymi). Urządzenie komunikuje się z backendem (serwerem ProteGO Safe) wyłącznie w sytuacji, gdy do aplikacji użytkownika zidentyfikowanego jako osoba chora zostanie wprowadzony specjalny kod PIN – przesłaniu podlega wyłącznie klucz diagnostyczny.	BRAK	Brak konieczności podejmowania dodatkowych działań.
92.	• **publikacja kodu źródłowego aplikacji** W wytycznych 2020/C 124 I/01 „Komisja zaleca, aby kod źródłowy aplikacji został podany do wiadomości publicznej i był dostępny do wglądu". Kod źródłowy aplikacji został podany do wiadomości publicznej i jest dostępny do zapoznania się.	BRAK	Brak konieczności podejmowania dodatkowych działań.
93.	• **zaangażowanie organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (PUODO)** Zgodnie z treścią wytycznych 2020/C 124 I/01 „[O]rgany ochrony danych powinny być w pełni zaangażowane w prace nad aplikacją i konsultowane w tym zakresie oraz powinny nadzorować wprowadzanie takiej aplikacji" Ministerstwo zwracało się do PUODO z prośbą o wzięcie udziału w pracach nad ProteGO Safe. Organ nadzorczy istotnie wystosował swoje uwagi i zalecenia co do funkcjonowania aplikacji ProteGO Safe, zwrócił również uwagę na ważne dla ochrony prywatności zagadnienia (odpowiedź PUODO dostępna pod linkiem: https://pliki.panoptykon.org/DIP/Cyfrowy%20Nadz%C3%B3r%20-%20EOG%20I/Przychodz%C4%85ca%20-%20odpowiedzi%20na%20wniosek/UODO_dip_obowi%C4%85zkowo%C5%9B%C4%87%20ProteGO/odpowied%C5%BA%20w%20sprawie%20ProteGO_30.04.2020%20%282%29.pdf).	BRAK	Brak konieczności podejmowania dodatkowych działań. Prezes Urzędu Ochrony Danych Osobowych został poproszony o opinię na temat projektowanego rozwiązania oraz wyraził swoje stanowisko i przedstawił zalecenia.
94.	• **wykonanie oceny skutków dla ochrony danych osobowych (art. 35 RODO)** Zgodnie z treścią wytycznych 2020/C 124 I/01, zdaniem Komisji „przetwarzanie danych w kontekście aplikacji będzie się kwalifikować jako przetwarzanie na dużą skalę szczególnych kategorii danych osobowych (tj. danych dotyczących zdrowia), Komisja pragnie zwrócić uwagę na art. 35 RODO dotyczący oceny skutków dla ochrony danych".	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Ocena skutków dla ochrony danych (DPIA) została wykonana, a jej udokumentowana forma (arkusz Oceny skutków dla ochrony danych (DPIA)) został opublikowany, umożliwiając opinii publicznej zapoznanie się z ustaleniami poczynionymi w trakcie badania ryzyka i skutków przetwarzania dla ochrony danych.		
	eHealth Network: Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. Wersja 1.0 z dnia 15 kwietnia 2020 r. (dalej jako „**zalecenia eHealth**").		
	Zagadnienie	Ryzyko	Proponowane działania
95.	• EF-01: minimalizacja danych z uwzględnieniem adekwatności Zgodnie z treścią zaleceń eHealth (EF-01) minimalny i jednocześnie adekwatny zakres danych niezbędnych do ustalenia kontaktów to okres czasu, odległość i kontekst środowiskowy. Aplikacja ProteGO Safe przechowuje informacje o okresie kontaktu urządzeń użytkowników (jak długo urządzenia znajdowały się blisko siebie; wartości w zakresie 5-30 minut) oraz o dacie kontaktu. Celem aplikacji nie jest powiadamianie organów ds. zdrowia, a użytkowników aplikacji o ryzyku epidemiologicznym wynikającym z kontaktu z osobą zakażoną. Powyżej wskazany zakres danych jest niezbędny do ustalenia zwiększenia ryzyka, jednocześnie inne informacje i dane nie będą miały wpływ na ustalenie ryzyka zakażenia, zatem pozostają zbędne i z tego względu zrezygnowano z ich zbierania.	BRAK	Brak konieczności podejmowania dodatkowych działań.
96.	• EF-02, TF-02: epidemiologicznie uzasadniony okres retencji danych Zgodnie z treścią zaleceń eHealth (EF-02) okres retencji danych powinien pozostawać epidemiologicznie uzasadniony, a więc nie powinien przekraczać 14 lub 16 dni. Dane użytkowników aplikacji są przechowywane wewnątrz aplikacji do czasu ich manualnego usunięcia przez użytkownika, do czasu usunięcia aplikacji ProteGO Safe z urządzenia końcowego lub usuwane automatycznie po upływie 14 dni od dnia ich wprowadzenia (w zależności od tego, które zdarzenie nastąpi wcześniej). Klucze diagnostyczne są przechowywane na serwerze ProteGO Safe przez okres 14 dni, a następnie automatycznie kasowane.	BRAK	Brak konieczności podejmowania dodatkowych działań.
97.	• EF-03, EF-04, EF-06: informowanie użytkowników o zagrożeniu Zgodnie z treścią zaleceń eHealth (EF-03, EF-04, EF-06) państwa członkowskie powinny opracować mechanizmy notyfikowania użytkowników o zwiększeniu zagrożenia epidemiologicznego dla jednostki, uwzględniając przy tym, że informacja o wzroście zagrożenia powinna być przekazana bezzwłocznie. Aplikacja ProteGO Safe powiadamia osoby zagrożone z tytułu kontaktu potencjalnie epidemiologicznego bezzwłocznie po otrzymaniu i dopasowaniu klucza diagnostycznego do zgromadzonych danych dotyczących kontaktów z innymi użytkownikami. Komunikat wyświetlany jest bezpośrednio w aplikacji, dodatkowo użytkownik może być monitowany o ważnej informacji w aplikacji za pomocą powiadomienia push (o ile wyrażone zostały odpowiednie zgody i zezwolenia, a system wspiera powiadomienia typu push).	BRAK	Brak konieczności podejmowania dodatkowych działań.
98.	• EF-05: potwierdzanie zakażenia za pomocą zewnętrznych mechanizmów autoryzujących Zgodnie z treścią zaleceń eHealth (EF-05) potwierdzanie zakażenia użytkownika aplikacji ProteGO Safe powinno się odbywać z wykorzystaniem mechanizmów uwierzytelniających, co pomoże uniknąć	BRAK	Brak konieczności podejmowania dodatkowych działań.

	wprowadzania do aplikacji informacji nieprawdziwych lub nieadekwatnych. Organy ds. zdrowia lub inne uprawnione jednostki powinny mieć możliwość potwierdzenia, że użytkownik jest osobą zakażoną przed zainicjowaniem mechanizmów ostrzegania innych użytkowników. Uwierzytelnienie osoby chorej na COVID-19 następuje poprzez wprowadzenie do Aplikacji losowego numeru PIN podanego przez przedstawiciela Centrum Kontaktu, który nie umożliwia identyfikacji, generowanego w sposób losowy (jednorazowego użytku).		
99.	• **EF-07: decentralizacja procesu powiadamiania o zagrożeniu jako środek zapewnienia prywatności użytkowników** Zalecenia eHealth (EF-07) wskazują na dwa możliwe sposoby wymiany informacji pomiędzy użytkownikiem a podmiotami odpowiedzialnymi za funkcjonowanie aplikacji i w konsekwencji innymi użytkownikami, w zakresie związanym z powiadamianiem o kontaktach potencjalnie epidemiologicznych. Aplikacja ProteGO Safe wykorzystuje zdecentralizowany model wymiany informacji dla identyfikacji kontaktów potencjalnie epidemiologicznych. Model opiera się na następujących założeniach: – dane użytkownika są przechowywane wyłącznie lokalnie, na urządzeniu końcowym użytkownika, na którym zainstalowana jest aplikacja ProteGO Safe. Aplikacja generuje pseudolosowe tymczasowe i dynamiczne identyfikatory telefonów, które pozostają w kontakcie z użytkownikiem, które jednak nie zawierają informacji osobistych dotyczących użytkownika, w tym również numeru telefonu; – ostrzeżenie o kontakcie potencjalnie epidemiologicznym i zwiększeniu ryzyka zakażenia jest przekazywane użytkownikowi bezpośrednio z aplikacji. Po odebraniu i zinterpretowaniu klucza diagnostycznego przez urządzenie użytkownika odbierającego klucz, aplikacja ProteGO Safe automatycznie generuje ostrzeżenie adresowane do użytkownika. Proces interpretacji i dopasowania klucza diagnostycznego do historii kontaktów odbywa się w całości w pamięci urządzenia końcowego użytkownika, z wykorzystaniem lokalnie działających skryptów aplikacji ProteGO Safe; – klucz diagnostyczny jest przekazywany przez urządzenie użytkownika zidentyfikowanego jako osoba zakażona po wprowadzeniu kodu PIN, który jest generowany losowo i pozostaje kodem jednorazowego użytku. Kod PIN jest przekazywany użytkownikowi zidentyfikowanemu jako osoba chora przez Centrum Kontaktu, które posiada potwierdzenie pozytywnego wyniku u osoby chorej, nie posiada jednak żadnego powiązania z użytkownikiem i aplikacją ProteGO Safe zainstalowaną na urządzeniu użytkownika. Użytkownik zidentyfikowany jako osoba zakażona musi samodzielnie wprowadzić kod PIN do aplikacji (robi to dobrowolnie, Centrum Kontaktu ani żaden inny podmiot nie ma możliwości wymuszenia wprowadzenia kodu PIN w aplikacji). Dopiero wówczas proces ostrzegania zostanie zainicjowany.	BRAK	Brak konieczności podejmowania dodatkowych działań.
100.	• **EF-07: brak możliwości wzajemnego identyfikowania się użytkowników** Zgodnie z treścią zaleceń eHealth (EF-07) użytkownicy aplikacji nie powinni mieć możliwości identyfikowania siebie nawzajem.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Zakres danych udostępnianych pomiędzy użytkownikami aplikacji ograniczony jest do niezbędnego minimum - ogranicza się wyłącznie do danych niezbędnych zakodowanych w Kluczu Diagnostycznym, umożliwiających wskazanie ryzyka transmisji wirusa SARS CoV-2 od Użytkownika, u którego wykryto obecność wirusa lub chorobę COVID-19. Są to informacje odnotowywane automatycznie w aplikacji, dotyczące spotkania (okres i siła sygnału Bluetooth). Użytkownik nie ma możliwości dopasowania informacji zgromadzonej w aplikacji dotyczącej kontaktu do konkretnej osoby fizycznej, ponieważ aplikacja nie odnotowuje ani czasu (godziny) spotkania ani miejsca spotkania, a wyłącznie datę.		
101.	• EF-07: brak możliwości zidentyfikowania użytkowników przez organy ds. zdrowia i inne podmioty odpowiedzialne Zalecenia eHealth (EF-07) zwracają uwagę, by aplikacje wykorzystywane do wczesnego ostrzegania o kontaktach potencjalnie epidemiologicznych nie umożliwiały podmiotom zewnętrznym, tj. organom i jednostkom zaangażowanym w zapewnienie operacyjności aplikacji, dostępu do danych osobowych użytkowników, również w formie zagregowanej i zanonimizowanych. Deweloperzy ProteGO Safe, GIS oraz MC wykorzystali wszelkie technicznie dostępne środki do zapewnienia, że dane osobowe użytkowników aplikacji ProteGO Safe nie będą w żadnej formie przekazywane podmiotom zewnętrznym. Osiągnięto to przede wszystkim poprzez decentralizację procesu ostrzegania, lokalne przechowywanie danych wprowadzanych lub zbieranych przez użytkowników (w tym danych o kontaktach), jak również przez wykorzystanie technologii niebazujących na technikach śledzących (zamiast geolokalizacji, transmisji danych sieciami bezprzewodowymi WiFi czy sieciami komórkowymi, do ustalania kontaktów wykorzystano technologię Bluetooth (BLE)). Zgodnie z zasadami opisanymi w arkuszu Oceny skutków dla ochrony danych (DPIA) „[I]dentyfikacja Urządzenia Użytkownika, który wprowadził Kod PIN a tym samym zainicjował dystrybucję Kluczy Diagnostycznych jest teoretycznie możliwa, niemniej identyfikacja Użytkownika, z uwagi na brak innych danych umożliwiających jednoznaczne wskazanie tożsamości osoby fizycznej, pozostaje niemożliwa (jedyną informacją, jaką dysponuje administrator, jest sygnał inicjujący wysyłkę Kluczy Diagnostycznych przez Serwer ProteGO Safe - istnieje możliwość, że Sewer odnotuje logi komunikacyjne, niemniej ich interpretacja i powiązanie z identyfikowalną osobą fizyczną pozostają niemożliwe)". Informacje przetwarzane w ramach ProteGO Safe nie umożliwiają (nawet pośrednio) identyfikacji osób fizycznych. Dane osobowe przetwarzane są zgodnie z zasadami wskazanymi w art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji.	BRAK	Brak konieczności podejmowania dodatkowych działań.
102.	• TF-01: technologia zbliżeniowa Zgodnie z treścią zaleceń eHealth (TF-01) należy opracować taką technologię zbliżeniową dla aplikacji, która będzie pozwalała na dokładne i powtarzalne ustalenie faktu zaistnienia kontaktu. Za optymalne eHealth przyjmuje przyjęcie minimalnej odległości 1,5m, należy przyjąć dokładność 0.5 metra, a wskazania takie uważa za zapewniające minimalizację wskazań fałszywie pozytywnych.	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Aplikacja ProteGO Safe dla ustalenia kontaktu pomiędzy urządzeniami użytkownika wykorzystuje technologię Bluetooth (BLE). Nie korzysta jednocześnie z technologii geolokalizacyjnych ani z transmisji danych za pomocą sieci komórkowych (wniosek bazowany na doświadczeniach empirycznych uzyskanych podczas korzystania z aplikacji ProteGO Safe). Technologia Bluetooth wykorzystywana przez ProteGO Safe nie wymaga aktywacji żadnych innych technologii lokalizacyjnych, w szczególności wskazanych powyżej. Technologia zbliżeniowa wykorzystywana w ProteGO Safe działa w oparciu o Privacy-Preserving Contact Tracing API wytworzone oraz udostępnione przez odpowiednio: – Google (https://www.google.com/covid19/exposurenotifications/) oraz – Apple (https://www.apple.com/covid19/contacttracing). Dane dotyczące zarejestrowanych spotkań są odnotowywane bezpośrednio w aplikacji użytkownika. Rejestrowany jest tymczasowy, zmienny klucz identyfikujący użytkownika, data kontaktu oraz okres kontaktu (jak długo urządzenia znajdowały się blisko siebie; wartości w zakresie 5-30 minut).		
103.	• **TF-02, TF-05: skuteczność i wiarygodność informacji; epidemiologicznie relewantna i dokładnie ustalana fizyczna odległość oraz skalowalność otoczenia** Zgodnie z treścią zaleceń eHealth (TF-02, TF-04) faktyczna odległość pomiędzy użytkownikami powinna być dokładnie rejestrowana, a zbierane dane powinny być powiązane z "epidemiologicznie istotną" odległością, uzgodnioną przez krajowe organy do spraw zdrowia. Skalowalność aplikacji powinna sięgać 100 mln. użytkowników w ciągu miesiąca, co wymusza korzystanie z rozwiązań generujących minimalne wymagania sprzętowe, które będą powszechnie dostępne. Dzięki zastosowaniu technologii Bluetooth (BLE) oraz Privacy-Preserving Contact Tracing API wytworzone oraz udostępnione przez Google i Apple, GIS jest w stanie kontrolować wartość epidemiologicznie relewantnej odległości i zapewnić, że ProteGO Safe rejestruje wyłącznie kontakty odpowiadające ustalonym warunkom. Skalowalność aplikacji zależy od ilości użytkowników, niemniej jednak technologicznie ProteGO Safe opiera się na prostych elementach niepowodujących dużego obciążenia urządzenia końcowego użytkownika (co zostało zauważone w testach empirycznych przy pracy z ProteGO Safe). Możliwość zachowania wymaganej skalowalności została zatem zachowana zgodnie z zaleceniami eHealth.	BRAK	Brak konieczności podejmowania dodatkowych działań.
104.	• **TF-02, TF-03: szyfrowanie identyfikatorów telefonów/użytkowników** Zgodnie z treścią zaleceń eHealth (TF-02, TF-03) zebrane identyfikatory użytkowników muszą być przechowywane w formie szyfrowanej. Krótkotrwałe ID, generowane losowe i dynamiczne (zmieniające się w czasie, zgodnie z ustalonym harmonogramem), zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne.	BRAK	Brak konieczności podejmowania dodatkowych działań.

105.	• **TF-03: tymczasowe, dynamiczne identyfikatory użytkowników** Zgodnie z treścią zaleceń eHealth (TF-03) identyfikatory użytkowników powinny być generowane pseudolosowo i okresowo zmieniane w celu zwiększenia ochrony przed podsłuchem, hakowaniem i śledzeniem przez osoby trzecie. Zgodnie z informacjami zamieszczonymi w arkuszu Oceny skutków dla ochrony danych (DPIA) „aplikacja bazuje na losowych i dynamicznych (zmieniających się w czasie, zgodnie z ustalonym harmonogramem) kluczach Urządzenia Użytkownika".	BRAK	Brak konieczności podejmowania dodatkowych działań.
106.	• **TF-04: uwierzytelnianie osoby chorej z wykorzystaniem kodów generowanych przez organy ds. zdrowia** Zgodnie z treścią zaleceń eHealth (TF-04) by zapobiec wprowadzaniu do oprogramowania informacji niezgodnych z prawną, w szczególności fałszywych informacji o osobach chorych, użytkownicy zidentyfikowani jako osoby chore powinny móc wprowadzić taką informację do aplikacji wykorzystując w tym celu pseudolosowych, jednorazowych kodów generowanych przez organy ds. zdrowia. Uwierzytelnienie osoby chorej na COVID-19 następuje poprzez wprowadzenie do Aplikacji losowego numeru PIN podanego przez przedstawiciela Centrum Kontaktu, który nie umożliwia identyfikacji (PIN generowany w sposób losowy, jednorazowego użytku)	BRAK	Brak konieczności podejmowania dodatkowych działań.
107.	• **TF-06: współpraca oprogramowania z urządzeniem końcowym użytkownika – powszechność/dostępność i zużycie energii** Zgodnie z treścią zaleceń eHealth (TF-06) śledzenie kontaktu powinno być możliwe przez każde urządzenie wyposażone w Bluetooth, niezależnie od platformy technologicznej. Możliwość śledzenia kontaktu powinna być dostępna na każdym systemie operacyjnym, a aplikacja wyposażona w zabezpieczenia przed nadmiernym zużyciem energii. Aplikacja ProteGO Safe wykorzystuje technologię Bluetooth Low Energy (BLE), która jest powszechnie wykorzystywaną technologią komunikacji bezprzewodowej urządzeń końcowych. Sama aplikacja jest zaś wspierana przez największych dostawców systemów operacyjnych dla telefonów komórkowych: Google i Apple, co wspiera jej uniwersalność i dostępność dla wszystkich użytkowników. Założeniem aplikacji jest dostępność dla jak największego zakresu urządzeń. Aplikacja ProteGO Safe generuje większe zużycie energii urządzenia końcowego dla urządzeń, które nie wspierają technologii Bluetooth Low Energy (BLE).		Ryzyko pozostaje niezależne od GIS i innych podmiotów odpowiedzialnych – zależy wyłącznie od tego, czy urządzenie końcowe użytkownika wspiera technologię Bluetooth Low Energy (BLE). W przypadku urządzeń wspierających wyłącznie klasyczne technologie Bluetooth, działanie aplikacji ProteGO Safe będzie wpływało na zwiększone zużycie energii.
108.	• **TF-08: publicznie dostępny kod źródłowy** Zgodnie z treścią zaleceń eHealth (TF-08) opublikowanie specyfikacji technicznych i kodu źródłowego aplikacji to sposoby na zmaksymalizowanie reużywalności, interoperacyjności, audytowalności i bezpieczeństwa aplikacji. Kod źródłowy aplikacji ProteGO Safe został podany do wiadomości publicznej i jest dostępny do zapoznania się.	BRAK	Brak konieczności podejmowania dodatkowych działań.

109.	• **IOP-01: interoperacyjność w oparciu o eHealth European Interoperability Framework** Zgodnie z treścią zaleceń eHealth (IOP-01) funkcjonowanie aplikacji powinno spełniać wymagania interoperacyjności, sprecyzowane w eHealth European Interoperability Framework z 23 listopada 2015 r. (https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf). Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, ProteGo Safe spełnia warunki interoperacyjności sprecyzowane w powyżej wskazanym dokumencie.	BRAK	Brak konieczności podejmowania dodatkowych działań.
110.	• **IOP-02: dostosowanie kryteriów epidemiologicznych** Zgodnie z treścią zaleceń eHealth (IOP-02) deweloperzy i organy zdrowia publicznego powinni dostosować się do wytycznych WHO i ECDC na temat determinantów śledzenia kontaktów, włącznie z definicją bliskiego kontaktu (odległość i czas ekspozycji) i czasu przez jaki dane o kontaktach powinny być przechowywane. Wskazane powyżej wytyczne WHO i ECDC zostały wzięte pod uwagę podczas tworzenia ProteGO Safe. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, ProteGo Safe spełnia warunki interoperacyjności sprecyzowane w powyżej wskazanych dokumentach.	BRAK	Brak konieczności podejmowania dodatkowych działań.
111.	• **IOP-03: rejestrowanie kontaktu z innymi użytkownikami ProteGO Safe** Zgodnie z treścią zaleceń eHealth (IOP-03) aplikacje muzą być w stanie określić bliskość kontaktu, zgodnie z przyjętymi kryteriami epidemiologicznymi, niezależnie od platformy technologicznej, czy aplikacji jaką każda z danych osób korzysta. Dzięki wykorzystaniu powszechnej technologii Bluetooth oraz Privacy-Preserving Contact Tracing API wytworzone oraz udostępnione przez Google i Apple, ProteGO Safe jest w stanie rejestrować kontakt z innymi użytkownikami, określając przy tym m.in. okres trwania kontaktu (czas, przez jaki dwóch użytkowników znajdowało się w zasięgu rejestrowanym, epidemiologicznie relewantnym).	BRAK	Brak konieczności podejmowania dodatkowych działań.
112.	• **IOP-04: komunikowanie informacji o osobach zakażonych innym krajom/regionom** Zgodnie z treścią zaleceń eHealth (IOP-04) organy zdrowia publicznego powinny uzgodnić protokoły wymiany informacji o łańcuchach transgranicznych kontaktów, zwłaszcza o zarażonych mających kontakt z osobami z innych państw. GIS i inne organy zdrowia publicznego podjęły dialog celem ustalenia zasad interoperacyjności. Na dzień przeprowadzenia niniejszego audytu prywatności, rozmowy nie zostały zakończone a ustaleń nie podjęto.		Należy kontynuować podjęte rozmowy z organami zdrowia publicznego celem wypracowania zasad interoperacyjności.
113.	• **IOP-05: informowanie o kontaktach potencjalnie epidemiologicznych** Zgodnie z treścią zaleceń eHealth (IOP-05) organy zdrowia publicznego powinny uzgodnić protokół informowania osób narażonych na zakażenie. GIS i inne organy zdrowia publicznego podjęły dialog celem ustalenia zasad interoperacyjności. Na dzień przeprowadzenia niniejszego audytu prywatności, rozmowy nie zostały zakończone a ustaleń nie podjęto.		Należy kontynuować podjęte rozmowy z organami zdrowia publicznego celem wypracowania zasad interoperacyjności.
114.	• **CS-01: krajowa ocena ryzyka** Zgodnie z treścią zaleceń eHealth (CS-01) krajowe organy powinny przeprowadzać całościową ocenę ryzyka, skupioną na potencjalnych zagrożeniach dla cyberbezpieczeństwa aplikacji, biorąc pod uwagę znane	BRAK	Brak konieczności podejmowania dodatkowych działań.

	problemy z zakresu bezpieczeństwa poszczególnych platform i protokołów komunikacyjnych, jak również niedawnych incydentów i zagrożeń. Istotne części krajowego systemu oceny ryzyka powinny zostać udostępnione zespołom projektowym pracującym nad aplikacją. Kompleksowa ocena ryzyka z punktu widzenia ochrony danych osobowych i informacji przetwarzanych przez ProteGO Safe została przeprowadzona i udokumentowana w skoroszycie 3 „Ocena i zarządzanie ryzykiem" arkusza Oceny skutków dla ochrony danych (DPIA).		
115.	• **CS-01: udostępnianie informacji i współpraca między podmiotami zaangażowanymi** Zgodnie z treścią zaleceń eHealth (CS-01) podmioty zaangażowane, biorąc przy tym pod uwagę cyberbezpieczeństwo i zarządzanie podatnościami, powinny udostępniać informacje i współpracować pomiędzy zespołami projektowymi i odpowiednimi organami krajowymi, włącznie z krajowymi Zespołami Reagowania na Incydenty Bezpieczeństwa Informatycznego, podmiotami zajmującymi się cyberbezpieczeństwem, Zespołami Reagowania na Incydenty Bezpieczeństwa Informatycznego poszczególnych produktów medycznych. Regularne briefingi dotyczące ryzyka są ważnym narzędziem w celu kreowania świadomości na temat zagrożeń dotyczących cyberbezpieczeństwa na wszystkich poziomach teamów projektowych. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, stosowne procedury w zakresie kooperacji i udostępniania informacji zostały wdrożone i obowiązują.	BRAK	Brak konieczności podejmowania dodatkowych działań.
116.	• **CS-01: procedury reagowania na incydenty** • **CS-02: procedury identyfikacji i zarządzania podatnościami** Zgodnie z treścią zaleceń eHealth (CS-01) ważne jest posiadanie planu zarządzania incydentami i podatnościami, łącznie z adekwatnymi procedurami powiadamiania krajowych Zespołów Reagowania na Incydenty i odpowiednich organów zajmujących się ochroną informacji i danych. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, stosowne procedury reagowania na incydenty, zawierające m.in. procedury powiadamiania oraz zarządzania incydentami i podatnościami, zostały wdrożone i obowiązują.	BRAK	Brak konieczności podejmowania dodatkowych działań.
117.	• **CS-02: testowanie poziomu bezpieczeństwa** Zgodnie z treścią zaleceń eHealth (CS-02) organy krajowe powinny zapewnić odpowiednie testy i badanie bezpieczeństwa aplikacji jak i backendu przez niezależnych ekspertów przed deploymentem jak i po wprowadzeniu każdej zmiany. Ustalony poziom ryzyka znajduje swoje potwierdzenie w testach bezpieczeństwa, m.in. przeprowadzonych przez Securitum (raport z przeprowadzonego testu bezpieczeństwa dostępny tutaj: https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport). Ministerstwo regularnie zleca retesty aplikacji, w tym również przed wprowadzeniem kolejnej wersji oprogramowania lub innych znaczących zmian.	BRAK	Brak konieczności podejmowania dodatkowych działań.

118.	• **CS-02: poddawanie oprogramowania ocenie niezależnych ekspertów** Zgodnie z treścią zaleceń eHealth (CS-02) organy krajowe powinny zadbać o to, by architektura kodu oprogramowania (aplikacji i backendu) umożliwia przeprowadzenie jej oceny przez niezależnych ekspertów. Kod źródłowy aplikacji ProteGO Safe został podany do wiadomości publicznej i jest dostępny do zapoznania się. Każdy może przeanalizować kod. Co więcej, podmioty odpowiedzialne dbają o przeprowadzanie testów bezpieczeństwa i dokumentowanie ustaleń tych testów oraz publikację raportów podsumowujących (np. wśród nich również testy bezpieczeństwa przeprowadzane przez Securitum; raport z przeprowadzonego testu bezpieczeństwa dostępny tutaj: https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport).	BRAK	Brak konieczności podejmowania dodatkowych działań.
119.	• **CS-02: umożliwienie zgłaszania błędów/nieprawidłowości i podatności** Zgodnie z treścią zaleceń eHealth (CS-02) istotnym sposobem zapewnienia bezpieczeństwa oprogramowania jest umożliwienie badaczom cybersecurity, ekspertom, użytkownikom i organizacjom zgłaszania błędów i/lub podatności zespołom projektowym. MC oraz inne podmioty odpowiedzialne wyznaczyły kanały raportowania błędów i zidentyfikowanych podatności. Użytkownik aplikacji, który napotkał błąd, może bez problemu zgłosić go bezpośrednio z poziomu aplikacji, może również ocenić produkt i wskazać istnienie błędów np. w formie komentarzy w Sklepie Google (zapoznając się z treścią sekcji „Oceny i opinie" w Sklepie Google zauważyć można, że Ministerstwo odpowiada na większość feedbacków dociekając szczegółów błędu).	BRAK	Brak konieczności podejmowania dodatkowych działań.
120.	• **CS-03: minimalizacja danych; ograniczenie przechowywania danych; szyfrowanie, pseudonimizacja i anonimizacja** Zgodnie z treścią zaleceń eHealth (CS-03) deweloperzy powinni ograniczyć przetwarzane dane, a same dane pseudonimizować/anonimizować kiedy tylko jest to możliwe, chronić jakiekolwiek pozostałe wrażliwe dane przetwarzane przez aplikację lub backend i usuwać je kiedy tylko są już zbędne. W podstawowej wersji aplikacji ProteGO Safe przetwarzany jest minimalny zakres danych - ograniczony do identyfikatora użytkownika oraz klucza diagnostycznego (losowe i okresowo zmieniane anonimowe identyfikatory urządzeń), a także danych statystycznych (w tym danych zanonimizowanych). Krótkotrwałe ID, generowane losowe i dynamiczne (zmieniające się w czasie, zgodnie z ustalonym harmonogramem), zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne. W ramach korzystania z funkcji dodatkowych, aplikacja pozwala na wprowadzenie przez użytkownika wyłącznie danych niezbędnych do wykonania oceny ryzyka zarażenia (w przypadku korzystania z Modułu Triażu) czy też kontroli stanu zdrowia użytkownika celem wczesnego wykrywania niepokojących objawów (w przypadku korzystania z Modułu Dziennika Zdrowia).	BRAK	Brak konieczności podejmowania dodatkowych działań.

	W ramach Modułu Analitycznego aplikacja przechowuje informacje o okresie kontaktu urządzeń użytkowników (jak długo urządzenia znajdowały się blisko siebie; wartości w zakresie 5-30 minut) oraz o dacie kontaktu. Dane osobowe użytkownika oraz inne informacje wprowadzane do aplikacji przez użytkownika są przechowywane lokalnie, na urządzeniu końcowym użytkownika. Dane osobowe przetwarzane w Aplikacji ProteGO Safe przetwarzane są w formie uniemożliwiającej identyfikację osoby, której dane dotyczą zarówno przez Ministra Cyfryzacji jak i GIS. Dane przekazywane podczas komunikacji z serwerem ProteGO Safe, znane Ministrowi Cyfryzacji jak i GIS podmiotom przetwarzane w Aplikacji ProteGO Safe to dane związane z wykorzystywaniem serwera zapewniającego przekazywanie Użytkownikom komunikatów. Serwer ProteGO Safe (Backend) nie umożliwia identyfikacji użytkownika ani połączenia (porównania) kluczy diagnostycznych (narażenia) z jakimikolwiek innymi danymi użytkownika. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Kluczowym jest używanie TLS w kodowaniu danych w transporcie gdy dochodzi do komunikacji poprzez WiFi lub dane komórkowe (przesyłania klucza diagnostycznego po wprowadzeniu przez osobę chorą kodu PIN w aplikacji, aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej). Zakres danych, a w szczególności zakres danych udostępnianych innym podmiotom niż osoba, której dotyczą ograniczony jest do niezbędnego minimum - ogranicza się wyłącznie do danych niezbędnych zakodowanych w Kluczu Diagnostycznym, umożliwiających wskazanie ryzyka transmisji wirusa SARS CoV-2 od Użytkownika, u którego wykryto obecność wirusa lub chorobę COVID-19. Klucze diagnostyczne (narażenia) są przechowywane na serwerze ProteGO Safe przez okres retencji wynoszący 14 dni, a następnie automatycznie kasowane. Możliwość przechowywania danych przez użytkownika na urządzeniu końcowym, gdzie zainstalowana jest aplikacja ProteGO Safe, ograniczona została poprzez wprowadzenie systemowego ograniczenia historii działania Modułu Analitycznego do 14 dni wstecz.		
121.	• CS-03: minimalizacja uprawnień Zgodnie z treścią zaleceń eHealth (CS-03) deweloperzy powinni ograniczyć do minimum uprawnienia aplikacji. Podczas pracy z aplikacją wielokrotnie weryfikowano, o przyznanie jakich uprawnień aplikacja prosi użytkownika. Pomijając prośbę o wyrażenie zgody na korzystanie z modułów Bluetooth, aplikacja nie wskazuje na konieczność przyznania innych, dodatkowych uprawnień. Zauważyć należy również, że o uprawnienia te aplikacja prosi w toku działania użytkownika (system nie przyznaje aplikacji uprawnień automatycznie, co dotyczy również korzystania z modułu Bluetooth – użytkownik musi podjąć działanie, by aplikacja mogła korzystać z technologii Bluetooth), tak wiec zastosowano prawidłowy model opt-in, zgodny z zasadą *privacy by default*.	BRAK	Brak konieczności podejmowania dodatkowych działań.

122.	• CS-04: bezpieczny software development • CS-05: korzystanie ze znanych i rekomendowanych algorytmów kryptograficznych; bezpieczeństwo identyfikatorów Zgodnie z treścią zaleceń eHealth (CS-04) deweloperzy powinni kierować dobrymi praktykami, zasadami bezpiecznego programowania, zasadami bezpiecznego projektowania i tworzenia aplikacji i serwisów backendowych, powinni używać najnowszych i aktualnych środowisk programistycznych, powinni testować swoje aplikacje tak często jak to tylko możliwe, korzystając ze zautomatyzowanych narzędzi do testowania i integracji, obejmujących nie tylko testy funkcjonalne, ale także testy bezpieczeństwa takie jak fuzz testing, skanowanie podatności, sprawdzanie jakości kodu, (statyczne i dynamiczne) narzędzia do analizy kodu, skanowanie kodu źródłowego w poszukiwaniu bibliotek i gotowego kodu. Platforma backendowa i wszystkie powiązane serwisy powinny być wzmocnione i/lub zpatchowane w celu zniwelowania ryzyka naruszenia danych, a interfejs między aplikacją a backendem powinien być zabezpieczony. Developerzy powinni wziąć pod uwagę zagrożenia dla ich środowisk programistycznych. Ważne jest wzięcie pod uwagę, że hakerzy często biorą na cel ataków programistów, administratorów i platformy programistyczne, gdyż mogą się tam znajdować hasła systemowe, wrażliwe dane uwierzytelniające, dostęp do kodu źródłowego, prawa dostępu do wrażliwych zasobów, hasła do backendu, itd. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, rozwiązania zapewniające realizację powyższych zaleceń zostały wdrożone i obowiązują. Deweloperzy przy tworzeniu aplikacji korzystali z dobrze znanych i rekomendowanych algorytmów i protokołów kryptograficznych. Szczególną uwagę poświęcono wymaganiom dla zapewnienia odpowiedniego wykorzystania każdego algorytmu i protokołu (np. random initialization vectors or nonces). Zaimplementowano także mechanizmy bezpieczeństwa przed przekazaniem/odtworzeniem identyfikatora (Identifier relay/replay prevention).	BRAK	Brak konieczności podejmowania dodatkowych działań.
123.	• CS-05: wbudowane protokoły bezpieczeństwa Zgodnie z treścią zaleceń eHealth (CS-05) deweloperzy powinni w jak najlepszy sposób wykorzystać wbudowane w systemy operacyjne smartfonów funkcje bezpieczeństwa, takie jak autentykacja użytkowników, sandboxy aplikacji, szyfrowania przestrzeń dyskowa dla każdej aplikacji. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, rozwiązania zapewniające realizację powyższych zaleceń zostały wdrożone i obowiązują.	BRAK	Brak konieczności podejmowania dodatkowych działań.
124.	• CS-06: bezpieczeństwo komunikacji; rozwiązania kryptograficzne i szyfrowanie Zgodnie z treścią zaleceń eHealth (CS-06) cała komunikacja sieciowa pomiędzy aplikacją a backendem powinna być szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Kluczowym jest używanie TLS w kodowaniu danych w transporcie gdy dochodzi do komunikacji poprzez WiFi lub dane komórkowe (aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej). Przy ProteGO Safe co do zasady zrezygnowano z komunikacji przez sieć bezprzewodową WiFi oraz sieci komórkowe. Niemniej do transmisji takiej dochodzić będzie w przypadku komunikowania aplikacji	BRAK	Brak konieczności podejmowania dodatkowych działań.

	użytkownika będącego osobą chorą, który zainicjował dystrybucję klucza diagnostycznego, z serwerem ProteGO Safe. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych.		
125.	• CS-07: secure-by-default i user-friendly Zgodnie z treścią zaleceń eHealth (CS-07) aplikacje muszą być możliwe do używania przez znaczną część populacji, nie tylko osoby techniczne. Aplikacje powinny być bezpieczne out-of-the-box z ustawieniami zapewniającymi security-by-default. W procesie projektowania należy kierować się jak największą intuicyjnością aplikacji w celu uniknięcia naruszenia jej bezpieczeństwa przez błąd użytkownika związany np. z błędną konfiguracją. Aplikacja ProteGO Safe zaprojektowana została w taki sposób, by każdy mógł jej używać (co osiągnięto poprzez ustalenie minimalnych wymagań sprzętowych, wykorzystanie powszechnie wspieranych technologii i algorytmów, rozwiązania pozwalające na ochronę zużycia baterii tj. korzystanie z technologii Bluetooth Low Energy (BLE) w urządzeniach wspierających tę technologię, zapewnienie dostępności aplikacji u największych dostawców systemów operacyjnych urządzeń mobilnych: w Sklepie Google i AppStore od Apple). Aplikacja nie wymaga skomplikowanej konfiguracji, przez co zredukowano ryzyko wystąpienia błędów konfiguracyjnych. Z uwagi na lokalny charakter działania ProteGO Safe, podmioty odpowiedzialne mają mniejszą możliwość lub brak możliwości ingerowania w system i stan bezpieczeństwa urządzenia użytkownika. Aplikacja nie jest przystosowana do przeprowadzania testów „onboarding security", w tym zakresie użytkownik musi samodzielnie zadbać o stan swojego urządzenia.		ProteGO Safe nie jest aplikacją antywirusową. Użytkownik musi mieć na względzie bezpieczeństwo swojego urządzenia nie tylko podczas lub w związku z korzystaniem z aplikacji ProteGO Safe, ale na co dzień. Ryzyko jest niezależne od podmiotów odpowiedzialnych za operacyjność ProteGO Safe, niemniej jednak dostrzegalne, a w konsekwencji konieczne do wskazania w ramach ryzyk. Przy analizie ryzyka wzięto pod uwagę możliwe konsekwencje związane z korzystaniem z aplikacji ProteGO Safe z wykorzystaniem urządzeń końcowych zainfekowanych złośliwym oprogramowaniem lub rootowanych.
126.	• CS-08: uwierzytelnianie Zgodnie z treścią zaleceń eHealth (CS-08) deweloperzy powinni skorzystać z możliwości uwierzytelniania możliwych do wykorzystania na smartfonach, zwłaszcza w przypadku informacji wrażliwych. ProteGO Safe jako aplikacja działająca lokalnie nie posiada dodatkowych zabezpieczeń uwierzytelniających użytkownika. Niemniej inicjacja transmisji danych (dystrybucji klucza diagnostycznego) jest zabezpieczona dodatkowym uwierzytelnieniem. Dotychczas nie zdecydowano się na wprowadzenie dodatkowych uwierzytelnień dla użytkowników ProteGO Safe ze względu na to, że może mieć negatywny wpływ na używalność aplikacji (z uwagi na notoryczne odpytywanie o kod PIN; niektóre osoby z grupy docelowej mogą mieć problemy z wprowadzaniem ciągu znaków, co może z kolei wpłynąć negatywnie na realizację wymogów wynikających z zaleceń eHealth o kodzie TF-06, zob. rubryka 107).		Dla dalszego podniesienia bezpieczeństwa danych przechowywanych w aplikacji ProteGO Safe można rozważyć rozwiązanie polegające na zabezpieczeniu aplikacji hasłem lub kodem PIN (w momencie uruchamiania aplikacji, by wejść do niej, użytkownik musiałby wpisywać samodzielnie ustalony, dodatkowy kod zabezpieczający aplikację przed dostępem osób przypadkowych, np. korzystających z telefonu użytkownika aplikacji). Z informacji uzyskanych od podmiotów odpowiedzialnych wynika, że rozważane jest wprowadzenie fakultatywnego uwierzytelniania.

			Celem wprowadzenia zmian, podmioty odpowiedzialne ponownie przeanalizują możliwy wpływ zmiany na używalność aplikacji.
127.	• CS-09: bezpieczne wykorzystanie bibliotek i zewnętrznego kodu Zgodnie z treścią zaleceń eHealth (CS-09) aplikacja w miarę możliwości powinna polegać w miarę możliwości na niskopoziomowych bibliotekach udostępnianych przez system operacyjny i unikać (w miarę możliwości) korzystania z zewnętrznych bibliotek. W przypadku wykorzystywania zewnętrznych bibliotek należy zachować szczególną ostrożność i upewnić się, że są one aktualne i istnieje możliwość sprawdzenia ich kodu źródłowego. Deweloperzy muszą zainwestować w sprawdzenie bibliotek, zewnętrznego kodu i ich bezpieczną integrację z projektem. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, rozwiązania zapewniające realizację powyższych zaleceń zostały wdrożone i obowiązują.	BRAK	Brak konieczności podejmowania dodatkowych działań.
128.	• CS-10: obsługa niezabezpieczonych smartfonów Zgodnie z treścią zaleceń eHealth (CS-10) deweloperzy powinni zdawać sobie sprawę z tego, że nie wszystkie smartfony korzystają z najnowszych wersji systemów operacyjnych. Takie urządzenia mogą korzystać z oprogramowania podatnego na ataki. Wiele smartfonów korzysta z przestarzałego oprogramowania, część ich jest zrootowana, po jailbreaku, lub w inny sposób zmodyfikowana. Podmioty odpowiedzialne i zespoły projektowe zdają sobie sprawę z zagrożenia, jakie niesie ze sobą korzystanie ze starszych wersji systemów operacyjnych i starszych technologii na urządzeniach, na których instalowana jest aplikacja ProteGO Safe. Ryzyka związane z korzystaniem z niezabezpieczonych urządzeń mobilnych zostały wzięte pod uwagę podczas przeprowadzania analizy ryzyka i zrównoważone z wykorzystaniem adekwatnych środków zabezpieczających.	BRAK	Brak konieczności podejmowania dodatkowych działań.
129.	• SG-01: automatyczna dezaktywacja/usuwanie aplikacji po pandemii/ustaniu zagrożenia epidemiologicznego Zgodnie z treścią zaleceń eHealth (SG-01) aplikacja powinna zostać automatycznie wyłączona a wszystkie dane usunięte wraz z końcem kryzysu. Zgodnie z założeniami projektowymi, o których użytkownicy są informowani w dokumentacji towarzyszącej aplikacji (Regulaminie ProteGO Safe (v.4.2.), Polityce prywatności ProteGO Safe (v.4.2.) oraz w opublikowanym przez Ministerstwo arkuszu Oceny skutków dla ochrony danych (DPIA)), aplikacja zostanie wyposażona w możliwość zdalnej dezaktywacji w momencie zakończenia pandemii COVID-19 lub stanu zagrożenia pandemicznego w następnej wersji oprogramowania. Na moment przeprowadzania audytu prywatności oraz opracowywania niniejszego raportu, zalecenie to nie jest spełnione. Zgodnie z uzyskanymi od podmiotów odpowiedzialnych informacjami, z uwagi na obawy o nieproporcjonalną ingerencję w prywatność (pełna realizacja, zakładająca usunięcie aplikacji wraz z danymi w niej przechowywanymi z urządzenia użytkownika wymagałaby technicznych rozwiązań umożliwiających zdalny		Konieczność umożliwienia zdalnego zdezaktywowania aplikacji z momentem zakończenia pandemii COVID-19 lub stanu zagrożenia epidemiologicznego. Odpowiednie rozwiązanie zostanie wdrożone w kolejnych wersjach aplikacji.

	dostęp podmiotów odpowiedzialnych do urządzenia końcowego użytkownika, co z uwagi na poszanowanie prywatności użytkowników jest niemożliwe do realizacji) oraz możliwe konsekwencje w postaci spadku zaufania do podmiotów publicznych oraz tego typu aplikacji i programów, rozwiązania, które choćby w stopniu potencjalnym wymagały ingerencji w urządzenia końcowe użytkownika nie są rozważane. Podmioty odpowiedzialne rozważają alternatywne możliwości dezaktywacji aplikacji, które nie będą wymagać dostępu do urządzenia końcowego użytkownika, w tym wprowadzenie rozwiązań umożliwiających zachowanie danych lub ich eksport po okresie pandemii, ewentualne pozostawienie możliwości korzystania z aplikacji ProteGO Safe po zakończeniu pandemii z jednoczesnym ograniczeniem funkcjonalności aplikacji, np. do funkcji informowania o prawach i obowiązkach, aktualnej sytuacji epidemiologicznej. Podmioty odpowiedzialne podjęły konsultacje z interesariuszami projektu ProteGO Safe, zgodnie z uzyskanymi informacjami planowane jest również przeprowadzenie konsultacji ze społecznością GitHub oraz Komisją Europejską.		
130.	• SG-02: nieobowiązkowy charakter Zgodnie z treścią zaleceń eHealth (SG-02) aplikacja powinna być oparta na zgodzie oraz powinno podać się wszelkie dane związane z przetwarzaniem danych. Przetwarzanie danych osobowych w aplikacji ProteGO Safe oparte jest na innych podstawach prawnych niż zgoda (na konieczności realizacji zadań wynikających z przepisów prawa powszechnie obowiązującego oraz na zabezpieczeniu ważnych interesów publicznych w zakresie zdrowia publicznego). Przechowywanie danych na urządzeniu końcowym bazuje na świadomej i dobrowolnej zgodzie użytkownika aplikacji. W oparciu o świadomą i dobrowolną zgodę użytkownika wykorzystywane są również technologie zbliżeniowe. Samo korzystanie z aplikacji jest nieobowiązkowe. Pobranie i inicjacja działania aplikacji jak również korzystanie z modułów dodatkowych jest dobrowolne.	BRAK	Brak konieczności podejmowania dodatkowych działań.
131.	• SG-03: brak śledzenia Zgodnie z treścią zaleceń eHealth (SG-03) dane o lokalizacji nie powinny być wymagane w celu śledzenia kontaktu. Celem aplikacji nie może być śledzenie ruchów jednostki czy wymuszanie zaleceń. Aplikacja ProteGO Safe dla ustalenia kontaktu pomiędzy urządzeniami użytkownika wykorzystuje technologię Bluetooth (BLE). Nie korzysta jednocześnie z technologii geolokalizacyjnych ani z transmisji danych za pomocą sieci komórkowych (wniosek bazowany na doświadczeniach empirycznych uzyskanych podczas korzystania z aplikacji ProteGO Safe). Technologia Bluetooth wykorzystywana przez ProteGO Safe nie wymaga aktywacji żadnych innych technologii lokalizacyjnych, w szczególności wskazanych powyżej. Zauważyć należy, że w systemach operacyjnych Android dla umożliwienia aplikacji korzystania z technologii Bluetooth konieczne będzie wyrażenie zgody systemowej na „lokalizację", ponieważ moduły Bluetooth traktowane są przez system jako tracing. Niemniej nie oznacza to, że aplikacja korzysta z technologii geolokalizacyjnych w systemach operacyjnych Android.	BRAK	Brak konieczności podejmowania dodatkowych działań.
132.	• SG-04: brak stygmatyzacji	BRAK	

	Zgodnie z treścią zaleceń eHealth (SG-04) aplikacja powinna gwarantować to, że żaden użytkownik nie pozna tożsamości żadnej z zainfekowanych osób lub osób mających bliski kontakt z zarażonymi. Zakres danych, a w szczególności zakres danych udostępnianych innym podmiotom niż osoba, której dotyczą ograniczony jest do niezbędnego minimum - ogranicza się wyłącznie do danych niezbędnych zakodowanych w kluczu diagnostycznym, umożliwiających wskazanie ryzyka transmisji wirusa SARS CoV-2 od użytkownika, u którego wykryto obecność wirusa lub chorobę COVID-19. Udostępnianiu może podlegać klucz diagnostyczny, zawierający informację o chorym użytkowniku (osobie chorej) oraz kluczach jego urządzenia. ProteGO Safe, w przypadku zidentyfikowania osoby zakażonej, umożliwia anonimowe przesłanie informacji za pośrednictwem serwera ProteGO Safe do urządzeń końcowych (aplikacji) innych użytkowników, które to następnie dokonują interpretacji, czy kontakt epidemiologiczny zaistniał czy nie oraz dokonują niezbędnej korekty ustalonego ryzyka zakażenia użytkownika odbierającego klucz diagnostyczny. Aplikacja nie informuje użytkownika będącego osobą chorą o tożsamości czy kluczach urządzeń użytkowników, które potwierdziły kontakt epidemiologiczny i w konsekwencji jego zaistnienia zwiększyły ryzyko dla użytkowników. Aplikacja nie przekazuje również użytkownikom odbierającym klucz diagnostyczny informacji o dacie czy czasie kontaktu z osobą zidentyfikowaną jako zakażona.		Brak konieczności podejmowania dodatkowych działań.
133.	• **SG-05: dane o kontaktach przechowywane lokalnie, na urządzeniu końcowym użytkownika** Zgodnie z treścią zaleceń eHealth (SG-05) w celu poprawy prywatności i bezpieczeństwa, dane o zbliżeniach (bliskich kontaktach), powinny być przechowywane jedynie na urządzeniu i usunięte po zakończeniu się istotnego z punktu widzenia epidemiologicznego okresu (rekomendowany czas to 14-16 dni). Jedynie po potwierdzeniu infekcji dane o kontaktach mogą być wgrane na serwery centralne i przekazane odpowiednim organom zdrowia publicznego, w zależności od systemu obranego przez dane państwo członkowskie. Dane użytkownika są przechowywane wyłącznie lokalnie, na urządzeniu końcowym użytkownika, na którym zainstalowana jest aplikacja ProteGO Safe. Aplikacja generuje pseudolosowe tymczasowe i dynamiczne identyfikatory. Urządzenie komunikując się bezpośrednio z innym urządzeniem na którym zainstalowana jest aplikacja ProteGO Safe przesyła bezpośrednio do tego urządzenia informację umożliwiającą ustalenie, że nastąpił kontakt (za pomocą technologii Bluetooth; w procesie nie uczestniczy zewnętrzny serwer lub inne urządzenie, nie wykorzystuje się technologii opartych na transmisjach danych sieciami bezprzewodowymi WiFi lub komórkowymi). Urządzenie komunikuje się z backendem (serwerem ProteGO Safe) wyłącznie w sytuacji, gdy do aplikacji użytkownika zidentyfikowanego jako osoba chora zostanie wprowadzony specjalny kod PIN – przesłaniu podlega wyłącznie klucz diagnostyczny.	BRAK	Brak konieczności podejmowania dodatkowych działań.
134.	• **SG-06: tymczasowe i pseudolosowo generowane identyfikatory**	BRAK	Brak konieczności podejmowania dodatkowych działań.

	Zgodnie z treścią zaleceń eHealth (SG-06) krótkotrwałe identyfikatory transmitowane między urządzeniami poprzez Bluetooth powinny być generowane pseudolosowo i okresowo zmieniane. Nie powinny umożliwiać zidentyfikowania konkretnego użytkownika przez innego, ani identyfikacji danego urządzenia. Zgodnie z informacjami zamieszczonymi w arkuszu Oceny skutków dla ochrony danych (DPIA) „aplikacja bazuje na losowych i dynamicznych (zmieniających się w czasie, zgodnie z ustalonym harmonogramem) kluczach Urządzenia Użytkownika".		
135.	• SG-07: pseudonimizacja Zgodnie z treścią zaleceń eHealth (SG-07) pseudonimy nie powinny być związane z długotrwałymi informacjami umożliwiającymi identyfikację. Użytkownicy Aplikacji nie są oznaczani danymi identyfikującymi osobę typu imię i nazwisko, lecz losowo generowanym identyfikatorem Użytkownika. Dla GIS czy MC, który zarządza Serwerem ProteGO Safe, dane te są anonimowe w rozumieniu art. 11 RODO. Aplikacja przypomina, by nie wprowadzać do niej nazwiska użytkownika (w każdym miejscu, w którym możliwe jest ustalenie lub zmiana lokalnie przechowywanego identyfikatora użytkownika).	BRAK	Brak konieczności podejmowania dodatkowych działań.
136.	• SG-08: kryptografia i szyfrowanie Zgodnie z treścią zaleceń eHealth (SG-08) aplikacja powinna w takim stopniu jaki jest tylko możliwy szyfrować dane w celu poprawy prywatności i bezpieczeństwa. Krótkotrwałe ID, generowane losowe i dynamiczne (zmieniające się w czasie, zgodnie z ustalonym harmonogramem), zawiera (szyfrowane) dane konieczne do identyfikacji urządzenia (niebędące jednocześnie ID samego urządzenia) i wysyłania powiadomień push kiedy jest to konieczne. Zgodnie z dokumentacją towarzyszącą ProteGO Safe, cała komunikacja sieciowa pomiędzy aplikacją a backendem (serwerem ProteGO Safe) jest szyfrowana przy użyciu dobrze znanych i rekomendowanych bibliotek kryptograficznych. Kluczowym jest używanie TLS w kodowaniu danych w transporcie gdy dochodzi do komunikacji poprzez WiFi lub dane komórkowe (przesyłania klucza diagnostycznego po wprowadzeniu przez osobę chorą kodu PIN w aplikacji, aplikacja dopuszcza używanie TLS w wersji 1.2 lub wyższej). Deweloperzy przy tworzeniu aplikacji korzystali z dobrze znanych i rekomendowanych algorytmów i protokołów kryptograficznych.	BRAK	Brak konieczności podejmowania dodatkowych działań.
	Technologia w walce z koronawirusem – 7 Filarów Zaufania Panoptykonu.		
	Zagadnienie	Ryzyko	Proponowane działania
137.	• minimalizacja danych: skorelowanie zakresu przetwarzanych danych z celami przetwarzania Zgodnie z treścią zasady minimalizacji danych wyrażonej przez Panoptykon „w celu przeciwdziałania pandemii można przetwarzać tylko te dane, które są niezbędne do realizacji celu założonego w ramach konkretnego narzędzia".	BRAK	Brak konieczności podejmowania dodatkowych działań.

	ProteGO Safe działa w związku z realizacją przez GIS obowiązków wynikających z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej. Zadaniem aplikacji ProteGo Safe jest dostarczenie narzędzia asystującego i chroniącego użytkownika i jego bliskich przed rozprzestrzenianiem się COVID-19. W tym celu aplikacja przechowuje informacje o okresie kontaktu urządzeń użytkowników oraz o dacie kontaktu. Informacje o miejscu i czasie kontaktu nie są przechowywane.		Zasada minimalizacji danych przy przetwarzaniu danych w aplikacji ProteGO Safe jest realizowana w pełni.
138.	• **ograniczenie możliwości dostępu do danych osobowych** Zdaniem Panoptykonu „dostęp do danych powinny mieć tylko osoby i instytucje, które ten cel realizują" . Dostęp do danych przetwarzanych w ProteGO Safe mają wyłącznie GIS (administrator danych) oraz podmioty, które współpracują z GIS w celu rozwoju i utrzymania ProteGO Safe, w tym Minister Cyfryzacji (podmiot odpowiedzialny za utrzymanie aplikacji ProteGO Safe), a także podmioty odpowiedzialne za wykonywanie zleconych przez MC prac rozwojowych i deweloperskich nad ProteGO Safe: TYTANI24 sp. z o.o. oraz we wskazanym w Polityce prywatności zakresie Operator Chmury Krajowej Sp. z o.o. (podmiot dostarczający infrastrukturę umożliwiającą pobieranie i aktualizowanie ProteGO Safe oraz utrzymujący Serwer ProteGO Safe), a także Cloudflare Inc. 101 Townsend St, San Francisco, CA 94107, USA (w zakresie dostarczania usługi zapobiegania atakom DDOS oraz zapewnienia najwyższych standardów bezpieczeństwa użytkowników).	BRAK	Brak konieczności podejmowania dodatkowych działań. Dostęp do danych osobowych przetwarzanych w ramach ProteGO Safe został ograniczony, ustalono rygorystyczne warunki dostępu do danych. Możliwość dostępu do danych skorelowano z koniecznością przetwarzania danych dla realizacji celów przetwarzania.
139.	• **poprawność danych** Zgodnie z założeniami Panoptykonu „wykorzystywane powinny być tylko możliwie najbardziej prawidłowe dane o ludziach." W aplikacji ProteGo Safe tylko osoby zweryfikowane medycznie jako chore na COVID-19 mogą zainicjować proces wysłania swoich kluczy diagnostycznych (warunkiem niezbędnym, jest wcześniejsze uzyskanie kodu PIN z Centrum Kontaktu), aby można było wysłać ostrzeżenie dla innych użytkowników. Co więcej, poprzez zapewnienie lokalnego charakteru przechowywania danych osobowych, użytkownik ma kompleksową kontrolę nad dotyczącymi go danymi osobowymi i nad ich poprawnością, a w razie potrzeby może bez problemów i w czasie rzeczywistym dokonać ich korekty.	BRAK	Brak konieczności podejmowania dodatkowych działań.
140.	• **ograniczenie czasu przechowywania** Zgodnie z założeniami Panoptykonu „dane osobowe nie powinny być przechowywane dłużej, niż jest to konieczne do zrealizowania konkretnego celu, jakiemu mają służyć. [..] W ustalaniu maksymalnych terminów powinni brać udział lekarze, epidemiolodzy i eksperci techniczni." Zgodnie z tym założeniem z Aplikacji ProteGO Safe po 14 dniach usuwane są następujące dane gromadzone lokalnie na urządzeniu: historia wyników analiz Modułu Analitycznego, okres kontaktu urządzeń użytkowników, wartości w zakresie 5-30 minut oraz data kontaktu urządzeń użytkowników. Użytkownik może tez samodzielnie usunąć te dane. Usunięcie aplikacji przez użytkownika z telefonu skutkuje usunięciem	BRAK	Brak konieczności podejmowania dodatkowych działań.

	danych przechowywanych w aplikacji. Klucze diagnostyczne są przechowywane na serwerze ProteGO Safe w postaci zaszyfrowanej przez okres retencji wynoszący 14 dni. 14 dniowy okres retencji wynika ze wskazanego przez WHO okresu inkubacji wirusa SARS CoV-2, który trwa ok. 1-14 dni.		
141.	• **lokalne przechowywanie danych na urządzeniu końcowym użytkownika** Zgodnie z założeniami Panoptykonu „zasadą powinno być gromadzenie i przetwarzanie danych osobowych na urządzeniu osoby, której te dane dotyczą […], a przekazanie danych na zewnętrzny serwer powinno następować tylko w ściśle określonych i uzasadnionych przypadkach (np. stwierdzonego incydentu zarażenia), a obywatel powinien być o tej konieczności uprzednio poinformowany" W aplikacji ProteGO Safe dane przechowywane są na urządzeniach użytkowników. Wszystkie informacje zawarte we wpisach w Module Dziennik Zdrowia oraz Module Triażu, a także historia spotykanych urządzeń przetwarzana w Module Analitycznym są przechowywane na urządzeniach użytkowników i tam analizowane. Na serwer mogą zostać przesłane jedynie dane zgromadzone przez osoby zweryfikowane przez Centrum Kontaktu. Tylko osoby zweryfikowane medycznie jako chore na COVID-19 mogą zainicjować proces wysłania kluczy diagnostycznych, aby można było wysłać ostrzeżenie dla innych użytkowników.	BRAK	Brak konieczności podejmowania dodatkowych działań.
142.	• **szyfrowanie i anonimizacja** Zgodnie z założeniami Panoptykonu „dane osobowe powinny być szyfrowane, anonimizowane (tam, gdzie to niemożliwe - pseudonimizowane)". Dane wprowadzane do ProteGO Safe umożliwiają zachowanie anonimowości użytkowników. Nie jest konieczna rejestracja, ani podawanie jakichkolwiek danych identyfikujących. Po instalacji aplikacji użytkownik może podać swoją nazwę, która może być dowolna. Aplikacja informuje użytkownika, że nazwą nie powinno być jego nazwisko. Wszelkie identyfikatory są generowane w sposób uniemożliwiający ich powiązanie z konkretnym urządzeniem lub użytkownikiem. Co więcej, zgodnie z arkuszem Oceny skutków dla ochrony danych (DPIA) „serwer nadający anonimowe identyfikatory oraz serwer przesyłający klucze diagnostyczne nie są ze sobą połączone. Identyfikacja osób chorych na COVID-19 jest niemożliwa z perspektywy aplikacji ProteGO Safe i serwerów ProteGO Safe".	BRAK	Brak konieczności podejmowania dodatkowych działań.
143.	• **bezpieczeństwo przetwarzania** Zdaniem Panoptykonu „[A]plikacje powinny zachowywać najwyższe standardy bezpieczeństwa i być poddawane odpowiednim audytom". Aplikacja została poddana audytom security, które nie wykazały zagrożeń o stopniu krytycznym i wysokim. Zgodnie z arkuszem Oceny skutków dla ochrony danych (DPIA) „ProteGO Safe zaprojektowano w taki sposób, aby minimalizować zagrożenia dla prywatności i bezpieczeństwa osób i społeczności oraz zagwarantować najwyższy poziom ochrony danych." Dane przechowywane są na urządzeniach użytkowników; zaimplementowano rozwiązania umożliwiające zachowanie anonimowości użytkowników;	BRAK	Brak konieczności podejmowania dodatkowych działań.

	tylko osoby zweryfikowane medycznie jako chore na COVID-19 mogą zainicjować proces wysłania swoich kluczy diagnostycznych.		
144.	• **przejrzyste informowanie – czytelna informacja dla obywateli** Panoptykon wskazuje, że „podstawą społecznego zaufania do narzędzi technologicznych służących walce z pandemią jest czytelna i zrozumiała informacja dla osób, których dane będą wykorzystywane." Informacje o podmiotach odpowiedzialnych za dostarczanie oprogramowania ProteGO Safe są łatwo dostępne – przy instalowaniu aplikacji, zarówno w AppStore jak i w Sklepie Google, wyświetla się informacja, że oferentem oprogramowania ProteGO Safe jest Ministerstwo Cyfryzacji. Cele przetwarzania danych i zakres zbieranych danych wskazane są w Polityce prywatności, z która należy zapoznać się przed rozpoczęciem użytkowania aplikacji (dostępna zarówno w aplikacji jak i na stronach Ministerstwa). Klauzula informacyjna została zawarta jedynie w treści Polityki prywatności. Należy ocenić, że klauzula ta powinna znaleźć się w formularzu.		Zgodnie z najlepszą praktyką, wskazane jest zamieszczenie w ekranie umożliwiającym potwierdzenie zapoznania się i akceptację Regulaminu oraz Polityki prywatności ProteGO Safe skróconej wersji klauzuli informacyjnej, zawierającej minimum informacji niezbędnych do uznania działań podejmowanych przez użytkownika aplikacji ProteGO Safe za świadome. Z informacji uzyskanych od podmiotów odpowiedzialnych za ProteGO Safe wynika, że zmiana w tym zakresie jest obecnie projektowana. W następnych wersjach aplikacji ProteGO Safe zostanie wprowadzony dodatkowy ekran zawierający treść odpowiadającą wymaganemu zakresowi informacji dla pierwszej warstwy klauzuli informacyjnej. Alternatywnie rozważane jest również dodanie takiej treści na ekranie, który umożliwia akceptację Regulaminu i Polityki prywatności podczas inicjowania pracy z aplikacją. Projektowana zmiana doprowadzi do pełnej eliminacji oznaczonego poziomu ryzyka
145.	• **otwartość kodu źródłowego i algorytmów** Według Panoptykonu „standardem dla narzędzi służących do walki z pandemią powinna być pełna otwartość kodu oraz algorytmów stosowanych do analizy danych (np. parametry brane pod uwagę przy określaniu ryzyka zakażenia w kontakcie społecznym muszą być jawne)" Kod źródłowy aplikacji ProteGO Safe został podany do wiadomości publicznej.	BRAK	Brak konieczności podejmowania dodatkowych działań.
146.	• **weryfikacja pod kątem cyberbezpieczeństwa i ochrony danych osobowych** Zgodnie z założeniami Panoptykonu „każde narzędzie, z którego państwo zamierza skorzystać w walce z pandemią, powinno zostać wcześniej zweryfikowane pod kątem cyberbezpieczeństwa i standardów ochrony danych osobowych."		ProteGO Safe nie jest aplikacją antywirusową. Użytkownik musi mieć na względzie bezpieczeństwo swojego urządzenia nie tylko

	Kompleksowa ocena ryzyka z punktu widzenia ochrony danych osobowych i informacji przetwarzanych przez ProteGO Safe została przeprowadzona i udokumentowana w skoroszycie 3 „Ocena i zarządzanie ryzykiem" arkusza Oceny skutków dla ochrony danych (DPIA). Ustalony poziom ryzyka znajduje swoje potwierdzenie w testach bezpieczeństwa, m.in. przeprowadzonych przez Securitum (raport z przeprowadzonego testu bezpieczeństwa dostępny tutaj: https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport). Ministerstwo regularnie zleca retesty aplikacji, w tym również przed wprowadzeniem kolejnej wersji oprogramowania lub innych znaczących zmian. Zgodnie z informacjami wynikającymi z dokumentacji towarzyszącej, stosowne procedury w zakresie kooperacji i udostępniania informacji oraz stosowne procedury reagowania na incydenty, zawierające m.in. procedury powiadamiania oraz zarządzania incydentami i podatnościami zostały wdrożone i obowiązują. MC oraz inne podmioty odpowiedzialne wyznaczyły kanały raportowania błędów i zidentyfikowanych podatności. Zastosowano rozwiązania pozwalające na zachowanie minimalizacji danych; ograniczenie przechowywania danych; szyfrowanie, pseudonimizację i anonimizację. Z uwagi na lokalny charakter działania ProteGO Safe, podmioty odpowiedzialne mają mniejszą możliwość lub brak możliwości ingerowania w system i stan bezpieczeństwa urządzenia użytkownika. Aplikacja nie jest przystosowana do przeprowadzania testów „onboarding security", w tym zakresie użytkownik musi samodzielnie zadbać o stan swojego urządzenia. ProteGO Safe jako aplikacja działająca lokalnie nie posiada dodatkowych zabezpieczeń uwierzytelniających użytkownika. Niemniej inicjacja transmisji danych (dystrybucji klucza diagnostycznego) jest zabezpieczona dodatkowym uwierzytelnieniem. Podmioty odpowiedzialne i zespoły projektowe zdają sobie sprawę z zagrożenia, jakie niesie ze sobą korzystanie ze starszych wersji systemów operacyjnych i starszych technologii na urządzeniach, na których instalowana jest aplikacja ProteGO Safe. Ryzyka związane z korzystaniem z niezabezpieczonych urządzeń mobilnych zostały wzięte pod uwagę podczas przeprowadzania analizy ryzyka i zrównoważone z wykorzystaniem adekwatnych środków zabezpieczających.		podczas lub w związku z korzystaniem z aplikacji ProteGO Safe, ale na co dzień. Ryzyko jest niezależne od podmiotów odpowiedzialnych za operacyjność ProteGO Safe, niemniej jednak dostrzegalne, a w konsekwencji konieczne do wskazania w ramach ryzyk. Przy analizie ryzyka wzięto pod uwagę możliwe konsekwencje związane z korzystaniem z aplikacji ProteGO Safe z wykorzystaniem urządzeń końcowych zainfekowanych złośliwym oprogramowaniem lub rootowanych. Dla dalszego podniesienia bezpieczeństwa danych przechowywanych w aplikacji ProteGO Safe można rozważyć rozwiązanie polegające na zabezpieczeniu aplikacji hasłem lub kodem PIN (w momencie uruchamiania aplikacji, by wejść do niej, użytkownik musiałby wpisywać samodzielnie ustalony, dodatkowy kod zabezpieczający aplikację przed dostępem osób przypadkowych, np. korzystających z telefonu użytkownika aplikacji).