RZĄDOWE CENTRUM BEZPIECZEŃSTWA
00-583 Warszawa, Al. Ujazdowskie 5
(1)

Rządowe Centrum Bezpieczeństwa

Warszawa, dnia 22.04.2021 r.

Znak sprawy: WO.091.1.2021

Egz. pojedynczy

ZAWIADOMIENIE OSOBY KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Charakter naruszenia ochrony danych osobowych

W dniach od 12 do 20 kwietnia 2021 r. na portalu „ArcGIS Online" dla określonych służb mundurowych został udostępniony formularz elektroniczny w celu zbierania niezbędnych danych funkcjonariuszy na potrzeby szczepień przeciwko chorobie COVID-19. Wytypowani przedstawiciele tych służb w wyżej wymienionych dniach sukcesywnie wprowadzali do formularza dane osobowe funkcjonariuszy do szczepień. W formularzu zgłoszeniowym znajdowały się następujące dane: imię i nazwisko, nr PESEL, służbowy adres e-mail, numer telefonu, pełna nazwa macierzystej jednostki organizacyjnej oraz jej adres.

W dniu 20.04.2021 r. Rządowe Centrum Bezpieczeństwa otrzymało informację, że dostęp do formularza był możliwy dla innych osób posiadających konto na ArcGIS. Przez to mogło dojść do naruszenia poufności Pani/Pana danych osobowych.

Opis możliwych konsekwencji naruszenia ochrony danych osobowych

Następstwem naruszenia Pani/Pana danych osobowych może być:

- założenie na Pani/Pana dane osobowe konta internetowego (np. w serwisach społecznościowych, poczty elektronicznej),
- podszycie się pod inną osobę lub instytucję w celu wyłudzenia od Pani/Pana dodatkowych określonych informacji (np. danych do logowania, szczegółów karty kredytowej),
- wykorzystania Pani/Pana danych do zarejestrowania karty telefonicznej typu prepaid, która może posłużyć do celów przestępczych,
- podjęcie przez osoby trzecie próby uzyskania na Pani/Pana szkodę, pożyczek w instytucjach pozabankowych np. przez Internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości,
- osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL,
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osobę trzecią do próby wyłudzenia ubezpieczenia,
- Pani/Pana dane osobowe mogą zostać wykorzystane np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego, tym samym skorzystać z Pani/Pana praw obywatelskich,
- osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilno-prawnych, np. najmu nieruchomości,
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osoby trzecie do ukrycia swojej tożsamości, np. przy otrzymywaniu mandatu,

- może Pani/Pan otrzymywać fałszywe SMS-y lub być narażona/y na przesyłanie spamu na podane konto poczty elektronicznej, linków do podrobionych stron elektronicznych płatności, aplikacji wykradających dane, fikcyjnych sklepów internetowych.

Opis środków zastosowanych przez administratora w celu zminimalizowania ewentualnych negatywnych skutków

W związku z zaistniałym naruszeniem ochrony danych osobowych:

- niezwłocznie zamknięto formularz zgłoszeniowy, celem uniemożliwienia komukolwiek dostępu do niego,
- w trybie pilnym zorganizowano spotkanie z firmą Esri Polska sp. z o.o. (dystrybutorem oprogramowania ArcGIS) celem przeanalizowana sytuacji i zabezpieczenia wszystkich danych, które mogły być dostępne dla osób nieuprawnionych,
- o incydencie poinformowano w dniu 20.04.2021 r. Administratora Danych – Ministra Zdrowia, który w dniu 22 kwietnia 2021 r. zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu ochrony danych osobowych,
- zdarzenie zgłoszono do CSIRT GOV,
- prowadzone jest wewnętrzne postępowanie wyjaśniające i podejmowane będą konsultowane z Ministerstwem Zdrowia inne środki zaradcze w zakresie ochrony danych osobowych,
- powiadomiono komendantów/szefów służb o zdarzeniu, których funkcjonariuszy to dotyczy,
- powiadomiono Prokuraturę Okręgową w Warszawie o uzasadnionym przypuszczeniu popełnienia przestępstwa.

Opis środków proponowanych osobie w celu zminimalizowania ewentualnych negatywnych skutków

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy:

- ignorować nieoczekiwane wiadomości SMS lub poczty elektronicznej, w szczególności od nieznanych nadawców,
- zachować ostrożność w sytuacji odbierania połączeń telefonicznych od nieznanych numerów telefonów, w szczególności przy podawaniu danych osobowych innym osobom,
- skorzystać z możliwości założenia konta w systemie informacji kredytowej lub gospodarczej, w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym wykorzystaniem, w tym monitorowania prób uzyskania kredytu.

Jeśli dowie się Pani/Pan o wykorzystaniu Pani/Pana danych przez osobę nieuprawnioną, prosimy o jak najszybsze przekazanie tej informacji nam oraz swoim przełożonym.

Dane kontaktowe w celu uzyskania dodatkowych informacji

Jeżeli ma Pani/Pan jakiekolwiek pytania lub chciałaby nam Pani/Pan przekazać dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt z:

1) Gestor zbioru danych osobowych – Beata Janowczyk
   Adres e-mail: beata.janowczyk@rcb.gov.pl
   Telefon: 22 36 16 930,
   lub
2) Inspektor Ochrony Danych RCB – Jan Teleon
   Adres e-mail: iod@rcb.gov.pl
   Telefon: 22 36 16 970.