

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Dotyczy incydentu bezpieczeństwa u zewnętrznego dostawcy oprogramowania medycznego – MyDr Sp. z o.o.

1. INFORMACJA O INCYDENCIE U DOSTAWCY ZEWNĘTRZNEGO

Z przykrością informujemy, że system naszego podmiotu przetwarzającego – firmy **MyDr Sp. z o.o.** z siedzibą w Warszawie – **24 czerwca 2026 roku** padł ofiarą cyberataku. W jego wyniku doszło do naruszenia poufności danych osobowych.

Kluczowe ustalenia i stan bezpieczeństwa:

- Incydent dotyczył dostawcy oprogramowania MyDr, a nie bezpośrednio infrastruktury Przychodni ESKULAP.
- Przeprowadzone przez MyDr analizy śledcze potwierdziły, że **incydent został opanowany** i nie ma dowodów wskazujących na dalszy nieuprawniony dostęp do systemów.
- Zespoły MyDr oraz zewnętrzni eksperci ds. cyberbezpieczeństwa stale monitorują sytuację i **nie wykryli, aby dane objęte incydem zostały publicznie udostępnione**.

2. ZAKRES DANYCH OBJĘTYCH ZDARZENIEM

Ustalenia dokonane przez MyDr przy wsparciu ekspertów wskazują, że incydent obejmował ograniczony zakres danych powstałych **przed 12 kwietnia 2024 r.** (z wyjątkiem nielicznych przypadków, w których mógł objąć dane zawarte w anulowanych skierowaniach na badania medyczne wystawione po tej dacie).

Wśród danych, które mogły znaleźć się w obszarze ryzyka, znajdują się:

- Imię i nazwisko, adres zamieszkania oraz dane kontaktowe (telefon, e-mail)
- Numer PESEL
- Dane dotyczące zdrowia oraz ubezpieczenia społecznego
- Informacje dotyczące pracodawcy (jeśli zostały podane) oraz inne dane identyfikacyjne

3. POTENCJALNE KONSEKWENCJE I ZALECANE ŚRODKI OSTROŻNOŚCI

Mimo że monitoring nie wykazał dotychczas przypadków wykorzystania ani ujawnienia danych, ze względu na charakter zdarzenia nie można całkowicie wykluczyć ryzyka. W celu zapewnienia Państwu maksymalnego bezpieczeństwa, przedstawiamy potencjalne zagrożenia oraz zalecane działania profilaktyczne:

Ewentualne konsekwencje:

- Możliwość próby zaciągnięcia kredytu lub pożyczki przez osoby nieuprawnione przy użyciu numeru PESEL.
- Próby uzyskania dostępu do usług medycznych/zdrowotnych w placówkach weryfikujących tożsamość PESEL-em.
- Ryzyko próby wykorzystania danych dotyczących zdrowia w sposób niekorzystny dla Pacjenta.

Zalecane działania ochronne:

- **Zastrzeżenie numeru PESEL** (np. poprzez aplikację mObywatel lub w urzędzie gminy).
- Włączenie alertów BIK (Biura Informacji Kredytowej) informujących o próbach zapytania o kredyt.
- Zachowanie ostrożności przy odbieraniu niespodziewanych połączeń, wiadomości SMS lub e-mail (phishing).

4. DZIAŁANIA PRZYCHODNI ESKULAP I KONTAKT

Zapewniamy, że jako Przychodnia ESKULAP traktujemy ochronę Państwa danych z najwyższą powagą. Jesteśmy w stałym kontakcie z dostawcą MyDr i weryfikujemy wszelkie wdrożone przez nich dodatkowe zabezpieczenia.

Z wyrazami szacunku,

Zarząd Przychodni ESKULAP

Bogusława Orzechowska, Jarosław Golubiewski Spółka Partnerska