DR FACE
by Osuch

Komunikat w sprawie naruszenia ochrony danych osobowych

publikowany na podstawie art. 34 ust. 3 lit. c Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. (RODO)

Szanowni Państwo,

informujemy, że w wyniku cyberataku na system Medyc, w którym nasza placówka prowadzi dokumentację pacjentów, doszło do naruszenia poufności danych osobowych naszych pacjentów. Pacjentom, których adresy e-mail posiadaliśmy. Przesłaliśmy Państwu indywidualne zawiadomienia na ten temat w dniu 8 października 2026 r. Niniejszy komunikat kierujemy do wszystkich osób, których dotyczy zdarzenie, w szczególności do osób, z którymi nie możemy skontaktować się indywidualnie, ponieważ nie posiadamy ich aktualnych danych kontaktowych albo wysłana do nich wiadomość nie została doręczona.

Najważniejsze informacje w skrócie

- Doszło do cyberataku na system Medyc spółki Qbusoft sp. z o.o., w którym nasza placówka prowadzi dokumentację pacjentów. Skopiowano dane pacjentów naszej placówki zarejestrowanych w systemie do 21 sierpnia 2026 r.
- Zakres skopiowanych danych zależy od tego, jakie informacje były zapisane o danej osobie. Potwierdzono skopiowanie danych identyfikacyjnych i kontaktowych: imienia i nazwiska, numeru PESEL, adresu zamieszkania, numeru telefonu i adresu e-mail.
- W przypadku pacjentów, którzy odbyli konsultację lub zabieg, wysoce prawdopodobne jest skopiowanie także zdjęć i plików PDF zapisanych w systemie, w tym zdjęć przesłanych przed zabiegiem, zgód oraz skanów dokumentacji medycznej.
- Dotychczas nie stwierdzono, aby dane zostały opublikowane, nie można jednak tego wykluczyć.
- Zalecamy zastrzeżenie numeru PESEL i ostrożność wobec wiadomości oraz telefonów powołujących się na wyciek.
- Dodatkowe informacje: rejestracja – tel. +48 501093653; Inspektor Ochrony Danych, e-mail: agata.szwed@asprotectis.pl

Kogo dotyczy zdarzenie?

Naruszenie objęło dane wszystkich osób zarejestrowanych w systemie Medyc naszej placówki do 21 sierpnia 2026 r., z całego okresu, w którym korzystamy z tego systemu, w tym:

– pacjentów, którzy przeszli zabieg;

– pacjentów, którzy odbyli konsultację bez zabiegu;

– osób, które umówiły wizytę, ale ostatecznie z niej nie skorzystały;

– osób, które kontaktowały się z placówką i zostały zapisane w systemie wyłącznie z numerem telefonu lub adresem e-mail.

Osób zarejestrowanych po 21 sierpnia 2026 r. naruszenie nie dotyczy.

Co się stało?

System naszego podmiotu przetwarzającego, tj. Qbusoft sp. z o.o. z siedzibą w Gdańsku (producenta oprogramowania Medyc), padł ofiarą cyberataku. Z ustaleń Qbusoft wynika, że w nocy z 22 na 23

sierpnia 2026 r. osoba nieuprawniona wykorzystała nieznaną wcześniej lukę w zabezpieczeniach systemu (podatność typu SQL injection), skopiowała dane pacjentów placówek korzystających z systemu Medyc i wysłała je poza system. Qbusoft potwierdził naruszenie 9 września 2026 r. W dniu 2 października 2026 r. otrzymaliśmy od Qbusoft potwierdzenie, że naruszenie objęło dane wszystkich pacjentów naszej placówki, wraz z informacją o zakresie tych danych, a 6 października 2026 r. – informacje uzupełniające.

Skopiowane dane sprawca zaszyfrował własnym narzędziem, dysponuje więc możliwością ich odczytania. Należy przyjąć, że ma do nich dostęp w czytelnej postaci.

O jakie dane chodzi?

Zakres danych zależy od tego, jakie informacje były zapisane o danej osobie w systemie. U części osób zapisane były wszystkie wymienione poniżej dane, u innych tylko niektóre z nich, na przykład wyłącznie imię i nazwisko z numerem telefonu albo sam adres e-mail. Jeżeli chcą Państwo wiedzieć, jakie dane były zapisane w Państwa przypadku, prosimy o kontakt z rejestracją.

Dane, których skopiowanie zostało potwierdzone

Imię i nazwisko, numer PESEL, adres zamieszkania, numer telefonu oraz adres e-mail – w zakresie, w jakim zostały zapisane w profilu danej osoby.

Dane, których skopiowanie jest wysoce prawdopodobne

Zdjęcia i pliki PDF zapisane w systemie w związku z konsultacją lub zabiegiem, w szczególności zdjęcia przesłane przez pacjentów przed zabiegiem, zgody na zabieg i znieczulenie oraz skany dokumentacji medycznej. Zawierają one informacje o stanie zdrowia, a zdjęcia także wizerunek. Zdjęć wykonywanych po zabiegu nie przechowujemy w tym systemie. Dane te dotyczą wyłącznie osób, które odbyły u nas konsultację lub zabieg.

Dane, których skopiowania nie można wykluczyć

Qbusoft nie potwierdził, ale też nie wykluczył, że naruszenie objęło inne dane zapisane w systemie, na przykład datę urodzenia, dane o wizytach i terminach wizyt, rozpoznania, wystawione recepty i skierowania, dane o rozliczeniach, a także informacje wpisane w uwagach do profilu pacjenta. U części pacjentów zagranicznych, nieposiadających numeru PESEL, w uwagach zapisany był numer paszportu.

Według informacji Qbusoft (stan na 6 października 2026 r.) dane nie zostały dotychczas opublikowane ani wystawione na sprzedaż. Sprawcy nie wystosowali żądań ani gróźb ich ujawnienia. Nie można jednak wykluczyć, że dane zostaną wykorzystane lub ujawnione w przyszłości, dlatego naruszenie wiąże się z wysokim ryzykiem dla praw i wolności osób, których dotyczy.

Jakie ewentualne konsekwencje zidentyfikowaliśmy?

Numer PESEL lub numer paszportu w połączeniu z imieniem, nazwiskiem, adresem i danymi kontaktowymi może posłużyć osobom nieuprawnionym do:

- zaciągnięcia kredytu, pożyczki lub zawarcia innych umów bez Państwa wiedzy;
- uzyskania dostępu do Państwa danych dotyczących zdrowia w placówkach medycznych, w których tożsamość potwierdza się numerem PESEL;
- podszycia się pod Państwa, na przykład przy zawieraniu umów na odległość.

Same dane kontaktowe (numer telefonu, adres e-mail), także bez innych danych, mogą zostać wykorzystane do:

- wiarygodnego podszywania się pod naszą placówkę, bank lub urząd w rozmowie telefonicznej, wiadomości SMS albo e-mail w celu wyłudzenia pieniędzy lub kolejnych danych.

Nieuprawnione użycie danych dotyczących zdrowia i zdjęć może naruszać Państwa prawa, w szczególności gdyby osoby trzecie próbowały wykorzystać te informacje:

- w sposób dla Państwa niekorzystny, w tym naruszający prywatność, dobra osobiste i tajemnicę lekarską;
- w celu oszustwa lub wywarcia nacisku, np. przez kontakt z powołaniem się na wiedzę o przebytym leczeniu.

Jakie działania mogą Państwo podjąć?

W przypadku numeru PESEL

- Można bezpłatnie zastrzec numer PESEL w aplikacji mobilnej mObywatel, przez Internet na stronie mObywatel.gov.pl lub osobiście w urzędzie gminy (miasta). Instytucje finansowe mają obowiązek sprawdzić przy zawieraniu umów, czy PESEL jest zastrzeżony, co ogranicza ryzyko zaciągnięcia zobowiązań na Państwa dane. Zastrzeżenie PESEL nie blokuje rejestracji u lekarza, realizacji recepty ani załatwienia sprawy w urzędzie. W usłudze mObywatel można również sprawdzić, kto i kiedy weryfikował Państwa numer PESEL.
- Można poinformować inne placówki medyczne, z których Państwo korzystają, że osoby trzecie mogą próbować posłużyć się Państwa numerem PESEL.

W przypadku numeru paszportu

- Warto skontaktować się z organem, który wydał paszport (np. właściwym konsulatem lub urzędem w kraju pochodzenia), w celu ustalenia, czy możliwe jest zastrzeżenie dokumentu lub jego wymiana.
- Warto zwracać uwagę na korespondencję dotyczącą umów lub zobowiązań zawartych bez Państwa wiedzy i niezwłocznie ją wyjaśniać.

W przypadku danych kontaktowych i danych dotyczących zdrowia

- Warto zachować szczególną ostrożność wobec niespodziewanych telefonów, wiadomości SMS i e-mail, których nadawca powołuje się na Państwa leczenie, na naszą placówkę albo na wyciek danych, zwłaszcza jeżeli wiadomość zawiera link i zachęca do „sprawdzenia, czy Twoje dane wyciekły”.
- Prosimy nie podawać haseł, kodów ani dodatkowych danych w odpowiedzi na takie kontakty. Nasza placówka nie prosi o nie telefonicznie, SMS-em ani e-mailem. W wiadomościach dotyczących tego zdarzenia odsyłamy wyłącznie do naszej strony internetowej drosuch.pl. Nietypową prośbę rzekomo od nas prosimy potwierdzić, dzwoniąc pod numer 501 093 653.
- W razie potwierdzenia, że dane wykorzystały osoby nieuprawnione, mogą Państwo dochodzić ochrony swoich praw na podstawie właściwych przepisów, w tym Kodeksu cywilnego.

Bez względu na zakres danych, w przypadku podejrzenia, że zostały one wykorzystane niezgodnie z prawem, można zgłosić to na Policję.

Jakie działania zostały już podjęte?

Aby ograniczyć skutki ataku, Qbusoft sp. z o.o. według przekazanych nam informacji:

1. usunął lukę wykorzystaną przez sprawcę oraz inne rozpoznane podatności i przetestował wprowadzone poprawki;
2. przeprowadził przegląd kodu źródłowego aplikacji pod kątem kolejnych podatności;
3. zmienił wszystkie dane dostępowe, które mogły trafić w ręce sprawców;
4. wdrożył dodatkowy monitoring serwerów i aplikacji oraz blokady podejrzanego ruchu;
5. zgłosił incydent Centralnemu Biuru Zwalczania Cyberprzestępczości, Prezesowi Urzędu Ochrony Danych Osobowych, CSIRT NASK, Centrum e-Zdrowia i ZUS;
6. monitoruje, czy dane, których dotyczy incydent, nie zostały upublicznione;
7. zapowiedział niezależny zewnętrzny audyt bezpieczeństwa.

Nasza placówka, jako administrator danych osobowych pacjentów, podjęła następujące działania:

- 2 i 6 października 2026 r. skierowaliśmy do Qbusoft sp. z o.o. żądania przekazania szczegółowych informacji o zakresie i przyczynach naruszenia;
- na podstawie otrzymanych odpowiedzi ustaliliśmy zakres naruszenia dotyczący naszej placówki;
- zgłosiliśmy naruszenie Prezesowi Urzędu Ochrony Danych Osobowych, zgodnie z art. 33 RODO;
- 8 października 2026 r. przesłaliśmy indywidualne zawiadomienia pacjentom, których adresy e-mail posiadaliśmy, a osoby, dla których posiadamy wyłącznie numer telefonu, informujemy wiadomością SMS;
- zmieniliśmy hasła wszystkich użytkowników systemu w naszej placówce oraz sprawdziliśmy konta i uprawnienia;
- na bieżąco śledzimy komunikaty Qbusoft i właściwych instytucji, a o istotnych nowych ustaleniach będziemy informować w tym miejscu.

Gdzie można uzyskać dalsze informacje?

Rejestracja placówki, tel. **501 093 653**, udzieli informacji o zdarzeniu, poinformuje, jakie dane były zapisane w Państwa przypadku, i na Państwa prośbę przekaże pełne zawiadomienie e-mailem lub listownie. Zawiadomienie jest dostępne w języku polskim i angielskim.

W sprawach związanych z ochroną danych osobowych przetwarzanych przez naszą placówkę, w tym w związku z niniejszym komunikatem, można kontaktować się z Inspektorem Ochrony Danych, Panią Agatą Szwed, pod adresem e-mail: **agata.szwed@asprotectis.pl**.

Oficjalne komunikaty dostawcy o incydencie są publikowane na stronie medyc.pl, w zakładce „Komunikaty”.

Przepraszamy za tę sytuację i za niepokój, który może ona wywołać.

Z poważaniem,
Piotr Osuch Chirurgia Plastyczna
Warszawa, 20 października 2026 r.