Warszawa, dnia 19 października 2026 r.

A2 Clinic sp. z o. o.
ul. Władysława Broniewskiego 87a
58-309 Wałbrzych

Zawiadomienie o wystąpieniu naruszenia

Szanowna Pani/Szanowny Panie,

jako administrator Pani/Pana danych osobowych, chcielibyśmy przekazać Pani/Panu informacje związane z incydentem po stronie A2 Clinic sp. z o.o. z siedzibą w Wałbrzychu (58-309) przy ul. Władysława Broniewskiego 87a (dalej jako: „A2 Clinic"), który to skutkował naruszeniem ochrony danych osobowych.

Dostawca systemu informatycznego wykorzystywanego przez naszą placówkę do prowadzenia elektronicznej dokumentacji medycznej - IQ DENTAL SYSTEM sp. z o. o. z siedzibą we Wrocławiu, ul. Władysława Broniewskiego 87a, 58-309 Wrocław, (dalej jako: „Spółka"), poinformował nas, że padł ofiarą ataku hakerskiego.

W wyniku cyberataku, doszło do nieuprawnionego dostępu do części infrastruktury systemu, który mógł umożliwić osobie nieuprawnionej dostęp do Pani/Pana danych osobowych przetwarzanych w systemie, co stanowi naruszenie ochrony danych osobowych w rozumieniu art. 4 ust. 12 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) („RODO").

W związku z tym, czujemy się zobowiązani do poinformowania, że mogło dojść do ujawnienia Pani/Pana danych osobowych w następującym zakresie: imię, nazwisko, adres zamieszkania, numer PESEL, data urodzenia, numer ID, dane teleadresowe, płeć i informacje stanie zdrowia (rezerwacja wizyty, bez wpisów w dokumentacji medycznej).

Zarówno po stronie A2 Clinic, jak i Spółki niezwłocznie wdrożono odpowiednie działania zaradcze. Sprawa otrzymała najwyższy priorytet. A2 Clinic pragnie zaznaczyć, że jest w stałym kontakcie ze Spółką, w tym przeprowadza weryfikację zastosowanych środków technicznych, fizycznych oraz organizacyjnych celem zabezpieczenia danych osobowych. A2 Clinic wystąpiła również z wnioskiem o udostępnienie informacji w zakresie podjętych środków zaradczych w ramach opisanego zdarzenia.

Pragniemy Panią/Pana zapewnić, że działania naprawcze zostały przez nas podjęte w możliwie najszerszym zakresie, jednakże w związku ze wskazanym powyżej zakresem danych osobowych, których naruszenie dotyczy, czujemy się zobowiązani do poinformowani Pani/Pana o możliwych konsekwencjach zaistniałego naruszenia oraz proponowanych środkach zaradczych.

1. **Konsekwencje zaistniałego naruszenia**

Z uwagi na wskazany powyżej zakres danych osobowych istnieje ryzyko, że osoba, która uzyskała do nich dostęp, może próbować wykorzystać je w sposób niezgodny z prawem, co może dodatkowo skutkować:

- sfałszowaniem dokumentu tożsamości, co może posłużyć do założenia konta bankowego,

- założeniem konta w serwisie aukcyjnym,
- próbą wyłudzenia lub wyłudzeniem dodatkowych danych w innych instytucjach, np. bankach, firmach ubezpieczeniowych, poprzez uwierzytelnienie się na odległość przy użyciu nr PESEL czy daty urodzenia,
- próbą zaciągnięcia lub zaciągnięciem zobowiązań finansowych przy użyciu Pani/Pana danych w instytucjach para-bankowych, których procedury nie wymagają osobistej styczności z wnioskującym i np. weryfikacji dowodu osobistego,
- próbą skorzystania lub skorzystaniem z przysługujących Pani/Panu jako osobie fizycznej praw, takich jak skorzystanie z prawa do bycia zapomnianym czy poprawiania danych osobowych, wycofania udzielonych zgód na przetwarzanie danych, czy praw obywatelskich (głosowanie) przy wykorzystaniu Pani/Pana numer Pesel,
- uzyskaniem dostępu do korzystania ze świadczeń opieki zdrowotnej przysługujących osobom, których dane naruszono oraz ich danych o stanie zdrowia, ponieważ często dostęp do systemów rejestracji Pacjenta można uzyskać telefonicznie potwierdzając swoją tożsamość za pomocą numeru PESEL,
- wyłudzeniem ubezpieczenia lub środków z ubezpieczenia, co może spowodować dla osób, których dane dotyczą, negatywne konsekwencje w postaci problemów związanych z próbą przypisania im odpowiedzialności za dokonanie takiego oszustwa,
- naruszeniem Pani/Pana dobrego imienia.

2. **Proponowane środki zaradcze**

W celu minimalizacji ewentualnych negatywnych skutków zaistniałego zdarzenia, oprócz przekazanych wcześniej informacji, zalecamy podjęcie następujących kroków:

- założenie konta w Biurze Informacji Kredytowej: www.bik.pl lub Krajowym Rejestrze Długów: www.konsument.krd.pl w celu monitorowania statusu swoich zobowiązań finansowych. Są to platformy on-line, do których docierają informacje z instytucji finansowych o zaciąganych zobowiązaniach finansowych oraz zapytaniach kredytowych

poprzedzających udzielenie pożyczki lub kredytu. Platformy pozwalają nie tylko na założenie konta i monitorowania stanu zaciągniętych zobowiązań, ale także umożliwiają ustawienie tzw. „alertów" – powiadomień o zapytanie z bazy lub nowych wpisach oraz umożliwiają ustawienie blokady w postaci zakazu zaciągania nowych zobowiązań finansowych (tzw. zastrzeżenie kredytowe);

- zachowanie szczególnej ostrożności w odpowiedzi na maile oraz połączenia przychodzące w których jest Pani/Pan proszona/y o podanie danych osobowych;
- zachowanie szczególnej ostrożności przy posługiwaniu się dowodem osobistym, w szczególności niepozostawianie go „w zastaw", zezwalanie na kopiowanie go poza instytucjami posiadającymi takie uprawnienie na mocy przepisów prawa, przesyłanie kopii dowodu osobistego drogą e-mail czy faksem;
- w przypadku jakiegokolwiek podejrzenia nadużycia na Pani/Pana rzecz przez osoby trzecie sprawę należy zgłosić do organów ścigania, celem wszczęcia postępowania mającego na celu zapobieżeniu nadużycia i wykrycia sprawcy,
- zachowanie szczególnej ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu,
- zachowaniu szczególnej ostrożności przy uzyskaniu danych o Pani/Pana osobie, w tym informacji o stanie Pani/Pana zdrowia,
- zgłoszenia faktu naruszenia danych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości",
- zastrzeżenie numeru PESEL w serwisie mobywatel.gov.pl poprzez zalogowanie się do systemu, wejście do sekcji „Twoje dane", potem Rejestr Zastrzeżeń PESEL i wybrać „Zastrzeż PESEL" lub „Cofnij zastrzeżenie".

Wskazuje również, iż w wyniku wskazanego zdarzenia przysługuje Pani/Panu możliwość skorzystania ze środków ochrony dóbr osobistych wskazanych w przepisach prawa, w tym ustawie Kodeks Cywilny i Kodeks Postępowania Cywilnego. Ma Pani/Pan prawo do żądania odszkodowania i zadośćuczynienia na wypadek nieuprawnionego wykorzystania Pani/Pana danych, w tym wystąpienia na drogę Sądową jak i poinformowania dalszych organów ścigania.

Pozostajemy do Pani/Pana pełnej dyspozycji w przypadku chęci uzyskania przez Panią/Pana dodatkowego wsparcia prawnego.

Pragniemy Panią/Pana najmocniej **przeprosić** za wszelkie niedogodności związane z niniejszą sprawą.

Zapewniamy, że w razie powzięcia przez A2 Clinic dodatkowych informacji w przedmiotowej sprawie, będziemy się Panią/Panem niezwłocznie kontaktować. Kontakt z Inspektorem Ochrony Danych A2 Clinic (funkcję Inspektora Ochrony Danych pełni Pani Katarzyna Pisarzewska) oraz jego zespołem możliwy jest za pośrednictwem pod adresem e-mail: daneosobowe@luxmed.pl.

Z wyrazami szacunku,
Zespół Ochrony Danych Osobowych A2 Clinic