

Zawiadomienie o naruszeniu ochrony danych osobowych

Działając na podstawie art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane dalej RODO, informujemy o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia Pani/Pana praw lub wolności.

Opis charakteru naruszenia

Z przykrością informujemy, że firma FELG Software, której system FELG Dent / FELG z której systemu korzysta nasza placówka, padła ofiarą cyberataku. W jego wyniku mogło dojść do nieuprawnionego dostępu do części danych osobowych.

Chcielibyśmy podkreślić, że nie oznacza to, że Pani/Pana dane zostały odczytane, wykorzystane lub upublicznione. Z informacji przekazanych przez FELG Software wynika, że analiza incydentu jest nadal prowadzona. Na obecnym etapie nie ma informacji potwierdzających, że dane objęte incydem zostały publicznie udostępnione lub wykorzystane przez osoby nieuprawnione. Przeprowadzone przez FELG Software analizy śledcze potwierdziły, że incydent został opanowany oraz że nie ma dowodów wskazujących na dalszy nieuprawniony dostęp do systemów.

Wśród danych objętych incydem mogły znaleźć się Pani/Pana: imię, nazwisko, adres, dane kontaktowe, numer PESEL, daty wizyt, informacje dotyczące płatności, informacje dotyczące recept oraz inne dane identyfikacyjne znajdujące się w dokumentacji.

Możliwe konsekwencje naruszenia

Dysponując wyżej wskazanymi danymi osobowymi, osoba nieuprawniona może podejmować działania związane z możliwością posługiwania się nimi tam, gdzie uwierzytelnienie wymaga podania imienia i nazwiska, adresu, numeru PESEL oraz innych danych, i tym samym osoba taka może:

- podejmować próby uzyskania na Pani/Pana szkodę pożyczek w instytucjach pozabankowych np. przez internet lub telefonicznie, w przypadkach niewymagających okazania dokumentu tożsamości;*
- podejmować próby uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, w*

przypadkach, gdy dostęp do systemów rejestracji pacjenta będzie oparty na potwierdzeniu swojej tożsamości z wykorzystaniem numeru PESEL;

- podejmować próby dyskryminacji Pani/Pana osoby poprzez ujawnienie informacji dotyczących zdrowia, wizyt lub recept;*
- próbować wykorzystać Pani/Pana dane osobowe np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego, a tym samym skorzystać z Pani/Pana praw obywatelskich;*
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osobę trzecią do próby wyłudzenia ubezpieczenia;*
- Osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilnoprawnych, np. najmu nieruchomości;*
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osoby trzecie do ukrycia swojej tożsamości, np. przy otrzymaniu mandatu;*
- Pani/Pana dane mogą zostać wykorzystane do zakładania kont na stronach internetowych, forach, sklepach i innych serwisach, tam gdzie jest brak weryfikacji zwrotnej za pomocą e-maila lub numeru telefonu (SMS/MMS).*

Działania podjęte

Aby ograniczyć negatywne skutki wykrytego ataku, FELG Software podjął następujące działania:

- niezwłocznie zabezpieczył system i zakończył incydent, a także wdrożył dodatkowe, ukierunkowane środki techniczne i organizacyjne mające na celu zapobieganie podobnym incydentom w przyszłości;*
- prowadzi szczegółową analizę incyduentu w celu ustalenia zakresu danych objętych naruszeniem;*
- zgłosił incydent właściwym organom, w tym Prokuraturze;*
- współpracuje z CERT Polska, CSIRT Centrum e-Zdrowia oraz Urzędem Ochrony Danych Osobowych;*
- kontynuuje monitoring systemów w celu wykrycia ewentualnych skutków incyduentu i niezwłocznego reagowania na pojawiające się zagrożenia.*

Nasza placówka jako administrator Państwa danych osobowych, po otrzymaniu informacji o incydencie, dokonała również zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.

Rekomendowane działania

Nasza placówka medyczna przygotowała listę środków zaradczych, których podjęcie zwiększy Pani/Pana bezpieczeństwo:

- *zastrzeżenie numeru PESEL z pomocą aplikacji mobywatel*
- *założenie konta w systemie informacji kredytowej, w celu otrzymania powiadomień o każdej próbie uzyskania pożyczki na Pani/Pana nazwisko, np. BIK <https://www.bik.pl/klienci-indywidualni/alerty-bik> lub <https://chronpesel.pl>*
- *zastrzeżenie dowodu osobistego lub innego dokumentu w banku, w którym Pani/Pan posiada konto, lub w innym, nawet jeśli Pani/Pan nie ma tam założonego konta- lista polskich banków przyjmujących takie zgłoszenia znajduje się na stronie: <https://dokumentyzastrzezone.pl/lista-bankow-zastrzegajacych-dokumenty-od-wszystkich-osob/>*
- *jeśli Pani/Pan podejrzewa, że mógł stać się ofiarą przestępstwa, niezwłocznie proszę zgłosić się na policję. Jeśli przestępstwo zostało popełnione z wykorzystaniem Pani/Pana danych osobowych, należy powiadomić podmioty używające tych danych, np. bank, pożyczkodawców lub sieci telekomunikacyjne. Należy zebrać oraz zachować dowody wszelkich formalnych czynności podjętych w związku z zajściem, aby móc je wykorzystać podczas ewentualnego procesu sądowego.*
- *jeśli używa Pani/Pan numeru PESEL jako loginu na jakimkolwiek portalu lub koncie internetowym- należy zmienić login (o ile dany serwis dopuszcza taką zmianę).*
- *jeśli zaobserwuje Pani/Pan jakiegokolwiek nieprawidłowości, należy nie udostępniać żadnych danych osobowych tylko zgłosić ten fakt organom ścigania.*
- *Jeżeli uzna Pani/Pan, że Pani/Pana dobra osobiste zostały naruszone w związku z wykorzystaniem je przez osoby nieuprawnione przysługuje Pani/Panu możliwość skorzystania ze środków ochrony dóbr osobistych wskazanych w przepisach ustaw*

Kodeks cywilny i Kodeks postępowania cywilnego w związku z ujawnieniem danych dot. Zdrowia.

Bardzo nam przykro, że doszło do takiej sytuacji i przepraszamy za wszystkie niedogodności.

W przypadku pytań dotyczących incydentu lub zakresu danych można skontaktować się:

Kontakt w sprawach dotyczących ochrony danych:

dane.gabinet (@) felg.app

Aktualne informacje dotyczące incydentu będą również udostępniane za pośrednictwem oficjalnych kanałów FELG.

<https://status.felg.cloud/incydent>