
12 września 2026 r.

Pan Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych
Urząd Ochrony Danych Osobowych
ul. Stanisława Moniuszki 1A
00-014 Warszawa

PETYCJA W INTERESIE PUBLICZNYM
WEZWANIE DO NATYCHMIASTOWYCH DZIAŁAŃ SYSTEMOWYCH I
OGÓLNOPOLSKIEJ KAMPANII INFORMACYJNEJ PO INCYDENCIE MYDR

Dotyczy: ochrony obywateli po masowym naruszeniu bezpieczeństwa danych osobowych, w tym numerów PESEL i danych dotyczących zdrowia

Szanowny Panie Prezesie,

Działając w imieniu Stowarzyszenia oraz w interesie publicznym, na podstawie art. 2 ust. 1, ust. 2 pkt 1 i ust. 3 ustawy z dnia 11 lipca 2014 r. o petycjach, wzywamy Prezesa Urzędu Ochrony Danych Osobowych do niezwłocznego podjęcia działań systemowych wobec skutków incydentu MyDr oraz do przeprowadzenia ogólnopolskiej kampanii informacyjnej skierowanej bezpośrednio do obywateli.

Nie składamy indywidualnej skargi w sprawie jednej placówki. Zwracamy się o reakcję organu nadzorczego na problem o masowej skali, który dotyczy bezpieczeństwa danych pacjentów, zaufania do ochrony zdrowia i realnego ryzyka wykorzystywania tożsamości obywateli.

**OBYWATEL NIE MOŻE ZOSTAĆ SAM Z KOLEJNYM SMS-EM O WYCIEKU NUMERU
PESEL I DANYCH O ZDROWIU.**

1. SKALA ZJAWISKA I CHAOS INFORMACYJNY

Rządowy serwis BezpieczneDane.gov.pl potwierdza nieuprawniony dostęp do bazy systemu MyDr, z którego korzystają przychodnie i gabinety lekarskie, oraz umożliwia sprawdzenie, czy numer PESEL danej osoby znalazł się w zbiorze objętym incydemtem. UODO wskazuje, że według doniesień medialnych naruszenie może dotyczyć niemal 19 mln osób oraz około 12 tys. podmiotów leczniczych. Są to liczby, które wymagają reakcji państwa porównywalnej z innymi zdarzeniami zagrażającymi bezpieczeństwu milionów obywateli.

W ostatnich dniach obywatele otrzymują kolejne SMS-y od różnych placówek medycznych. Prezes Zarządu w jednym tygodniu otrzymała dwa powiadomienia od dwóch różnych placówek, oba wskazujące na możliwość naruszenia danych, w tym numeru PESEL i danych dotyczących zdrowia. W mediach oraz publicznych dyskusjach internetowych powtarzają się relacje osób otrzymujących podobne wiadomości, pytania o ich autentyczność oraz obawy przed kredytem, oszustwem i wykorzystaniem informacji medycznych.

Zastrzegamy dla rzetelności: kilka wiadomości od różnych placówek nie musi dowodzić kilku odrębnych włamań. Może być następstwem jednego incydentu u wspólnego dostawcy i rozproszonego obowiązku zawiadamiania wykonywanego przez wielu administratorów. Z punktu widzenia obywatela skutek pozostaje jednak ten sam - alarmujące komunikaty przychodzą sukcesywnie, mają różną treść, a odpowiedzialność i źródło informacji są nieczytelne.

Potencjalna skala	niemal 19 mln osób - liczba przywołana przez UODO za doniesieniami medialnymi
Sieć administratorów	około 12 tys. podmiotów leczniczych - skala wskazana przez UODO za doniesieniami medialnymi
Dane	numer PESEL oraz możliwe dane dotyczące zdrowia - dane szczególnej kategorii
Doświadczenie	dwa powiadomienia z dwóch różnych placówek otrzymane przez Prezesa Zarządu w jednym tygodniu
Najważniejsze ryzyka	kradzież tożsamości, oszustwa, phishing, dyskryminacja, stygmatyzacja i naruszenie dóbr osobistych

2. DOTYCHCZASOWA REAKCJA NIE ZAPEWNI WYSTARCZAJĄCEJ OCHRONY SPOŁECZNEJ

Odnotowujemy, że Prezes UODO zapowiedział kontrolę w spółce MyDr, opublikował informacje dla administratorów i odpowiedzi na pytania z infolinii. Działania te są potrzebne. Nie rozwiązują jednak problemu komunikacji z milionami osób, które otrzymują krótkie wiadomości od kolejnych placówek i nie wiedzą, czy SMS jest autentyczny, jaki dokładnie zakres ich danych został objęty incydemem ani jakie czynności powinni wykonać dzisiaj, a jakie przez kolejne miesiące.

Sam UODO wyjaśnia, że w związku z incydemem MyDr osoba nie musi składać indywidualnej skargi, ponieważ Prezes UODO prowadzi kontrolę. Urząd wskazuje również, że kara finansowa nie jest nakładana na wniosek, lecz z inicjatywy organu po indywidualnej ocenie sprawy. Oznacza to, że ciężaru uruchamiania reakcji państwa nie wolno przerzucać na obywatela.

Nie akceptujemy modelu, w którym obywatel ma sam rozpoznawać prawdziwość wiadomości, dociekać relacji pomiędzy placówką a dostawcą systemu, pisać kolejne skargi i oczekiwać latami na rozstrzygnięcie.

P. zna konkretne postępowania przed Prezesem UODO trwające około 2-2,5 roku. Tak długi czas w sprawach dotyczących bieżącej ochrony praw człowieka podważa praktyczną skuteczność ochrony. Publicznie opisane orzecznictwo sądów administracyjnych potwierdza, że przewlekłość postępowań UODO nie jest problemem wyłącznie teoretycznym.

3. PODSTAWA OBOWIĄZKU DZIAŁANIA

Dane dotyczące zdrowia należą do szczególnych kategorii danych, o których mowa w art. 9 RODO. Ich ujawnienia nie można odwrócić przez wymianę dokumentu lub zmianę hasła. Mogą one przez lata służyć do profilowania, szantażu, dyskryminacji, stygmatyzacji albo uwiarygodniania kolejnych oszustw.

Art. 57 ust. 1 lit. a, b, d, f i h RODO powierza organowi nadzorczemu między innymi monitorowanie i egzekwowanie stosowania RODO, upowszechnianie wiedzy społeczeństwa o ryzykach i prawach, udzielanie administratorom informacji, rozpatrywanie skarg oraz prowadzenie postępowań. Art. 58 RODO zapewnia uprawnienia dochodzeniowe i naprawcze. Art. 83 ust. 1 RODO wymaga, by administracyjne kary pieniężne były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

Z tych przepisów wynika nie tylko możliwość, ale obowiązek aktywnego działania Prezesa UODO. Komunikat umieszczony na stronie Urzędu nie jest równoznaczny z dotarciem do milionów obywateli. Przy tej skali potrzebna jest informacja powtarzana w telewizji, radiu, serwisach informacyjnych, mediach społecznościowych, placówkach medycznych i kanałach administracji publicznej.

4. ŻĄDANIA

Wzywamy Prezesa UODO do podjęcia następujących działań:

1. W terminie 7 dni uruchomić jednoznaczny, stale aktualizowany komunikat kryzysowy dla obywateli, widoczny na stronie głównej UODO i dystrybuowany w kanałach ogólnopolskich.
2. Zainicjować wspólnie z Ministerstwem Cyfryzacji, Ministerstwem Zdrowia, NASK, CERT Polska i Rzecznikiem Praw Pacjenta ogólnopolską kampanię informacyjną w telewizji, radiu, internecie i placówkach ochrony zdrowia. Kampania ma docierać do osób, które nie śledzą specjalistycznych stron urzędowych.
3. Przygotować jeden państwowy poradnik dla osoby, która otrzymała SMS, wraz z prostą ścieżką sprawdzenia autentyczności komunikatu i uzyskania informacji o konkretnych kategoriach danych.
4. Opracować i zalecić administratorom jednolity wzór zawiadomienia bez aktywnych linków, z pełną nazwą placówki, datą incydentu, wskazaniem źródła danych, rzeczywistym zakresem naruszenia, kontaktem do IOD oraz jasnym opisem działań ochronnych.
5. Kontynuować działania z urzędu nie tylko wobec MyDr, ale również ocenić wykonanie obowiązków przez reprezentatywną grupę administratorów danych medycznych, w szczególności na gruncie art. 28, 32, 33 i 34 RODO.
6. Po zakończeniu ustaleń zastosować wobec podmiotów, których odpowiedzialność zostanie potwierdzona, środki naprawcze i sankcje skuteczne, proporcjonalne oraz odstraszające. Skala możliwego naruszenia nie pozwala na reakcję wyłącznie symboliczną.
7. Publikować co najmniej raz w miesiącu zbiorczą informację o postępie działań: liczbie zgłoszeń naruszeń, liczbie administratorów objętych analizą, kategoriach danych, wykonanych kontrolach, wydanych zaleceniach i zakończonych postępowaniach - w granicach niezagrożających śledztwu ani bezpieczeństwu systemów.
8. Przedstawić plan sektorowego wzmocnienia bezpieczeństwa danych medycznych, obejmujący wymagania wobec dostawców systemów, regularne testy zabezpieczeń, ocenę ryzyka łańcucha dostaw, kontrolę uprawnień oraz procedury reagowania kryzysowego.
9. Ujawnić dane o sprawności postępowań UODO za lata 2024-2026: średni i medianowy czas zakończenia spraw, liczbę spraw trwających ponad 12 i 24 miesiące oraz działania zmierzające do eliminacji przewlekłości.
10. W terminie 30 dni przedstawić publiczny harmonogram dalszych działań w sprawie MyDr oraz wskazać jednostkę UODO odpowiedzialną za komunikację z osobami dotkniętymi incydentem.

5. MINIMUM INFORMACYJNE DLA OBYWATELA

Kampania publiczna powinna wprost i bez języka urzędowego wyjaśniać obywatelowi:

- jak sprawdzić w serwisie BezpieczneDane.gov.pl, czy jego numer PESEL znalazł się w zbiorze objętym incydem;
- jak bezpłatnie zastrzec numer PESEL oraz sprawdzić historię jego weryfikacji;
- jak potwierdzić autentyczność SMS-a bez klikania w link i bez korzystania z numeru podanego w wiadomości;
- jakich danych nigdy nie podawać rozmówcy, nawet gdy zna on nazwę przychodni, lekarza albo szczegóły wcześniejszej wizyty;
- jak włączyć dodatkowe zabezpieczenia kont i rozpoznać próbę phishingu lub oszustwa;
- gdzie zgłosić podejrzaną SMS, próbę wyłudzenia, użycie tożsamości albo brak informacji od administratora;
- jak uzyskać od placówki informację o dokładnym zakresie danych objętych naruszeniem i jak dochodzić praw z RODO;
- że ryzyko związane z danymi medycznymi nie kończy się po kilku dniach i wymaga długotrwałej ostrożności.

KRÓTKI SMS NIE JEST SYSTEMEM OCHRONY. SYSTEM OCHRONY MUSI WYJAŚNIAĆ, WERYFIKOWAĆ, OSTRZEGAĆ I EGZEKWOWAĆ ODPOWIEDZIALNOŚĆ.

6. OCZEKIWANA INFORMACJA ZWROTNA

Oczekujemy potraktowania niniejszego wystąpienia jako petycji w interesie publicznym, opublikowania jej w Biuletynie Informacji Publicznej zgodnie z ustawą o petycjach oraz przekazania odpowiedzi obejmującej konkretne decyzje, terminy, jednostki odpowiedzialne i mierzalny zasięg działań informacyjnych.

Prosimy o wskazanie, które z powyższych działań zostaną wdrożone, w jakim terminie, a w przypadku odmowy - o przedstawienie pełnego uzasadnienia prawnego i faktycznego. Odpowiedź ogólna, ograniczona do odesłania do istniejących podstron internetowych lub powtórzenia treści RODO, nie będzie adekwatna do społecznej skali problemu.

Miliony osób nie powinny dowiadywać się o zagrożeniu dla ich tożsamości i prywatności z kolejnych, niejednorodnych SMS-ów. Oczekujemy od konstytucyjnie niezależnego organu nadzorczego obecności tam, gdzie obywatele rzeczywiście szukają informacji - w głównych mediach, w prostych komunikatach i w działaniach podejmowanych z urzędu, zanim szkody staną się nieodwracalne.

Z wyrazami szacunku

Prezes Zarządu

7. PODSTAWA PRAWNA I MATERIAŁY ŹRÓDŁOWE

- UODO, "Administrator musi zgłosić wyciek, do którego doszło w podmiocie przetwarzającym", 12.08.2026 - <https://uodo.gov.pl/pl/138/4538>
- UODO, "Prezes UODO skontroluje spółkę MyDr", 13.08.2026 - <https://uodo.gov.pl/pl/138/4540>
- UODO, "Pytania zadawane przez podmioty danych oraz administratorów związane z incydentem bezpieczeństwa MyDr", 27.08.2026 - <https://uodo.gov.pl/pl/615/4550>
- UODO, "Wyciek danych - co dalej?", 12.08.2026 - <https://uodo.gov.pl/pl/138/4539>
- BezpieczneDane.gov.pl, informacja o incydencie MyDr i możliwość sprawdzenia numeru PESEL - <https://bezpiecznedane.gov.pl/>
- UODO, informacje o Prezesie Urzędu i dane kontaktowe - <https://uodo.gov.pl/pl/544>
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 - RODO - <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679>
- Ustawa z dnia 11 lipca 2014 r. o petycjach - ELI - <https://eli.gov.pl/eli/DU/2014/1195/oql>
- TVN24, relacje pacjentów otrzymujących SMS-y po incydencie MyDr - <https://tvn24.pl/biznes/tech/wyciek-danych-pacjentow-ostzegaja-przed-kredytami-i-oszustwami-st9227309>
- Dziennik Gazeta Prawna, opis orzeczenia WSA w sprawie przewlekłości postępowania Prezesa UODO, sygn. II SAB/Wa 86/25 - <https://edgp.gazetaprawna.pl/prawo/prawo-administracyjne/artykuly/11263685,organ-prowadzil-sprawe-przewleklo-kiedy-sad-pryzna-stronie-rekompens.html>

Stan źródeł i informacji publicznych sprawdzono na dzień 12 września 2026 r. Relacje medialne i internetowe wykorzystano wyłącznie do wykazania społecznej skali niepewności; ustalenia o incydencie i kompetencjach organu oparto przede wszystkim na źródłach urzędowych i obowiązujących przepisach.