



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.168.2026
Warszawa, 07 września 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 25 sierpnia br. Posłanki na Sejm RP Pani Magdaleny Filipek-Sobczak w sprawie cyberataku i wycieku danych zdrowotnych nawet 19 mln Polaków (interpelacja nr 19215)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłankę pytania.

Ad 1) Ilu dokładnie obywateli dotyczy przedmiotowy incydent i na jakiej podstawie Ministerstwo Cyfryzacji oszacowało skalę możliwego wycieku na blisko 19 milionów osób?

Według aktualnych danych zdarzenie dotyczy ok. 18,8 mln osób oraz ponad 12 tys. placówek medycznych korzystających z oprogramowania MyDr EDM. Naruszenie objęło dane historyczne gromadzone do kwietnia 2024 r. Szczegółowa analiza zakresu danych jest przeprowadzana. Informacje te bazują danych z obsługi incydenty przez firmę MyDr Sp. z o.o., działań realizowanych przez zespół reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego CSIRT NASK, który wspiera firmę w obsłudze incydentu oraz czynności realizowanych przez Centralne Biuro Zwalczania Cyberprzestępczości Policji pod nadzorem Prokuratury.

Ad 2) Jakie dokładnie kategorie danych zostały wykradzione lub mogły zostać wykradzione? Czy obejmują one numery PESEL, adresy zamieszkania, numery telefonów, adresy e-mail, historię leczenia, informacje o diagnozach, chorobach, wizytach lekarskich, wystawionych receptach, przyjmowanych lekach, zwolnieniach lekarskich lub skierowaniach?

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.

Ad 3) Czy Ministerstwo posiada wiedzę, kiedy dokładnie doszło do włamania do systemów MyDr, kiedy atak został wykryty oraz kiedy o zdarzeniu zostały poinformowane właściwe organy państwa?

Zgodnie z komunikatem Prokuratury Okręgowej w Warszawie nieuprawniony dostęp do systemu nastąpił nie później niż 6 sierpnia 2026. Pierwsze czynności z urzędu podjęli funkcjonariusze Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) w dniu 10 sierpnia 2026 r., a formalne dochodzenie wszczęto 12 sierpnia 2026 r.¹

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

¹ <https://www.gov.pl/web/po-warszawa/postepowania-przygotowawcze-w-sprawie-bezprawnego-uzyskania-danych-wrażliwych-z-systemu-my-dr-sp-z-oo-i-ich-bezprawnego-przetwarzania>

cyberbezpieczeństwa². 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. Ponadto, w ramach realizacji zadań Pełnomocnika Rządu ds. Cyberbezpieczeństwa Ministerstwo Cyfryzacji na bieżąco koordynuje działania w ramach kanału komunikacji PCOC oraz w innych roboczych dwu- lub wielostronnych kontaktach pomiędzy właściwymi instytucjami.

Ad 4) Jak długo cyberprzestępcy mogli posiadać nieuprawniony dostęp do infrastruktury informatycznej oraz danych pacjentów?

Szczegółowe ustalenia dotyczące ataku oraz wykorzystanych podatności w systemie prywatnej firmy są przedmiotem działań CSIRT NASK oraz postępowań prowadzonych przez CBZC pod nadzorem Prokuratury. Zgodnie z komunikatem CBZC z dnia 18.08.2026 r. z uwagi na dobro postępowania oraz złożoność czynności prowadzonych przez CBZC, obecnie Policja nie ujawnia szczegółów śledztwa³.

Ad 5) Czy skradzione dane zostały już opublikowane, wystawione na sprzedaż lub przekazane osobom trzecim? Czy polskie służby posiadają informacje wskazujące, że przestępcy próbują wykorzystać je do wyłudzeń lub innych przestępstw?

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 potencjalne anomalie wskazujące na możliwość wykorzystywania danych z wycieku.

Ad 6) Czy przed cyberatakiem systemy MyDr były przedmiotem kontroli, audytów lub testów bezpieczeństwa prowadzonych przez instytucje państwowe? Jeżeli tak, kiedy przeprowadzono ostatnią taką kontrolę i jakie były jej wyniki?

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

Ad 7) Czy w toku dotychczasowych czynności stwierdzono zaniedbania po stronie administratora lub podmiotów odpowiedzialnych za bezpieczeństwo systemu?

Szczegółowe ustalenia dotyczące ataku oraz wykorzystanych podatności w systemie prywatnej firmy są przedmiotem działań CSIRT NASK oraz postępowań prowadzonych przez CBZC pod nadzorem Prokuratury. Zgodnie z komunikatem CBZC z dnia 18.08.2026 r. z uwagi na dobro postępowania oraz złożoność czynności prowadzonych przez CBZC, obecnie Policja nie ujawnia szczegółów śledztwa.

Urząd Ochrony Danych Osobowych zapowiedział kontrolę firmy MyDr⁴.

Ad 8) Jakie konkretne działania podejmie państwo w celu ochrony osób, których dane zostały skradzione, poza rekomendacją zastrzeżenia numeru PESEL?

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

² 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)

³ <https://cbzc.policja.gov.pl/bzc/aktualnosci/1013,Komunikat-dot-wycieku-danych-pacjentow-z-systemu-informatycznego.html>

⁴ <https://uodo.gov.pl/pl/138/4540>

to bezpłatna usługa publiczna. Chroni przed skutkami kradzieży tożsamości i spłaty zobowiązań finansowych wziętych przez oszustów na wykradzione dane⁵.

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 elektronicznej⁶ (np. lista ostrzeżeń).

Zespoły CSIRT i służby na bieżąco monitorują sieć (w tym fora przestępcze oraz darknet), by wychwycić potencjalne upublicznienie danych. Wyszukiwane są potencjalne anomalie wskazujące na możliwość wykorzystywania danych z wycieku.

Ad 9) Kiedy każda osoba poszkodowana otrzyma indywidualną informację o tym, czy jej dane wyciekły oraz jaki dokładnie zakres jej danych został przejęty?

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

Ad 10) Czy Rząd planuje zapewnić poszkodowanym bezpłatne narzędzia umożliwiające monitorowanie prób wykorzystania ich danych, w szczególności prób zaciągania zobowiązań finansowych lub kradzieży tożsamości?

Obywatele mogą zastrzec PESEL w prosty sposób zarówno w aplikacji mObywatel, jak i na stronie internetowej w domenie 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 dane⁷.

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 elektronicznej (np. lista ostrzeżeń).

Ad 11) Jakie działania zostaną podjęte wobec około 12 tysięcy placówek medycznych korzystających z przedmiotowego oprogramowania, aby zweryfikować bezpieczeństwo ich systemów i zapobiec kolejnym incydentom?

Incydent obsługuje firma MyDr. Weryfikacja i zapewnienie bezpieczeństwa systemów MyDr pozostaje w zakresie obowiązków spółki. Firma w komunikacie zapewniała, że "Na dzień dzisiejszy potwierdzamy, że: nasze systemy są w pełni operacyjne i bezpieczne w użyciu, zarówno dla pacjentów, jak i lekarzy"⁸.

⁵ <https://www.gov.pl/web/cyfryzacja/chron-swoje-dane-z-mobywatelem-zastrzez-numer-pesel-w-aplikacji>

⁶ Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. z 2024 r. poz. 1803 z późn. zm.)

⁷ <https://www.gov.pl/web/cyfryzacja/chron-swoje-dane-z-mobywatelem-zastrzez-numer-pesel-w-aplikacji>

⁸ <https://pro.mydr.pl/portal-info>

Jednocześnie firma w swych działaniach dotyczących cyberbezpieczeństwa jest wspierana przez CSIRT NASK, który koordynuje obsługę incydentu, zgodnie z swoimi kompetencjami określonymi w art. 26 ust. 3 i 6 ustawy o krajowym systemie cyberbezpieczeństwa. Czynności w tej sprawie realizuje Centralne Biuro Zwalczania Cyberprzestępczości oraz Prokuratura.

W zakresie cyberbezpieczeństwa sektora ochrony zdrowia działania realizuje sektorowy zespół CSIRT CeZ, działający w strukturze Centrum e-Zdrowia podległego Ministerstwu Zdrowia. CSIRT CeZ na bieżąco monitoruje potencjalny wpływ incydentu na podmioty korzystające z oprogramowania dostawcy oraz prowadzi działania prewencyjne obejmujące stopniową wymianę certyfikatów P1. Działania te mają charakter zapobiegawczy i stanowią dodatkowe wzmocnienie bezpieczeństwa⁹.

Ad 12) Czy po tym zdarzeniu Ministerstwo Cyfryzacji planuje przeprowadzenie nadzwyczajnych audytów cyberbezpieczeństwa systemów informatycznych wykorzystywanych przez podmioty ochrony zdrowia do przetwarzania danych medycznych milionów obywateli?

Podwyższone i mające zastosowanie do znacznie szerszego kręgu podmiotów wymogi cyberbezpieczeństwa wprowadzone zostały poprzez nowelizację ustawy o KSC, która weszła w życie 3 kwietnia 2026 r. Wymogi w zakresie cyberbezpieczeństwa określone są szczegółowo w przywołanym art. 8 w odpowiedzi na pytanie nr 13.

Jednocześnie znowelizowana ustawa o KSC wprowadziła obowiązki dotyczące audytów, określone w art. 15.

W kontekście powyższych wymogów należy zwrócić uwagę na status firmy MyDr Sp. z o.o. i innych podobnych dostawców usług w KSC oraz specyficzny okres przejściowy związany z nowelizacją ustawy o KSC. Implikuje to bowiem możliwość działania instytucji państwa w ramach przewidzianych prawem trybów. Gdy wszystkie przepisy zaczną obowiązywać Państwo Polskie będzie miało większą możliwość oddziaływania w celu zapewniania cyberbezpieczeństwa państwa, gospodarki i obywateli.

Niezależnie od powyższego należy zwrócić uwagę, że w marcu br. Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał także komunikat z zaleceniami dla sektora ochrony zdrowia i innych podmiotów KSC¹⁰. Ich zastosowanie przez podmioty z sektora ochrony zdrowia znacznie podniesienie poziom cyberbezpieczeństwa przez podmioty z tego sektora.

Jednocześnie za opracowanie sektorowych wytycznych, zgodnie z art. 42 ustawy o KSC, odpowiadają organy właściwe ds. cyberbezpieczeństwa w poszczególnych sektorach, tj. dla sektora ochrony zdrowia Minister Zdrowia oraz Minister Obrony Narodowej (dla podmiotów podległych MON).

Ad 13) Czy Rząd zamierza dokonać zmian prawnych lub wprowadzić dodatkowe standardy bezpieczeństwa dla prywatnych podmiotów przetwarzających na tak dużą skalę dane dotyczące zdrowia obywateli?

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,

⁹ <https://www.cez.gov.pl/pl/page/o-nas/aktualnosci/dzialania-prewencyjne-po-incydencie-dotyczacym-fir...>

¹⁰ <https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa--zalecenia-dla-sektora-ochrony-zdrowia-i-innych-podmiotow-ksc>

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 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 zapewnienia cyberbezpieczeństwa państwa, gospodarki i obywateli.

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

- 1) firma MyDr Sp. z o.o. oraz inni podobni dostawcy usług 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 uznać 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 podobni dostawcy usług 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 zaczną 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.

Ad 14) Kto ponosi odpowiedzialność za nadzór nad bezpieczeństwem tak dużych zbiorów danych medycznych i czy w ocenie Pana Ministra obecny system nadzoru okazał się wystarczający?

W zakresie cyberbezpieczeństwa zgodnie z informacjami przedstawionymi w odpowiedzi na pytania nr 12 i 13.

W zakresie ochrony danych osobowych zgodnie z rozporządzeniem 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) oraz ustawą o ochronie danych osobowych¹¹. Zgodnie z ww. ustawą organem właściwym w sprawie ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (art. 34).

Ad 15) Jakie konsekwencje prawne, administracyjne lub finansowe mogą zostać wyciągnięte wobec podmiotów odpowiedzialnych za ewentualne zaniedbania, jeżeli zostaną one potwierdzone?

W zakresie cyberbezpieczeństwa zgodnie z informacjami przedstawionymi w odpowiedzi na pytania nr 12 i 13.

W zakresie ochrony danych osobowych zgodnie z przepisami prawa przywołanymi w odpowiedzi na pytanie 14.

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

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

¹¹ Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 z późn. zm.)