Zielona Góra, dnia 08.05.2026 r.

Zawiadomienie o możliwości naruszenia ochrony danych osobowych

Na podstawie 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), Zdrojowa Clinic Lubuskie Centrum Gastroenterologii i Hepatologii Dariusz Giezowski, będący Administratorem Państwa danych osobowych informuje o wystąpieniu incydentu bezpieczeństwa, który może mieć wpływ na bezpieczeństwo Państwa danych osobowych.

1. Opis zdarzenia

Nasz dostawca usług poczty elektronicznej poinformował nas o wykryciu w dniu 30 kwietnia 2026 roku nieautoryzowanego dostępu do jednego z serwerów obsługujących naszą korespondencję elektroniczną. W wyniku tego ataku osoby nieuprawnione mogły uzyskać dostęp do treści wiadomości e-mail wymienianych z naszą placówką.

2. Rodzaje danych objętych ryzykiem

Istnieje ryzyko, że niepowołane osoby uzyskały dostęp do Państwa danych osobowych przekazywanych w toku komunikacji e-mailowej, takich jak:

- dane kontaktowe (adresy e-mail, numery telefonów),
- dane adresowe (adres zamieszkania, korespondencyjny)
- dane identyfikacyjne (imię, nazwisko, numer PESEL),
- dokumentacja medyczna oraz informacje o stanie zdrowia.

3. Podjęte działania zaradcze

Natychmiast po wykryciu naruszenia, dostawca usług poczty elektronicznej wdrożył skuteczne blokady i zabezpieczenia. **Zapewniamy, że dalsza komunikacja z placówką jest już bezpieczna.**
Administrator, niezwłocznie po otrzymaniu zgłoszenia:

- rozpoczął proces szczegółowej weryfikacji skali zdarzenia,
- zgłosił incydent do Prezesa Urzędu Ochrony Danych Osobowych (UODO).

Złożone zostało zawiadomienie o możliwości popełnienia przestępstwa.

4. Możliwe konsekwencje dla naszych Pacjentów i Kontrahentów

Należy podkreślić, że obecnie nie ma pewności czy Państwa dane zostały wykradzione, niemniej jednak zalecamy zachowanie szczególnej czujności i ostrożności, zwracania szczególnej uwagi na nietypowe zdarzenia czy na jakiekolwiek sygnały mogące świadczyć o wykorzystywaniu Państwa danych niezgodnie z przepisami prawa.

Naruszenie poufności Państwa danych może wiązać się z ryzykiem ich nieuprawnionego wykorzystania, w tym:

- naruszenie prawa do prywatności, w związku z incydentem polegającym na ujawnieniu osobie nieupoważnionej danych osobowych zwykłych (tj. imię, nazwisko, adres zamieszkania i nr PESEL);
- naruszenie dóbr osobistych wynikające z możliwości ujawnienia imienia i nazwiska, oraz nr PESEL wraz z pozostałymi danymi;
- 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 itp.);
- uzyskanie przez osoby trzecie pożyczek w instytucjach pozabankowych z użyciem imienia, nazwiska i nr PESEL osoby dotkniętej naruszeniem (np. przez Internet, bez konieczności okazywania dokumentu tożsamości);
- uzyskanie przez osoby trzecie dostępu do systemów obsługujących udzielanie świadczeń medycznych osoby dotkniętej naruszeniem (czasami w takich systemach tożsamość potwierdza się za pomocą numeru PESEL);
- ryzyko otrzymania wezwania do zwrotu środków, których faktycznie Państwo nie otrzymaliście;
- 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;
- ryzyko otrzymania wezwania do złożenia wyjaśnień w sprawie, z którą nie macie Państwo nic wspólnego;
- ryzyko wystąpienia ukierunkowanych ataków socjotechnicznych, oszustw metodą “na wnuczka” czy “na policjanta”;
- wzrost zagrożenia fizycznego (np. włamania, stalking, niechciane wizyty).

5. Proponowane środki zaradcze – jakie działania mogą Państwo podjąć?

W związku z ryzykiem ujawnienia Państwa danych osobowych, możecie Państwo zminimalizować wystąpienie opisanych wyżej ryzyk m.in. poprzez:

- zastrzeżenie numeru PESEL. Od 1 czerwca 2024 r. instytucje finansowe (np. banki) mają obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki. W dowolnym momencie mogą Państwo cofnąć

zastrzeżenie, wykonać przysługujące Państwu czynności a następnie zastrzec numer ponownie. Zastrzeżenie numeru PESEL w żaden sposób nie zablokuje Państwa możliwości rejestracji do lekarza, realizacji recepty czy załatwienia sprawy urzędowej, ale zabezpiecza Państwa przed zawarciem umowy kredytu/pożyczki w Państwa imieniu przez osoby do tego nieuprawnione.
Zastrzec numer PESEL można na wiele sposobów, w tym elektronicznie, za pośrednictwem Internetu oraz osobiście w urzędzie. Wszelkie szczegóły tego jak to zrobić znajdują się na rządowej stronie: https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie.;

- przejrzenie dostępnych informacji w Internecie na swój temat i usunięcie tych, które mogą wykorzystać przestępcy do nielegalnej działalności, w szczególności numery 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;
- zachowanie szczególnej rozwagi podczas umieszczania jakichkolwiek prywatnych danych na swój temat w Internecie. Obecnie zakres przestępczej działalności internetowej jest bardzo szeroki i aktywny;
- weryfikację swoich haseł wykorzystywanych w różnych portalach, sklepach internetowych, kontach pocztowych i ich zmianę w taki sposób by były w każdym takim miejscu niepowtarzalne;
- weryfikację występowania Państwa danych w bazie znanych wycieków danych, za pośrednictwem rządowego portalu https://bezpiecznedane.gov.pl.
Jeżeli dowiedzą się Państwo o upublicznieniu, wykorzystaniu lub o jakimkolwiek dalszym ujawnieniu danych osobowych, bardzo proszę o niezwłoczne przekazanie tej informacji do Inspektora Ochrony Danych Zdrojowa Clinic lub o kontakt z najbliższą jednostką Policji albo o zgłoszenie na numer alarmowy 112. Ponadto mają Państwo prawo złożyć zawiadomienie do prokuratury o możliwości popełnienia przestępstwa w związku z wejściem nieuprawnionej osoby w posiadanie Państwa danych osobowych i wykorzystywanie ich w jakikolwiek niedozwolony sposób.

6. Dane kontaktowe

W razie jakichkolwiek pytań lub wątpliwości, proszę o kontakt z Inspektorem Ochrony Danych, Magdaleną Siemaszko, za pośrednictwem poczty elektronicznej: m.siemaszko@zdrojowaclinic.pl.

Najmocniej przepraszamy za wszelkie niedogodności. Podkreślamy, że poufność i bezpieczeństwo Państwa danych są dla nas najwyższym priorytetem i podejmujemy wszelkie możliwe kroki, aby podobne sytuacje nie miały miejsca w przyszłości.