



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.167.2026
Warszawa, 21 września 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 25 sierpnia br. Pośla na Sejm RP Pana Jana Warzechy w sprawie wycieku danych z systemów firmy MyDr (interpelacja nr 19319)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

Ad 1) Kiedy Ministerstwo Cyfryzacji po raz pierwszy otrzymało informację o możliwości wycieku z systemów MyDr i jakie działania podjęło w pierwszych godzinach po jej uzyskaniu?

Ministerstwo Cyfryzacji otrzymało informację o incydencie od zespołu reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego CSIRT NASK w dniu 10.08.2026 r. poprzez kanał komunikacji Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), o którym mowa w ustawie o krajowym systemie cyberbezpieczeństwa¹. Zespół CSIRT NASK, który otrzymał informacje w tej sprawie podjął kontakt z firmą i rozpoczął realizację swoich zadań, w tym koordynację obsługi incydentu, zgodnie z swoim zakresem odpowiedzialności określonym w art. 26 ust. 3 i 6 ustawy o KSC.

12.08.2026 r. odbyło się posiedzenie PCOC w tej sprawie.

Ad 2) Ilu obywateli faktycznie dotyczy naruszenie, jakie dokładnie kategorie danych zostały przejęte oraz kiedy każda z poszkodowanych osób zostanie o tym bezpośrednio poinformowana?

Firma będąca właścicielem systemu MyDr EDM potwierdziła wystąpienie kradzieży danych. CSIRT NASK koordynuje obsługę incydentu, czynności w tej sprawie realizuje Centralne Biuro Zwalczania Cyberprzestępczości oraz Prokuratura.

Według aktualnych danych zdarzenie dotyczy ok. 18,8 mln osób oraz ponad 12 tys. placówek medycznych korzystających z oprogramowania MyDr EDM, wielkość pozyskanej bazy przekracza 2 TB. Naruszenie objęło dane historyczne gromadzone do kwietnia 2024 r. Szczegółowa analiza zakresu danych jest przeprowadzana.

Wstępne analizy wskazują na przejęcie bazy danych zawierającej zarówno dane osobowe jak i w niektórych przypadkach informacje dotyczące procesu leczenia. Zakres przejętych informacji nie jest jednolity i różni się w zależności od osoby.

Zgodnie z przepisami RODO firma MyDr jako podmiot przetwarzający dane (procesor) powinien poinformować o wycieku administratorów danych (placówki medyczne i gabinety korzystające z tego oprogramowania), którzy w zależności od uwarunkowań zobowiązani są powiadomić osoby dotknięte wyciekiem danych oraz Prezesa UODO.

¹ Art. 62a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm) (dalej: ustawa o KSC)

Ad 3) Czy przed cyberatakiem przeprowadzono kontrole lub audyty bezpieczeństwa systemów MyDr, a jeżeli tak, jakie były ich wyniki i czy stwierdzone nieprawidłowości zostały usunięte?

Ministerstwo Cyfryzacji nie prowadziło kontroli lub audytów bezpieczeństwa systemów MyDr. W obecnym stanie prawnym Ministerstwo Cyfryzacji nie posiada podstaw prawnych, aby przeprowadzić tego rodzaju kontrolę lub audyty bezpieczeństwa systemów MyDr.

Ad 4) Jakie konkretne formy bezpłatnej ochrony, poza możliwością zastrzeżenia numeru PESEL, rząd zapewni osobom zagrożonym kradzieżą tożsamości, oszustwami finansowymi i szantażem z wykorzystaniem danych medycznych?

Obywatele mogą zastrzec PESEL w prosty sposób zarówno w aplikacji mObywatel, jak i na stronie internetowej gov.pl oraz w urzędzie gminy. Możliwość zastrzeżenia numeru PESEL to bezpłatna usługa publiczna. Chroni przed skutkami kradzieży tożsamości i spłaty zobowiązań finansowych wziętych przez oszustów na wykradzione dane².

Obywatele mogą ponadto na portalu bezpiecznedane.gov.pl skorzystać z powiadomień mailowych o wyciekach. Planowane jest także dodanie powiadomień sms, jak również integracja portalu bezpiecznedane.gov.pl z aplikacją mObywatel, co umożliwi przekazywanie ostrzeżeń o wyciekach poprzez tę aplikację.

Ministerstwo Cyfryzacji i inne instytucje KSC prowadzą także liczne inne działania podnoszące poziom cyberbezpieczeństwa, w tym samych obywateli, które pozwalają ograniczyć skutki działań przy wykorzystaniu przejętych danych, przykładowo wynikające z ustawy o zwalczaniu nadużyć w komunikacji elektronicznej³ (np. lista ostrzeżeń).

Na chwilę obecną żadne dane z wycieku nie zostały upublicznione. Zespoły CSIRT i służby na bieżąco monitorują sieć (w tym fora przestępcze oraz darknet), by wychwycić potencjalne upublicznienie danych. Wyszukiwane są również potencjalne anomalie wskazujące na możliwość wykorzystywania danych z wycieku.

Ad 5) Kto poniesie odpowiedzialność za ewentualne zaniedbania oraz w jakim terminie Ministerstwo przedstawi plan zmian prawnych i organizacyjnych, które mają zapobiec podobnym wyciekom w przyszłości?

Obecnie prowadzone jest śledztwo Policji pod nadzorem Prokuratury, Urząd Ochrony Danych Osobowych zapowiedział natomiast kontrolę firmy MyDr⁴.

Odnosząc się do zmian prawnych i organizacyjnych należy zwrócić uwagę, że podwyższone i mające zastosowanie do znacznie szerszego kręgu podmiotów wymogi cyberbezpieczeństwa wprowadzone zostały poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa, która weszła w życie 3 kwietnia 2026 r. Szczegółowe wymogi cyberbezpieczeństwa określone zostały w art. 8. W szczególności przepisy te stanowią, że podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający m.in: szacowanie ryzyka, wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (m.in. bezpieczeństwo łańcuchów dostaw, zapewnienie ciągłości działania), zarządzania incydentami, stosowanie mechanizmów zapewniających

² <https://www.gov.pl/web/cyfryzacja/chron-swoje-dane-z-mobywatelem-zastrzez-numer-pesel-w-aplikacji>

³ Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. z 2024 r. poz. 1803 z późn. zm.)

⁴ <https://uodo.gov.pl/pl/138/4540>

poufność, integralność, dostępność i autentyczność danych, aktualizacja oprogramowania i eliminowanie podatności, stosowanie mechanizmów kryptograficznych.

W kontekście tych wymogów należy zwrócić uwagę na status firmy MyDr Sp. z o.o. i innych podobnych dostawców usług w KSC oraz na okres przejściowy związany z nowelizacją ustawy o KSC. Gdy wszystkie przepisy zaczną obowiązywać Państwo Polskie będzie miało większą możliwość oddziaływania na podmioty KSC w celu zapewniania cyberbezpieczeństwa państwa, gospodarki i obywateli.

Ze względu na przewidziany w ustawie tryb samoidentyfikacji należy wskazać, że jeśli przedsiębiorstwo MyDr Sp. z o.o. lub inni dostawcy usług, będą podlegać obowiązkowi KSC, oznaczać to będzie, że:

- 1) firma MyDr Sp. z o.o. oraz inni dostawcy systemów wykorzystywanych przez podmioty lecznicze mają czas do 3 października 2026 r. na wpis do wykazu podmiotów kluczowych i podmiotów ważnych;
- 2) organ właściwy ds. cyberbezpieczeństwa dla danego sektora (zgodnie z art. 41 ustawy o KSC) ma prawo wystąpić do konkretnego podmiotu o przekazanie danych i informacji w celu ustalenia, czy podmiot podlega pod ustawę o KSC i należy go uznać za podmiot kluczowy lub podmiot ważny (art. 43 ust. 1);
- 3) organ właściwy ds. cyberbezpieczeństwa może decyzją, na podstawie art. 71 ust. 1 ustawy o KSC uznać za podmiot kluczowy lub podmiot ważny także podmioty, które nie spełniają kryteriów wielkościowych (co najmniej średniego przedsiębiorstwa), jednak np. jako jedyne świadczą usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej, zakłócenie usługi spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego, zakłócenie usługi spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub świadczenie usługi przez ten podmiot ma istotne znaczenie na poziomie wojewódzkim lub krajowym lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy.

Jednocześnie należy podkreślić, że ustawa o KSC przewiduje także wymagania bezpieczeństwa w obszarze łańcucha dostaw. Oznacza to, że nawet jeśli podmiot MyDr Sp. z o.o. lub inni dostawcy systemów wykorzystywanych przez podmioty lecznicze na szeroką skalę nie podlegaliby pod ustawę o KSC, to ze względu na to, że swoje usługi świadczą podmiotom, które są podmiotami kluczowymi lub podmiotami ważnymi, również ma obowiązki z zakresu cyberbezpieczeństwa. Obowiązek zagwarantowania bezpiecznego łańcucha dostaw spoczywałby w takiej sytuacji na podmiotach leczniczych jako podmiotach kluczowych, a nie na samym dostawcy.

Obowiązki z ustawy o KSC zaczynają obowiązywać od 3 kwietnia 2027 r., obecnie trwa okres dostosowawczy.

Wydłużenie okresu dostosowawczego (z 6 miesięcy do 12 miesięcy) wynika z uzgodnień na etapie sejmowym w trakcie procesu legislacyjnego nowelizacji ustawy o KSC. Analogicznie wstrzymanie stosowania przepisów o karach pieniężnych na okres 2 lat także wynika z tych uzgodnień.

Jednocześnie Ministerstwo Cyfryzacji analizuje potencjalne uzupełnienie przepisów dotyczących cyberbezpieczeństwa. Przy czym należy mieć na uwadze przedstawione powyżej kwestie związane z okresem dostosowawczym nowelizacji ustawy o KSC uchwalonej w tym roku, która już wprowadziła wysokie wymagania dotyczące cyberbezpieczeństwa.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych