Racibórz, 26.03.2026 r.

CENTRUM MEDYCZNE "ESKULAP” sp. z o.o.
ul. Kolejowa 19A
47-400 Racibórz

Szanowni Państwo,

CENTRUM MEDYCZNE "ESKULAP” sp. z o.o. informuje że w dniu 24 marca 2026 r. doszło do naruszenia ochrony Państwa danych osobowych w naszym podmiocie leczniczym. Naruszenie polegało na zaszyfrowaniu danych przetwarzanych i przechowywanych na naszych serwerach dedykowanych do obsługi pacjentów placówki. Do zaszyfrowania danych doszło w wyniku ataku typu „ransomware”. Przedmiotowe zdarzenie wiąże się z wysokim ryzykiem naruszenia praw i wolności naszych pacjentów. W wyniku działania cyberprzestępców doszło do utraty dostępności do danych osobowych (dostępu do danych medycznych, historii choroby), a także do wysokiego ryzyka naruszenia ich poufności (wycieku danych). Dotyczy to danych osobowych pacjentów naszej placówki oraz osób powiązanych z pacjentem (np. osób upoważnionych, bliskich, przedstawicieli ustawowych).

Po wykryciu zdarzenia natychmiastowo podjęto działania zmierzające do ograniczenia skutków ataku oraz przywrócenia działania naszej placówki. W wyniku tych działań udało się odzyskać dostęp do danych wytworzonych w naszej placówce do dnia 24.06.2021r. Dokonaliśmy zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowaliśmy uprawnione instytucje (CERT Polska), a także złożyliśmy zawiadomienie o podejrzeniu popełnienia przestępstwa.

Zgodnie z 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) jesteśmy zobowiązani do zawiadomienia Państwa jako osób dotkniętych przedmiotowym naruszeniem.

Poniżej znajdą Państwo szczegółowe informacje.

NA CZYM POLEGA ZDARZENIE?
Ustalono, że naruszenie dotyczyło następujących kategorii danych osobowych pacjentów i osób powiązanych z pacjentem:

- Dane kontaktowe (np. imię, imiona, nazwisko, email, nr telefonu, adres)
- Dane pośrednio identyfikujące (np. data urodzenia),
- Dane jednoznacznie identyfikujące (np. PESEL, nr dowodu osobistego),
- Dane szczególnej kategorii (dane dotyczące zdrowia – historia choroby).

Podkreślamy, iż **nie ma obecnie dowodów na wykorzystanie Państwa danych w sposób nieuprawniony**, jednak **nie można całkowicie wykluczyć takiego ryzyka**. Naruszenie ochrony danych osobowych miało charakter incydentu cyberbezpieczeństwa polegającego na ataku typu *ransomware*. Istnieje wysokie prawdopodobieństwo, że dane osobowe mogły zostać w sposób nieuprawniony pozyskane przez sprawców przed ich zaszyfrowaniem. W konsekwencji nie można wykluczyć ich dalszego wykorzystania w sposób niezgodny z prawem, w tym ich sprzedaży, nielegalnego rozpowszechniania lub użycia do działań przestępczych, takich jak oszustwa czy kradzież tożsamości.

JAKIE JEST RYZYKO ZWIĄZANE ZE ZDARZENIEM?
W związku z naruszeniem możliwe jest wystąpienie następujących, negatywnych konsekwencji:

1. Naruszenie prawa do prywatności, w związku z incydentem polegającym na ujawnieniu osobie nieupoważnionej danych osobowych (np. imię, nazwisko, adres zamieszkania i nr PESEL),
2. Naruszenie dóbr osobistych wynikające z możliwości ujawnienia danych osobowych,
3. Dyskryminacja wynikająca w szczególności z ujawnienia osobom nieupoważnionym Państwa danych osobowych dotyczących stanu zdrowia,
4. Ograniczenie możliwości korzystania z praw obywatelskich i usług kierowanych do ogółu obywateli, w związku z ujawnieniem imienia, nazwiska i nr PESEL (np. głosowania w ramach budżetu obywatelskiego, internetowej rejestracji wizyt w urzędach),
5. Uzyskanie przez osoby trzecie pożyczek w instytucjach parabankowych z użyciem imienia, nazwiska i nr PESEL osoby dotkniętej naruszeniem (np. przez Internet, bez konieczności okazywania dokumentu tożsamości),
6. Uzyskanie przez osoby trzecie dostępu do systemów obsługujących udzielanie świadczeń medycznych osoby dotkniętej naruszeniem,
7. Próby zawarcia umów cywilnoprawnych na szkodę osoby, której dane ujawniono, w związku z ujawnieniem imienia, nazwiska i nr PESEL, np. umów z operatorami telekomunikacyjnymi czy dostawcami sygnału RTV,
8. Uzyskanie przez osoby trzecie możliwości podjęcia próby założenia firmy z wykorzystaniem Państwa danych osobowych, która następnie może posłużyć do wyłudzeń podatkowych, narażając Państwa na nieprzyjemności i konieczność wykazania Państwa braku związku ze sprawą,
9. Uzyskanie przez osoby trzecie możliwości złożenia fałszywej deklaracji podatkowej w Państwa imieniu, powodując tym działaniem wszczęcie postępowania wyjaśniającego w Urzędzie Skarbowym;
10. Ryzyko otrzymania wezwania do zwrotu środków, których faktycznie Państwo nie otrzymaliście,
11. Ryzyko podjęcia próby zamiany Państwa adresu korespondencyjnego, numeru telefonu lub adresu e-mail powiązanego z kontem bankowym oraz z innymi kontami (np. kontem kredytowym, leasingowym, kontami rozliczeniowymi za dostarczone media (gaz, prąd, wodę etc.), czy wszelkiego rodzaju abonamenty i subskrypcje), co może utrudnić Państwu dostęp do tych internetowych kont, a także ryzyko przejęcia istotnych dokumentów w korespondencji z powiązanymi podmiotami,
12. Ryzyko uzyskania dostępu do Państwa świadczeń w ZUS lub NFZ,
13. Ryzyko otrzymania wezwania do złożenia wyjaśnień w sprawie, z którą nie macie Państwo nic wspólnego,
14. Ryzyko wystąpienia ukierunkowanych ataków socjotechnicznych, np.: oszustw metodą “na wnuczka” czy “na policjanta”,
15. Wzrost zagrożenia fizycznego (np. włamania, stalking, niechciane wizyty).

Informujemy, że obecnie istnieją wysokie ryzyka związane z ewentualnym wykorzystaniem Państwa danych osobowych w sposób nieuprawniony, narażające Państwa na ewentualne naruszenia praw i wolności.

CO ZROBILIŚMY I PLANUJEMY ZROBIĆ W ZWIĄZKU ZE ZDARZENIEM?

W związku ze zdarzeniem:

- zawiadomiliśmy o nim naszego Inspektora ochrony danych.
- zgłosiliśmy sprawę do Prezesa Urzędu Ochrony Danych Osobowych,
- złożyliśmy zawiadomienie o popełnieniu przestępstwa,
- zgłosiliśmy sprawę do CERT POLSKA
- podjęliśmy odpowiednie kroki, w celu jeszcze lepszego zabezpieczenia infrastruktury IT,
- zleciliśmy kolejne szkolenia dla naszego personelu medycznego i administracyjnego w zakresie szeroko rozumianej ochrony danych osobowych i cyberbezpieczeństwa

CO MOGĄ PAŃSTWO ZROBIĆ W ZWIĄZKU ZE ZDARZENIEM?

Poniżej przedstawiamy do rozważenia propozycje działań, które mogą Państwo podjąć w związku z przedmiotowym naruszeniem. Pomoże to zabezpieczyć Państwa dane przed niewłaściwym wykorzystaniem:

- Zastrzeżenie numeru PESEL - można to zrobić przez stronę mObywatel.gov.pl lub osobiście w urzędzie gminy / miasta,
- Skorzystanie z Krajowego Rejestru Długów - pozwoli to na weryfikację, czy bank, firma pożyczkowa, operator telekomunikacyjny lub inna firma szukała informacji o Państwa na podstawie numeru PESEL,
- Zachowanie ostrożności przy podawaniu danych innym osobom, zwłaszcza przez telefon i internet,
- Zgłaszanie właściwym organom każdej próby tzw. kradzieży tożsamości,
- Sprawdzenie, czy Państwa dane nie zostały udostępnione w sieci,
- Wykorzystanie dwuetapowej lub wieloetapowej weryfikacji tożsamości w serwisach, które umożliwiają takie narzędzia,
- Zwrócenie szczególnej uwagi na próby logowania na konta,
- Weryfikowanie alertów przesyłanych na adresy e-mail,
- Przejrzenie dostępnych informacji w Internecie na swój temat i usunięcie tych, które mogą wykorzystać przestępcy do nielegalnej działalności, w szczególności nr telefonów komórkowych, adresy e-mail, wizerunek, adresy zamieszkania, ale także zbędne informacje o miejscach pobytu czy zainteresowaniach i wszelkie inne szczegóły, które mogą zostać wykorzystane przez przestępców do podszywania się pod Państwa,

Ponadto informujemy, że w związku ze zdarzeniem przysługuje Państwu prawo skorzystania ze środków ochrony dóbr osobistych, zgodnie z przepisami art. 24 i 448 Kodeksu Cywilnego, oraz art. 82 RODO, na zasadach określonych w tytule VI Kodeksu Postępowania Cywilnego.

Powiadamiając Państwa liczymy na to, iż nasze wyjaśnienia i podjęte działania będą zgodne z Państwa oczekiwaniami. Podkreślamy, iż do naruszenia doszło w wyniku działań cyberprzestępców. Jeżeli mają Państwo wątpliwości co do obsługi przedmiotowego naruszenia ochrony danych osobowych mogą się Państwa zwrócić również do Prezesa Urzędu Ochrony Danych Osobowych.
W razie pytań lub wątpliwości prosimy o kontakt.

Dodatkowo informujemy, iż mogą się Państwo również skontaktować z naszym Inspektorem Ochrony Danych, w celu uzyskania dodatkowych informacji: Inspektor Ochrony Danych - Grzegorz Procajło, e-mail: rodo@jamano.pl

[PODPIS]

Podpisany elektronicznie przez
Jarosław Aleksander Krężel
26.03.2026
15:35:40 +01'00'