

Bochnia, 21.09.2026 r.

PONOWNE ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowni Państwo,

w związku ze zgłoszeniem zaistniałego incydentu do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych, dnia 18 września 2026 r. otrzymaliśmy uwagi od organu nadzorczego, dotyczące konieczności ponownego zawiadomienia stron. Zgodnie z wystąpieniem Prezesa Urzędu Ochrony Danych Osobowych oraz w trosce o pełną transparentność i rzetelność przekazywanych informacji, przekazujemy poniżej ponowną, pełną treść zawiadomienia.

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), ponownie 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 dotyczy danych przetwarzanych w systemach administracyjnych placówki należących do następujących kategorii osób:

- pacjentów – naruszenie dotyczy danych takich jak: imię i nazwisko, adres zamieszkania, numer PESEL, numer rachunku bankowego, dane o stanie zdrowia (w tym historie wizyt) oraz skany kart EKUZ,
- kontrahentów oraz dostawców – naruszenie dotyczy danych takich jak: imię i nazwisko, kwoty oraz przedmiot zawartych umów, dane zawarte w rejestrze umów, a także dokumentacja związana z zamówieniami publicznymi.
- uczestników wydarzeń organizowanych przez SPGZOZ – naruszenie dotyczy wizerunku utrwalonego na dokumentacji zdjęciowej.

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:

W odniesieniu do PACJENTÓW:

- ryzyko kradzieży tożsamości lub wyłudzenia finansowego (zaciągnięcie pożyczek pozabankowych na skradziony PESEL),
- możliwość przeprowadzenia ataków socjotechnicznych/phishing'u (próby wyłudzenia dodatkowych danych lub pieniędzy poprzez fałszywe SMS-y lub e-maile podszywające się pod placówkę lub banki),
- ryzyko naruszenia prywatności w związku z ujawnieniem informacji o stanie zdrowia,
- ryzyko bezprawnego skorzystania ze świadczeń medycznych na Państwa dane lub nieautoryzowanych wpisów w historii leczenia,
- możliwość założenia kont internetowych na Państwa dane,
- prawdopodobieństwo otrzymywania niechcianych wiadomości e-mail/połączeń telefonicznych,
- dyskryminację,
- ostracyzm społeczny,
- naruszenie dóbr osobistych.

W odniesieniu do KONTRAHENTÓW I DOSTAWCÓW:

- ryzyko utraty poufności informacji handlowych (ujawnienie stawek, warunków umów i danych ofertowych podmiotom trzecim lub konkurencji),
- możliwość naruszenia relacji biznesowych i dóbr osobistych,
- ryzyko naruszenia prywatności w związku z ujawnieniem danych kontaktowych.

Mając na uwadze możliwe konsekwencje związane z naruszeniem bezpieczeństwa Państwa danych osobowych, zalecamy:

Jeśli jesteś PACJENTEM:

- 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,
- 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,
- weryfikację Internetowego Konta Pacjenta (IKP) – regularne sprawdzanie historii wizyt, e-recept i e-zwolnień pod kątem braku nieautoryzowanych wpisów,
- 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 oraz zachowanie czujności przy podawaniu danych osobowych innym osobom lub instytucjom,
- skorzystanie ze środków ochrony dóbr osobistych wskazanych w Kodeksie Cywilnym oraz Kodeksie postępowania cywilnego,
- skorzystanie ze wsparcia psychologicznego w sytuacji odczuwania silnego stresu.

Jeśli jesteś KONTRAHENTEM/DOSTAWCĄ:

- zwiększenie czujności w nadchodzących postępowaniach przetargowych oraz weryfikację nietypowych zapytań ofertowych lub prób kontaktu ze strony podmiotów trzecich pod powołaniem się na dotychczasowe umowy,
- zachowanie ostrożności przy podawaniu danych osobowych innym osobom oraz instytucjom,
- zwracanie uwagi na podejrzaną korespondencję,
- skorzystanie ze środków ochrony dóbr osobistych wskazanych w Kodeksie Cywilnym oraz Kodeksie postępowania cywilnego,
- skorzystanie ze wsparcia psychologicznego w sytuacji odczuwania silnego stresu.

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 Gminnego
Zakładu Opieki Zdrowotnej w Bochni

mgr Małgorzata Oziomek