

Bochnia, 30.07.2026 r.

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowni Państwo,

działając w imieniu Samodzielnego Publicznego Gminnego Zakładu Opieki Zdrowotnej w Bochni (SPGZOZ), na podstawie art. 34 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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), zawiadamiamy o zaistnieniu naruszenia ochrony danych osobowych, , które miało miejsce w siedzibie administracji w miesiącu lipcu. Naruszenie miało charakter wewnętrzny i polegało na wykonaniu i przeniesieniu kopii dokumentów zawierających dane osobowe na trzy prywatne nośniki danych (dyski zewnętrzne) ze stacji roboczych.

Naruszenie objęło szeroki katalog Państwa danych osobowych w zakresie: danych identyfikacyjnych i kontaktowych (imię, nazwisko, adres zamieszkania, numer telefonu, numer PESEL, miejsce i data urodzenia, numer Prawa Wykonywania Zawodu, kwalifikacje, dyplomy, zaświadczenia), danych kadrowo-płacowych i finansowych (wymiar etatu, stanowisko, historia zatrudnienia, wymiar urlopu, karty ewidencji czasu pracy, świadectwa pracy, dokumenty rozliczeniowe ZUS, numery rachunków bankowych, przelewy wypłat, karty wynagrodzeń, kwoty podwyżek, nagród, odpraw, kwoty składek, zasiłków, zaliczek na podatek, zestawienia etatów, informacje o potrąceniach komorniczych, kwoty zadłużenia w PKZP/ZFŚS, przynależność do PZU, PPK, PKZP oraz Izb Pielęgniarskich) oraz danych szczególnej kategorii (dane dotyczące zdrowia zawarte w skanach orzeczeń lekarskich z zakresu medycyny pracy, orzeczeń sanitarno-epidemiologicznych, skanach zaświadczeń ZUS ZLA, dane z Rejestru wypadków przy pracy, skierowania na badania, skany zaświadczeń z Krajowego Rejestru Karnego).

Natychmiast po wykryciu incydentu podjęliśmy kroki w celu zabezpieczenia danych osobowych:

- zawiadomiono organy ścigania (Policję) w celu zabezpieczenia i odzyskania skopiowanych nośników,
- na stacjach roboczych wdrożono pełne szyfrowanie dysków,
- wdrożono dodatkowe wewnętrzne procedury bezpieczeństwa i weryfikacji operacji wykonywanych na danych,
- dokonano zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.

Niemniej jednak, przejęcie wskazanego katalogu danych niesie za sobą wysokie ryzyko wystąpienia negatywnych skutków, takich jak:

- ryzyko kradzieży tożsamości lub wyłudzenia finansowego (np. próba zaciągnięcia pożyczek, kredytów lub zakupów ratalnych na dane przez osoby trzecie, a także założenie konta internetowego lub bankowego z wykorzystaniem numeru PESEL),
- możliwość przeprowadzenia ataków socjotechnicznych/phishing'u (próby wyłudzenia dodatkowych danych lub pieniędzy z wykorzystaniem wiedzy o zatrudnieniu czy sytuacji finansowej),
- ryzyko podszywania się pod uprawnienia zawodowe (ryzyko wykorzystania numeru PWZ, dyplomów oraz zaświadczeń do podszywania się pod pracownika medycznego/wykonywania zawodu przez osobę nieuprawnioną),
- możliwość naruszenia prywatności i dóbr osobistych w związku z ujawnieniem danych medycznych, pracowniczych,
- prawdopodobieństwo otrzymywania niechcianej korespondencji (spam tradycyjny/SMS/połączenia telefoniczne/e-mail),
- możliwość rozpowszechnienia danych osobowych do innych osób nieuprawnionych.

W celu maksymalnej ochrony przed skutkami wycieku danych, stanowczo zalecamy podjęcie następujących kroków:

- zastrzeżenie numeru PESEL – najprościej i bezpłatnie wykonają to Państwo w aplikacji mObywatel, na oficjalnym portalu rządowym www.gov.pl (usługa „Zastrzeż swój numer PESEL”) lub osobiście w dowolnym urzędzie gminy. Zastrzeżenie PESEL skutecznie blokuje możliwość zaciągania zobowiązań finansowych przez osoby nieuprawnione,
- zachowanie ostrożności przy podawaniu danych osobowych innym osobom oraz instytucjom,
- ostrożność przy odbieraniu korespondencji – nieklikanie w podejrzane linki wysyłane w wiadomościach SMS lub e-mail oraz zweryfikowanie tożsamości rozmówcy przed podaniem jakichkolwiek danych przez telefon,
- zwrócenie szczególnej uwagi na wszelkie powiadomienia dotyczące danych osobowych,
- włączenie Alertów BIK – utworzenie konta w Biurze Informacji Kredytowej (www.bik.pl) i włączenie usługi powiadomień SMS/e-mail, która poinformuje o każdej próbie zapytania o Państwa dane kredytowe.

W przypadku, kiedy dowie się Pani/Pan, iż Pani/Pana dane osobowe zostały wykorzystane w niewłaściwym, bezprawnym celu, bardzo prosimy o niezwłoczny kontakt z nami.

Mamy głęboką nadzieję, iż poprzez zaistniały incydent, ta sytuacja nie przyniesie Państwu negatywnych konsekwencji. Zapewniamy także, że podany punkt kontaktowy, tj. biuro@spgzozbochnia.pl jest punktem bezpiecznym, umożliwiającym szybki i bezproblemowy kontakt z naszym Podmiotem. Dodatkowo wskazujemy, iż w przypadku problemów lub wątpliwości związanych z naruszeniem bezpieczeństwa Państwa danych osobowych można skontaktować się z naszym Inspektorem Ochrony Danych – Panią Aleksandrą Szydłowską – pod adresem e-mail: iod@iods.pl oraz pod numerem telefonu: 574 439 221.

p.o. Dyrektora
Samodzielnego Publicznego Szpitala
Zakładu Opieki Zdrowotnej w Bochni
.....
lek.med. Michał Ożewski
(podpis p.o. Dyrektora SP ZOZ w Bochni)