

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowna Pani, Szanowny Panie,

na podstawie art. 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 („RODO”), zawiadamiamy o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia Pani/Pana praw lub wolności.

Administratorem Pani/Pana danych osobowych jest Gabinet Lekarski Marcin Krupa z siedzibą w Turku przy ul. Armii Krajowej 1, 62-700 Turek. Tel. 602 421 047.

Co się stało?

W związku z otrzymaną informacją od MyDr Sp. z o.o. z siedzibą w Warszawie o cyberataku na systemy informatyczne tej spółki, stwierdziliśmy naruszenie poufności danych osobowych. MyDr świadczy na rzecz naszej placówki usługi informatyczne i przetwarza dane osobowe pacjentów w naszym imieniu jako podmiot przetwarzający.

Według informacji przekazanych przez MyDr w wyniku cyberataku doszło do nieuprawnionego dostępu do części środowiska informatycznego, w którym przetwarzany był ograniczony zakres danych osobowych zebranych przed 12 kwietnia 2024 r.

Nie oznacza to, że wszystkie dane objęte zdarzeniem zostały odczytane, skopiowane, wykorzystane lub publicznie udostępnione. Na dzień sporządzenia niniejszego zawiadomienia, analizy oraz monitoring prowadzone przez MyDr nie wykazały przypadków publicznego udostępnienia ani bezprawnego wykorzystania tych danych. Brak takich dowodów nie pozwala jednak całkowicie wykluczyć nieuprawnionego dostępu do danych, ich skopiowania lub wykorzystania w przyszłości.

Chcemy pomóc Pani/Panu zachować bezpieczeństwo na wypadek zmiany okoliczności naruszenia, dlatego przekazujemy informacje o ewentualnych konsekwencjach oraz zalecanych środkach ostrożności, które mogą pomóc w ochronie danych osobowych i ograniczeniu potencjalnych skutków incydentu.

MyDr poinformował nas, że incydent został opanowany, a możliwość dalszego nieuprawnionego dostępu do systemów została usunięta.

Jakich Pani/Pana danych mogło dotyczyć naruszenie?

Według informacji przekazanych przez MyDr naruszenie mogło obejmować następujące kategorie Pani/Pana danych:

- imię i nazwisko;
- adres zamieszkania;
- numer telefonu lub adres poczty elektronicznej;
- numer PESEL;
- stopień pokrewieństwa, w przypadku opiekunów prawnych;

- informacje dotyczące stanu zdrowia zapisane w dokumentacji medycznej;

Jakie ewentualne konsekwencje zidentyfikowaliśmy?

Wśród danych objętych naruszeniem mógł znajdować się numer PESEL, który w połączeniu z imieniem i nazwiskiem oraz danymi kontaktowymi, w określonych sytuacjach, mógłby posłużyć osobom nieuprawnionym do działań niezgodnych z prawem. W szczególności, jeśli dane te zostałyby publicznie ujawnione, mogłyby zostać użyte przez osoby nieuprawnione do:

- próby podszywania się pod Panią/Pana lub kradzieży tożsamości;
- próby zaciągnięcia kredytu, pożyczki albo zawarcia innej umowy z wykorzystaniem Pani/Pana danych;
- próby zakładania kont lub uzyskiwania usług w Pani/Pana imieniu;
- kierowanie do Pani/Pana wiarygodnie wyglądających wiadomości, telefonów lub ofert w celu wyłudzenia dodatkowych danych, haseł, kodów autoryzacyjnych albo pieniędzy;
- próby uzyskania dostępu do informacji lub usług medycznych poprzez podszywanie się pod Panią/Pana;
- ujawnienie informacji dotyczących Pani/Pana zdrowia osobom nieuprawnionym;
- naruszenie prywatności, tajemnicy informacji związanych z Pani/Pana leczeniem;
- wykorzystanie informacji o stanie zdrowia do manipulacji, wywierania presji, oszustwa lub kierowania spersonalizowanych ofert usług medycznych, pseudomedycznych albo terapeutycznych;

Na dzień sporządzenia zawiadomienia nie posiadamy informacji, aby którakolwiek z powyższych konsekwencji rzeczywiście wystąpiła. Nie ma zatem powodów do niepokoju, jednakże zalecamy zachowanie zwiększonej ostrożności.

Jakie działania może Pan/Pani podjąć?

1. Zastrzec numer PESEL

Rekomendujemy bezpłatne zastrzeżenie numeru PESEL:

- w aplikacji mObywatel;
- przez Internet w serwisie mObywatel.gov.pl;
- osobiście w dowolnym urzędzie gminy.

Instytucje finansowe są obecnie zobligowane weryfikować przy zawieraniu umów, czy PESEL jest zastrzeżony, co ogranicza ryzyko użycia danych do nieuprawnionego zaciągania zobowiązań na szkodę innych osób. Zastrzeżenie PESEL nie blokuje jednak możliwości rejestracji u lekarza, realizacji recepty czy załatwienia sprawy w urzędzie – więcej informacji pod linkiem: <https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie>.

2. Zachować ostrożność wobec podejrzanych kontaktów

Prosimy:

- nie przekazywać osobom kontaktującym się telefonicznie lub elektronicznie haseł, kodów SMS, danych logowania, danych karty płatniczej ani dodatkowych informacji medycznych;
- nie otwierać podejrzanych załączników i nie korzystać z linków przesyłanych przez nieznane osoby;
- weryfikować tożsamość osoby podającej się za pracownika placówki medycznej, MyDr, banku, Policji lub innej instytucji – np. wyszukać instytucję w Internecie i zadzwonić na znaleziony numer;
- kontaktować się z daną instytucją, korzystając z numeru telefonu lub adresu podanego na jej oficjalnej stronie, a nie z danych otrzymanych w podejrzanej wiadomości.

Nasza placówka ani MyDr nie będą prosić Pani/Pana o podanie hasła, kodu autoryzacyjnego lub dokonanie płatności w związku z tym naruszeniem.

3. Kontrolować informacje finansowe i medyczne

Warto:

- zwracać uwagę na korespondencję dotyczącą nieznanych zobowiązań, rachunków lub umów;
- regularnie sprawdzać historię rachunku bankowego;
- rozważyć sprawdzenie informacji kredytowej lub uruchomienie powiadomień o próbach zaciągnięcia zobowiązania;
- sprawdzić Internetowe Konto Pacjenta, w szczególności historię leczenia, recept i skierowań, oraz zgłosić zauważone nieprawidłowości;
- zachować ostrożność wobec osób, które znają informacje dotyczące Pani/Pana zdrowia i wykorzystują je do przedstawienia oferty lub wyłudzenia dodatkowych danych.

4. Zgłosić podejrzenie wykorzystania danych

Jeżeli stwierdzi Pani/Pan, że dane zostały wykorzystane niezgodnie z prawem, należy możliwie szybko:

- zawiadomić bank, pożyczkodawcę, placówkę medyczną albo inną instytucję, której dotyczy próba wykorzystania danych;
- zabezpieczyć otrzymane wiadomości, numery telefonów, dokumenty i inne dowody.
- zawiadomić Policję;

Informacje o sposobie zgłoszenia znajdują się pod adresem:

<https://www.gov.pl/web/gov/zglos-przestepstwo>.

Jakie działania zostały podjęte przez MyDr?

Zgodnie z informacjami przekazanymi naszej placówce MyDr:

1. niezwłocznie opanował i zakończył incydent, a także wdrożył dodatkowe, ukierunkowane środki techniczne i organizacyjne mające na celu zapobieganie podobnym incydom w przyszłości;
2. zaangażował wyspecjalizowaną firmę z zakresu cyberbezpieczeństwa w celu przeprowadzenia szczegółowej analizy incydomu;
3. zgłosił incydent wyspecjalizowanej jednostce Policji - Centralnemu Biuru Zwalczenia Cyberprzestępczości Policji i ściśle z nią współpracuje;
4. współpracuje z Ministerstwem Cyfryzacji, Centrum e-Zdrowia, CSIRT NASK i CSIRT Centrum e-Zdrowia;
5. współpracuje z Urzędem Ochrony Danych Osobowych;
6. kontynuuje monitoring systemów w celu wykrycia ewentualnych skutków incydomu i niezwłocznego reagowania na pojawiające się zagrożenia;
7. prowadzi stały monitoring Internetu w celu wykrycia, czy dane, których dotyczy incydent, zostały upublicznione.

Jakie działania podjęła nasza placówka?

Jako administrator Pani/Pana danych osobowych:

1. dokonaliśmy oceny charakteru naruszenia oraz ryzyka dla praw i wolności pacjentów;
2. zgłosiliśmy naruszenie Prezesowi Urzędu Ochrony Danych Osobowych w dniu 05.09.2026 r.;
3. zawiadamiamy osoby, których dane mogły zostać objęte naruszeniem;
4. pozostajemy w kontakcie z MyDr, aby monitorować naruszenie;

Gdzie można uzyskać dodatkowe informacje?

Informacje na temat incydomu bezpieczeństwa danych w systemie MyDr można znaleźć na stronie <https://pacjent.mydr.pl/>.

W przypadku dodatkowych pytań dotyczących zakresu incydomu prosimy o kontakt dane@mydr.pl.

W sprawach dotyczących naruszenia może Pani/Pan skontaktować się z naszą placówką nr tel. 602 421 047.

Przepraszamy za zaistniałą sytuację. Zapewniamy, że traktujemy ochronę danych osobowych i informacji dotyczących zdrowia pacjentów jako sprawę wymagającą szczególnej ochrony.

Z poważaniem

Marcin Krupa

Gabinet Lekarski Marcin Krupa, Lekarz.