Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.201.2026
Warszawa, 25 października 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 8 października br. Posła na Sejm RP Pana Bartosza Józefa Kownackiego w sprawie stanu cyberbezpieczeństwa państwa, masowych wycieków danych medycznych Polaków oraz odpowiedzialności za skuteczność systemu ochrony cyberprzestrzeni (interpelacja nr 20206)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jak Pan Premier ocenia skuteczność polityki cyberbezpieczeństwa prowadzonej przez Rząd i Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, skoro w ciągu kilku tygodni ujawniono kolejne poważne incydenty dotyczące danych medycznych milionów obywateli?

Zagrożenia w cyberprzestrzeni mają charakter dynamiczny i stale rosnący, dlatego w celu kompleksowej rozbudowy i wzmocnienia Krajowego Systemu Cyberbezpieczeństwa (KSC) w bieżący roku uchwalono nowelizację ustawy o krajowym systemie cyberbezpieczeństwa[1]. Przepisy te wprowadzają nowe mechanizmy zwiększające bezpieczeństwo usług i systemów, z których codziennie korzystają obywatele, przedsiębiorcy oraz instytucje publiczne, w tym w zakresie nadzoru. Przy czym obecnie obowiązują przewidziane prawem okresy dostosowawcze – wprowadzone m.in. w wyniku poprawek w Sejmie – co oznacza, że pełną skuteczność oraz kompletność narzędzi zarządczych i kontrolnych rząd uzyska po ich zakończeniu.

Równolegle przyjęto nową Strategię Cyberbezpieczeństwa RP[2], stanowiącą kluczowy dokument kierunkowy dla dalszego rozwoju KSC oraz wyznaczającą długofalowe cele w zakresie budowania odporności cyfrowej państwa.

Ad 2) Ile - od 13 grudnia 2023 r. do dnia udzielenia odpowiedzi na niniejszą interpelację - odnotowano incydentów cyberbezpieczeństwa, w których doszło lub mogło dojść do nieuprawnionego dostępu do danych co najmniej 100 tys. osób? Proszę o przedstawienie ich wykazu wraz z datą, podmiotem, rodzajem danych i liczbą osób objętych incydentem.

Ad 3) Ile osób - według aktualnej wiedzy Rządu, po wyeliminowaniu przypadków wielokrotnego liczenia tych samych osób - zostało w tym okresie dotkniętych naruszeniami bezpieczeństwa danych?

Ad 4) Ile spośród tych incydentów dotyczyło danych medycznych lub innych danych szczególnych kategorii w rozumieniu art. 9 RODO?

Ministerstwo Cyfryzacji nie prowadzi klasyfikacji incydentów według kryterium liczby osób, których dane dotyczą, nie są również klasyfikowane pod kątem kategorii przetwarzanych danych osobowych, w tym danych szczególnych kategorii, o których

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.) (ustawa o KSC)
[2] Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. z 2026 r. poz. 309)

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

mowa w art. 9 RODO. Koordynacje obsługi incydentów prowadzą właściwe zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

Niezależnie od zgłaszania incydentów cyberbezpieczeństwa należy wskazać, że zgodnie z art. 33 RODO administratorzy danych osobowych są obowiązani do zgłaszania naruszeń ochrony danych osobowych właściwemu organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W Polsce właściwym organem nadzorczym w tym zakresie jest Prezes Urzędu Ochrony Danych Osobowych.

Ad 5) Jakie informacje o zagrożeniach dla systemów informatycznych sektora ochrony zdrowia otrzymywali od początku obecnej kadencji Rządu: Prezes Rady Ministrów, Minister Cyfryzacji, Pełnomocnik Rządu do spraw Cyberbezpieczeństwa, Minister Zdrowia, Centrum e-Zdrowia, CSIRT NASK i CSIRT GOV?

Informacje dotyczące zagrożeń dla systemów informacyjnych, w tym dla sektora ochrony zdrowia, są przekazywane na bieżąco w ramach stałej koordynacji oraz wymiany informacji w Połączonym Centrum Operacyjnym Cyberbezpieczeństwa (PCOC). Kanał ten zapewnia sprawny przepływ informacji o zagrożeniach, incydentach, podatnościach i identyfikowanych ryzykach pomiędzy właściwymi instytucjami, w tym Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa, zespołami CSIRT poziomu krajowego i CSIRT-ami sektorowymi, służbami oraz właściwymi resortami.

Ad 6) Czy przed atakiem na MyDr organy państwa posiadały informacje wskazujące na niewystarczający poziom zabezpieczeń systemów dostawców oprogramowania dla placówek medycznych? Jeżeli tak - kiedy informacje te wpłynęły, do jakich instytucji zostały skierowane i jakie działania podjęto?

Rosnący poziom zagrożeń w cyberprzestrzeni sprawia, że wszystkie sektory narażone są na cyberataki. W związku z identyfikowanymi ryzykami oraz koniecznością podniesienia poziomu cyberbezpieczeństwa we wszystkich sektorach doprowadzono do uchwalenia nowelizacji ustawy o KSC. Nowe przepisy wprowadzają kompleksowe, poszerzone wymogi techniczne i organizacyjne (określone m.in. w art. 8 ustawy o KSC) dla 18 sektorów – obejmując docelowo ponad 100 tysięcy podmiotów – oraz nakładają na podmioty kluczowe i podmioty ważne obowiązek zagwarantowania bezpiecznego łańcucha dostaw (a wiec pośrednio wymogi cyberbezpieczeństwa obejmują też podmioty nie wchodzące w skład KSC).

Ad 7) Dlaczego podmiot obsługujący systemy wykorzystywane przez ponad 12 tys. placówek i przechowujący dane niemal połowy mieszkańców Polski mógł funkcjonować w sytuacji, w której - jak wynika z odpowiedzi Ministerstwa Cyfryzacji - resort nie posiadał kompetencji do przeprowadzenia kontroli lub audytu jego cyberbezpieczeństwa?

Na podstawie powszechnie obowiązującego prawa oraz zawartych umów między dostawcą oprogramowania i klientami. W dotychczasowym stanie prawnym Ministerstwo Cyfryzacji nie posiadało podstaw prawnych do przeprowadzania bezpośrednich kontroli, audytów czy testów penetracyjnych w takich przypadkach.

W zakresie ochrony danych osobowych uprawnienie do przeprowadzenia kontroli posiada Prezes Urzędu Ochrony Danych Osobowych.

W zakresie cyberbezpieczeństwa przepisy ustawy o KSC, które obowiązywały w latach 2018-2026 nie dawały podstaw do kontroli tego rodzaju podmiotów, gdyż nie klasyfikowały się one jako podmioty KSC. Dopiero nowelizacja ustawy o KSC, która weszła w życie w kwietniu 2026 r. daje szersze możliwości kontroli i nadzoru oraz w odniesieniu do znacznie większej liczby podmiotów, gdyż rozszerzono liczbę objętych

ustawą sektorów, jak również z uwagi na przyjęte kryteria, liczba podmiotów KSC wzrosła z kilkuset do obecnie ponad 60 tys. podmiotów. Przy czym należ zwrócić uwagę na ww. okresy przejściowe oraz określony w ustawie termin na identyfikację i rejestrację w Wykazie KSC, który upłynął 3 października 2026 r.

Ad 8) Kiedy Rząd zidentyfikował tę lukę kompetencyjną i dlaczego nie została ona wcześniej usunięta? Kto personalnie odpowiadał za przygotowanie zmian prawnych w tym zakresie?

W celu kompleksowego uszczelnienia przepisów z zakresu cyberbezpieczeństwa oraz objęcia kompleksowymi poszerzonymi wymogami szerszego kręgu podmiotów Ministerstwo Cyfryzacji przygotowało nowelizację ustawy o KSC. Z uwagi na skomplikowany i wieloobszarowy charakter regulacji i złożony proces legislacyjny, nowelizacja ustawy o KSC została uchwalona 23 stycznia 2026 r., a weszła w życie 3 kwietnia 2026 r.

Ad 9) Jakie konkretne działania systemowe podjęto przed atakiem na MyDr w celu podniesienia cyberbezpieczeństwa prywatnych dostawców oprogramowania medycznego i ile podmiotów faktycznie zostało nimi objętych?

Przed wystąpieniem incydentu w firmie MyDr podejmowano szereg działań systemowych i legislacyjnych, w tym uchwalono nowelizację ustawy o KSC, dzięki której wprowadzono m.in. podwyższone wymogi cyberbezpieczeństwa (art. 8), obowiązek audytów (art. 15) podmiotów z 18 sektorów.

Równolegle wydawano rekomendacje i komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz prowadzono cykliczne szkolenia[3] i ćwiczenia (np. KSC-EXE).

Ad 10) Jakie działania zostały podjęte po incydencie MyDr i dlaczego - pomimo jego bezprecedensowej skali - w kolejnych tygodniach ujawniane były następne poważne incydenty dotyczące systemów przechowujących dane pacjentów?

Incydenty w firmie MyDr i u innych dostawców oprogramowania dla sektora ochrony zdrowia były przedmiotem prac Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), w ramach którego koordynowana działania instytucji państwa. Ponadto, w ramach realizacji zadań Pełnomocnika Rządu ds. Cyberbezpieczeństwa Ministerstwo Cyfryzacji na bieżąco koordynowało działania w ramach kanału komunikacji PCOC oraz w innych roboczych dwu- lub wielostronnych kontaktach pomiędzy właściwymi instytucjami.

Zespół CSIRT NASK realizował zadania w zakresie koordynacji obsługi incydentu (zgodnie ze swoimi zadaniami określonymi w art. 26 ustawy o KSC) zarówno w przypadku incydentu w firmie MyDr jak i u innych dostawców oprogramowania medycznego, którzy zgłosili incydent.

Natomiast wsparcie sektorowe zapewniał CSIRT CeZ. Warto podkreślić znaczenie jednego z działań CSIRT CeZ, które pomaga podnieść poziom cyberbezpieczeństwa u innych dostawców oprogramowania dla sektora ochrony zdrowia, tj. opracowanie zaleceń bezpieczeństwa dla dostawców rozwiązań IT dla ochrony zdrowia. Zalecenia obejmują m.in. obszary zarządzania bezpieczeństwem, ochrony danych, architektury systemów, zarządzania dostępami oraz monitorowania i reagowania na incydenty. Materiał został rozpowszechniony za pośrednictwem organizacji zrzeszających dostawców i producentów oprogramowania[4].

[3] https://www.gov.pl/web/baza-wiedzy/szkolenia
[4] https://www.cez.gov.pl/pl/page/o-nas/aktualnosci/tylko-do-wrzesnia-2026-roku-wykryto-blisko-1400-incydentow-rosnie

Równolegle czynności dochodzeniowo-śledcze prowadzi Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) pod nadzorem Prokuratury, a Urząd Ochrony Danych Osobowych (UODO) prowadzi działania kontrolne w zakresie ochrony danych.

Ad 11) Czy Rząd zamierza wprowadzić obowiązkowe audyty bezpieczeństwa, testy penetracyjne, minimalne standardy szyfrowania, segmentacji infrastruktury, uwierzytelniania wieloskładnikowego, wykonywania kopii bezpieczeństwa oraz zarządzania podatnościami dla podmiotów przechowujących dane medyczne na dużą skalę?

Wprowadzenie wymogów dotyczących m.in. audytów oraz standardów cyberbezpieczeństwa zostało uregulowane odpowiednio w art. 15 i art. 8 znowelizowanej ustawy o KSC.

Na podstawie art. 42 ustawy o KSC, organy właściwe do spraw cyberbezpieczeństwa posiadają kompetencje do sprawowania nadzoru, prowadzenia kontroli oraz weryfikacji faktycznego stosowania zabezpieczeń przez podmioty KSC.

Ad 12) Czy zostanie utworzony rejestr kluczowych dostawców oprogramowania dla ochrony zdrowia, których kompromitacja może prowadzić do naruszenia danych setek tysięcy lub milionów pacjentów, oraz mechanizm ich regularnego audytowania?

Znowelizowana ustawa o KSC wprowadziła „Wykaz podmiotów kluczowych i podmiotów Ważnych" (Wykaz KSC) – art. 7-7m, prowadzony w systemie teleinformatycznym S46, o którym mowa w art. 46 ustawy o KSC.

Ad 13) Czy po serii opisanych incydentów Pan Premier przeprowadził ocenę działań Pełnomocnika Rządu do spraw Cyberbezpieczeństwa i Ministerstwa Cyfryzacji? Jeśli tak - jakie są jej wyniki i czy stwierdzono błędy, zaniechania lub niewystarczające działania?

Ministerstwo Cyfryzacji oraz Pełnomocnik Rządu do spraw Cyberbezpieczeństwa wykorzystują wszystkie przewidziane prawem instrumenty w sposób możliwie najbardziej efektywny. Bieżące reagowanie na zagrożenia oraz sprawny przepływ informacji realizowane są poprzez stały kanał wymiany informacji w ramach PCOC, natomiast zespoły CSIRT poziomu krajowego realizują zadania dotyczące m.in. koordynacji obsługi incydentów w oparciu o art. 26 ustawy o KSC.

Dążąc do systemowego podniesienia poziomu cyberbezpieczeństwa w Polsce, uchwalono nowelizację ustawy o KSC, która weszła w życie w kwietniu 2026 r. i wprowadziła podwyższone wymagania w zakresie cyberbezpieczeństwa. Jednocześnie obowiązujące obecnie ustawowe okresy dostosowawcze sprawiają, że pełny wachlarz instrumentów i uprawnień przewidzianych nowymi przepisami uzyska pełną skuteczność po ich zakończeniu.

Ad 14) Kto na poziomie politycznym ponosi odpowiedzialność za skuteczność systemu ochrony danych i cyberbezpieczeństwa w sytuacji, gdy kolejne podmioty posiadające dane milionów Polaków okazują się podatne na skuteczne ataki?

Zasady ochrony danych osobowych oraz obowiązki administratorów i podmiotów przetwarzających wynikają bezpośrednio z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), które ustanawia jednolite standardy ochrony danych osobowych obowiązujące w całej Unii Europejskiej. Zgodnie z art. 24 i 32 RODO za zgodność przetwarzania danych osobowych z jego przepisami, w tym zapewnienie odpowiedniego poziomu bezpieczeństwa, odpowiadają poszczególni administratorzy, a określone obowiązki w tym zakresie spoczywają również na podmiotach przetwarzających. RODO przewiduje także, że nadzór nad przestrzeganiem jego przepisów sprawują niezależne organy nadzorcze wyznaczone w poszczególnych

państwach członkowskich. W Polsce organem tym jest Prezes Urzędu Ochrony Danych Osobowych. Minister Cyfryzacji nie jest organem nadzorczym w rozumieniu RODO i zgodnie z zasadą legalizmu wyrażoną w art. 7 Konstytucji RP nie może zastępować niezależnego Prezesa UODO w wykonywaniu jego kompetencji nadzorczych, również w przypadku naruszeń ochrony danych osobowych o znacznej skali.

Ad 15) Czy w świetle skali ujawnionych incydentów Pan Premier nadal uważa, że obecny model zarządzania cyberbezpieczeństwem państwa oraz działania Pełnomocnika Rządu do spraw Cyberbezpieczeństwa są skuteczne?

Ministerstwo Cyfryzacji oraz Pełnomocnik Rządu do spraw Cyberbezpieczeństwa konsekwentnie realizują zadania związane z zapewnieniem skutecznego systemu cyberbezpieczeństwa państwa w oparciu o obowiązujące ramy prawne. Odpowiedzią na rosnącą skalę oraz dynamikę zagrożeń w cyberprzestrzeni było uchwalenie nowelizacji ustawy o KSC, która wprowadziła kompleksowe rozwiązania i podwyższone standardy ochrony. Należy jednak zaznaczyć, że w toku prac parlamentarnych – m.in. w wyniku poprawek przyjętych w Sejmie – do ustawy wprowadzono okresy dostosowawcze dla podmiotów objętych nowymi obowiązkami. W konsekwencji pełny wachlarz instrumentów prawnych, zarządczych i kontrolnych przewidzianych w znowelizowanych przepisach da rządowi pełne narzędzia do skutecznego egzekwowania bezpieczeństwa cyfrowego po zakończeniu tych okresów przejściowych.

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

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa