



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.154.2026
Warszawa, 08 września 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 17 sierpnia br. Pośła na Sejm RP Pana Bartłomieja Pejo w sprawie cyberataku na systemy firmy MyDr oraz wycieku danych blisko 19 milionów obywateli (interpelacja nr 19211)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

Ad 1) Jaka jest dokładna chronologia incydentu, w szczególności kiedy nastąpiło pierwsze nieuprawnione wejście do systemów, kiedy firma MyDr wykryła atak oraz kiedy powiadomiono Ministra Cyfryzacji, właściwy CSIRT, organy ścigania, administratorów danych i Prezesa UODO?

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 roku¹.

W tym samym dniu odbyło się posiedzenie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) w tej sprawie. Firma MyDr obecnie nie dokonała samoidentyfikacji jako podmiot krajowego systemu cyberbezpieczeństwa (KSC) (zgodnie z ustawą podmioty mają czas na samoidentyfikację do 3 października 2026 r.), więc na chwilę obecną nie podlega ustawowemu obowiązkowi zgłaszania incydentów do zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Zespół CSIRT NASK otrzymał informacje w tej sprawie i podjął kontakt z firmą. Ministerstwo Cyfryzacji otrzymało informację o incydencie od CSIRT NASK w dniu 10.08.2026 r. poprzez kanał komunikacji PCOC.

Natomiast obowiązek powiadomienia administratorów danych (placówek medycznych) oraz Prezesa Urzędu Ochrony Danych Osobowych (UODO) wynika z przepisów RODO i spoczywa na podmiocie przetwarzającym.

Ad 2) Ilu dokładnie obywateli dotyczy naruszenie? Proszę o podanie liczby potwierdzonych unikatowych osób, rekordów, numerów PESEL, objętych incydemntem placówek oraz okresu, z którego pochodzą dane. Czy wśród poszkodowanych są osoby małoletnie?

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.

Ad 3) Jakie kategorie danych zostały ujawnione? Czy wyciek obejmuje imiona i nazwiska, numery PESEL, adresy, numery telefonów, adresy e-mail, informacje o placówkach i lekarzach, datach wizyt, rozpoznaniach, wynikach badań, receptach, lekach,

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>

skierowaniach lub dokumentacji medycznej? Proszę o wskazanie liczby osób dotkniętych wyciekiem w odniesieniu do każdej kategorii danych.

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. Na dzień tworzonej odpowiedzi, żadne dane z wycieku nie zostały upublicznione. CBZC oraz właściwy CSIRT na bieżąco monitorują sieć, by wychwycić potencjalne upublicznienie danych.

Ad 4) Czy potwierdzono faktyczne skopiowanie i wyniesienie danych poza infrastrukturę MyDr, czy jedynie możliwość uzyskania do nich dostępu? Na jakich dowodach informatyki śledczej oparto potwierdzenie wycieku i jaka część deklarowanych przez sprawców 2,5 TB danych została zweryfikowana?

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 Okręgowa w Warszawie. Dotychczasowe ustalenia wskazują na pozyskanie przez sprawców bazy o wielkości przekraczającej 2 TB.

Ad 5) Czy potwierdzono doniesienia o wykorzystaniu podatności typu XXE podczas obsługi certyfikatów PKCS#12, uzyskaniu możliwości zdalnego wykonania kodu oraz przejściu klucza API do repozytorium GitHub? Czy podatność była wcześniej znana, a jeżeli tak – od kiedy i dlaczego nie została usunięta?

Szczegółowe ustalenia dotyczące wektora 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 śledztwa².

Ad 6) Czy atakujący uzyskali dostęp do kodu źródłowego, kluczy API, certyfikatów, danych uwierzytelniających lub innych sekretów umożliwiających dostęp do kolejnych systemów? Czy wszystkie takie klucze i certyfikat zostały unieważnione i wymienione?

Według Centrum e-Zdrowia (CeZ), jednostki podległej Ministerstwu Zdrowia, nie stwierdzono naruszenia ani nieuprawnionego użycia certyfikatów komunikacji z systemem P1. Zapobiegawczo CeZ i firma MyDr realizują proces stopniowej wymiany tych certyfikatów. Szczegółowe informacje znajdują się w komunikacie CeZ³.

Ad 7) Czy stwierdzono możliwość dostępu do systemów Centrum e-Zdrowia, systemu P1, Internetowego Konta Pacjenta, systemu e-recept, e-skierowań, systemów NFZ albo infrastruktury poszczególnych placówek? Czy wykluczono przemieszczanie się sprawców pomiędzy połączonymi systemami?

Incydent nie dotyczy systemów Ministerstwa Cyfryzacji ani żadnych państwowych systemów informatycznych. Bezpieczeństwo centralnych usług e-zdrowia (P1, IKP, e-recepta) nie zostało naruszone.

Ad 8) Czy naruszenie dotyczyło wyłącznie poufności danych, czy również ich integralności i dostępności? Czy wykluczono możliwość zmiany, usunięcia lub dodania fałszywych informacji w dokumentacji medycznej, receptach albo historii leczenia?

Dostępne informacje wskazują na naruszenie poufności danych historycznych (wyciek). Nie odnotowano wpływu incydentu na bieżące funkcjonowanie jednostek systemu

² <https://cbzc.policja.gov.pl/bzc/aktualnosci/1013,Komunikat-dot-wycieku-danych-pacjentow-z-systemu-informatycznego.html>

³ <https://www.cez.gov.pl/pl/page/o-nas/aktualnosci/dzialania-prewencyjne-po-incydencie-dotyczacym-fir...>

ochrony zdrowia oraz integralność danych w systemach centralnych. Podmioty lecznicze wykorzystujące oprogramowanie MyDr EDM funkcjonują w normalnym trybie.

Ad 9) Jakże dokładnie działania podjęto w celu odcięcia sprawców, zabezpieczenia dowodów oraz przywrócenia systemów? Kto przeprowadził niezależną analizę powłamaniami i na jakiej podstawie uznano, że systemy MyDr mogą obecnie bezpiecznie obsługiwać placówki medyczne?

Incydent obsługuje firma MyDr. Weryfikacja i zapewnienie bezpieczeństwa systemów MyDr pozostaje w zakresie obowiązków spółki. Firma w komunikacie z 12.08.2006 r. zapewniała, że "Na dzień dzisiejszy potwierdzamy, że: nasze systemy są w pełni operacyjne i bezpieczne w użyciu, zarówno dla pacjentów, jak i lekarzy"⁴.

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 cyberbezpieczeństwa⁵. Czynności w tej sprawie realizuje Centralne Biuro Zwalczania Cyberprzestępczości oraz Prokuratura Okręgowa w Warszawie.

Ad 10) Czy firma MyDr była w dniu incydentu wpisana albo złożyła wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych w ramach Krajowego Systemu Cyberbezpieczeństwa? Jaki status posiadała, jakie obowiązki wynikające z ustawy o KSC miały do niej zastosowanie i czy incydent został zgłoszony za pośrednictwem systemu S46?

Firma MyDr w dniu incydentu nie była wpisana ani nie złożyła wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych w ramach Krajowego Systemu Cyberbezpieczeństwa. W związku z tym incydent nie był zgłoszony poprzez system S46. Obowiązek korzystania z systemu S46 dla podmiotów KSC będzie obowiązywać od 3 kwietnia 2027 r.

Ad 11) Czy ze względu na obsługę około 12 tysięcy placówek medycznych rozważane jest uznanie MyDr za podmiot kluczowy lub ważny niezależnie od kryterium wielkości, z uwagi na systemowe znaczenie świadczonych usług i potencjalne skutki dla zdrowia publicznego?

Podmioty, które na dzień wejścia w życie nowelizacji ustawy o KSC spełniały kryteria podmiotu kluczowego lub podmiotu ważnego mają termin do 3 października 2026 r. na samorejestrację. Jeśli podmiot nie spełnia kryteriów, np. wielkościowych, jest możliwość w drodze decyzji uznania za podmiot kluczowy lub podmiot ważny, zgodnie z art. 71 ustawy o KSC. Na chwilę obecną taka decyzja nie została wydana w odniesieniu do firmy MyDr.

Należy jednocześnie zwrócić uwagę, że w ramach nowelizacji ustawy o KSC obowiązkami w zakresie cyberbezpieczeństwa objęto szeroki katalog podmiotów, w tym podmioty z sektora ochrony zdrowia. Nawet jeśli dostawca oprogramowania dla podmiotów KSC sam nie jest bezpośrednio zakwalifikowany jako podmiot KSC, powinien podlegać wymaganiom dotyczącym łańcucha dostaw podmiotów kluczowych i podmiotów ważnych, które są obowiązane do zapewnienia bezpieczeństwa stosowanych produktów i usług ICT, stosowanie do art. 8 ust. 1 ustawy o KSC.

Ad 12) Ilu administratorów danych zostało już poinformowanych przez MyDr? Ile placówek zgłosiło naruszenie Prezesowi UODO, a ile rozpoczęło bezpośrednie informowanie pacjentów? Czy rząd przygotowuje jednolity wzór komunikatu, aby każdy

⁴ <https://pro.mydr.pl/portal-info>

⁵ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.) (ustawa o KSC)

obywatel otrzymał jasną informację, jakie jego dane zostały ujawnione i jakie działania powinien podjąć?

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. Zgodnie z deklaracjami firmy MyDr, przygotowywane są do przekazania placówkom medycznym zweryfikowane pakiety informacyjne potrzebne do realizacji ich obowiązków wynikających z RODO.

Ad 13) Kiedy dane pochodzące z tego incydentu zostaną udostępnione do sprawdzenia w portalu „Bezpieczne Dane”? Czy obywatel otrzyma wyłącznie informację o obecności w wycieku, czy również o konkretnych kategoriach ujawnionych danych, dacie zdarzenia i administratorze, który je przetwarzał?

Mając na względzie stanowisko Centralnego Biura Zwalczania Cyberprzestępczości⁶, Ministerstwo Cyfryzacji oczekiwało na informację od Policji dotyczącą terminu, w którym możliwe będzie dodanie danych pochodzących z wycieku do serwisu bezpiecznedane.gov.pl. Po przekazaniu zweryfikowanych informacji, zespół NASK-PIB, prowadzący wskazany serwis, w dniu 29 sierpnia 2026 r. dodał informacje o wycieku z firmy MyDr, dzięki czemu obywatele mogą zweryfikować, czy ich dane znalazły się w tym wycieku.

Kierując się dobrem obywateli, do serwisu przekazano wyłącznie informację o numerach PESEL, które znalazły się w wycieku. Nie udostępniono natomiast informacji dotyczących zakresu ujawnionych danych. Należy podkreślić, że portal nie przechowuje numerów PESEL, lecz wyłącznie ich bezpieczne skróty kryptograficzne. Ponadto serwis umożliwia wyłącznie zalogowanemu użytkownikowi sprawdzenie, czy jego numer PESEL znalazł się w bazie danych objętych wyciekiem.

Ad 14) Czy rząd uruchomi dla poszkodowanych dedykowaną infolinię, powiadomienia w aplikacji mObywatel, uproszczone zastrzeganie numeru PESEL oraz mechanizmy ostrzegania o próbach wykorzystania wykradzionych danych? Czy przewidziano bezpłatne monitorowanie prób zaciągania zobowiązań na dane poszkodowanych?

Ministerstwo Cyfryzacji nie prowadzi dedykowanej infolinii w związku z tym incydem.

Obywatele mogą zastrzec PESEL w prosty sposób zarówno w aplikacji mObywatel, jak i na stronie internetowej w domenie gov.pl⁷ oraz w urzędzie gminy⁸.

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.

Właściwe instytucje KSC monitorują cyberprzestrzeń pod kątem potencjalnego wykorzystania danych z wycieku.

Ad 15) Czy banki, operatorzy telekomunikacyjni, placówki medyczne i inne podmioty narażone na wykorzystanie wykradzionych danych otrzymały wskaźniki zagrożeń oraz zalecenia dotyczące wykrywania prób oszustw, przejęcia kont i kampanii phishingowych?

⁶ <https://cbzc.policja.gov.pl/bzc/aktualnosci/1013,Komunikat-dot-wycieku-danych-pacjentow-z-systemu-informatycznego.html>

⁷ <https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie>

⁸ <https://www.gov.pl/web/cyfryzacja/chron-swoje-dane-z-mobywatelem-zastrzez-numer-pesel-w-aplikacji>

Właściwe instytucje KSC monitorują cyberprzestrzeń pod kątem potencjalnego wykorzystania danych z wycieku.

Ad 16) Czy Ministerstwo Cyfryzacji, wspólnie z Ministerstwem Zdrowia, przeprowadzi pilny audyt największych dostawców systemów elektronicznej dokumentacji medycznej? Czy zostaną wprowadzone obowiązkowe minimalne standardy obejmujące m.in. segmentację infrastruktury, wieloskładnikowe uwierzytelnianie, zarządzanie kluczami, szyfrowanie danych, testy penetracyjne, monitoring bezpieczeństwa i kontrolę łańcucha dostaw?

Znowelizowana ustawa o KSC nakłada na podmioty KSC (w tym z sektora ochrony zdrowia) obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji, uwzględniającego m.in. uwierzytelnianie wieloskładnikowe (MFA), plany ciągłości działania oraz bezpieczeństwo łańcucha dostaw, zarządzanie dostępem, kryptografię. Wymogi w zakresie cyberbezpieczeństwa określone są szczegółowo w art. 8 ustawy o KSC.

W marcu br. Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał także komunikat z zaleceniami dla sektora ochrony zdrowia i innych podmiotów KSC⁹.

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 17) Czy zostanie przygotowany i opublikowany raport poincydentowy zawierający przyczynę ataku, chronologię, skalę naruszenia, ocenę zastosowanych zabezpieczeń, podjęte działania naprawcze oraz rekomendacje systemowe? W jakim terminie raport zostanie przedstawiony opinii publicznej i właściwej komisji sejmowej?

Obecnie priorytetem są prowadzone czynności związane z wyjaśnieniem okoliczności incydentu, oceną jego skutków oraz ustaleniem sprawców. Działania realizowane są przez właściwe organy i służby, w tym CBZC i Prokuraturę. CSIRT NASK zapewnia wsparcie eksperckie i techniczne w zakresie obsługi incydentu.

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

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

⁹ <https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa--zalecenia-dla-sektora-ochrony-zdrowia-i-innych-podmiotow-ksc>