



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.178.2026
Warszawa, 16 września 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 1 września br. Pośla na Sejm RP Pana Dariusza Piontkowskiego w sprawie bezpieczeństwa danych osobowych i zabezpieczenia systemów masowo przetwarzających dane obywateli (interpelacja nr 19493)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

Ad 1) Czy Ministerstwo Cyfryzacji przeprowadziło analizę ryzyka wystąpienia podobnych masowych wycieków danych w innych podmiotach działających na terenie Polski?

Ad 2) Czy Ministerstwo posiada informacje o innych systemach, w których przechowywane są dane milionów Polaków, a których zabezpieczenia mogą stanowić potencjalny cel cyberataków?

Ad 3) Czy przeprowadzane są dodatkowe kontrole lub audyty bezpieczeństwa systemów podmiotów, które przetwarzają dane osobowe na masową skalę?

Ad 4) Czy Ministerstwo planuje wprowadzenie dodatkowych wymogów dotyczących szyfrowania, przechowywania, dostępu i wykonywania kopii zapasowych danych szczególnie wrażliwych?

Ad 7) Czy Ministerstwo jest obecnie w stanie zagwarantować, że podobny wyciek danych na masową skalę nie dotyczy innych systemów wykorzystywanych przez administrację publiczną lub podmioty realizujące zadania publiczne?

Ad 9) Czy Ministerstwo planuje stworzenie jednolitego systemu monitorowania bezpieczeństwa podmiotów, które przetwarzają dane szczególnie wrażliwe na masową skalę?

Ad 10) Czy w związku z ostatnim incydentem Ministerstwo przygotowało lub przygotowuje pakiet zmian prawnych zwiększających bezpieczeństwo danych obywateli? Jeżeli tak, jakie rozwiązania mają zostać wprowadzone i w jakim terminie.

Odpowiadając na powyższe pytania należy wskazać, że obowiązki podmiotów prawnych w zakresie zapewnienia cyberbezpieczeństwa utrzymywanych przez nich systemów informacyjnych określa ustawa o krajowym systemie cyberbezpieczeństwa¹, której istotna nowelizacja weszła w życie 3 kwietnia 2026 r.

Nowelizacja ta wprowadziła podwyższone i mające zastosowanie do znacznie szerszego kręgu podmiotów (docelowo nawet ponad 100 tys. podmiotów w 18 sektorach) wymogi cyberbezpieczeństwa.

Podmioty objęte ustawą zobowiązane są do rejestracji w Wykazie Podmiotów Kluczowych i Podmiotów Ważnych (Wykaz KSC) w terminie do 3 października 2026 r. Zgodnie z art. 7 ust. 1 ustawy o KSC Wykaz jest prowadzony w celu:

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

- 1) identyfikacji podmiotów kluczowych i podmiotów ważnych;
- 2) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi i podmiotami ważnymi a CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa;
- 3) umożliwienia prowadzenia czynności nadzorczych nad podmiotami kluczowymi i podmiotami ważnymi.

Informacje ujęte w Wykazie określone są w art. 7 ust. 2 ustawy o KSC.

Wyzkaz jest prowadzony w systemie zarządzania cyberbezpieczeństwem S46, o którym mowa w art. 46 ustawy o KSC. System S46 wspiera m.in.:

- 1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
- 2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
- 3) zgłaszanie i obsługę incydentów;
- 4) szacowanie ryzyka na poziomie krajowym;
- 5) ostrzeganie o cyberzagrożeniach;
- 6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;
- 7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych.

Podmioty KSC, zgodnie z nowymi przepisami, szczególnie określonymi w art. 8, obowiązane są do wdrożenia wymagań z zakresu cyberbezpieczeństwa, w tym w szczególności do wdrożenia systemu zarządzania bezpieczeństwem informacji, który ma zapewniać m.in. prowadzenie systematycznego szacowania ryzyka wystąpienia incyduentu, wdrożenie polityki szacowania ryzyka, wdrożenie polityki kontroli dostępu, bezpieczeństwo fizyczne i środowiskowe, bezpieczeństwo zasobów ludzkich, bezpieczeństwo i ciągłość łańcucha dostaw, edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, plany awaryjne i plany odtworzeniowe. Konieczne jest także stosowanie bezpiecznych środków komunikacji elektronicznej uwzględniających uwierzytelnianie wieloskładnikowe.

Podkreślić należy, że nawet jeśli niektóre podmioty nie zostaną zakwalifikowane jako podmioty kluczowe lub podmioty ważne, a współpracują z tymi podmiotami, w szczególności występują w ich łańcuchu dostaw np. w obszarze połączeń i zależności systemów czy usług, to one również powinny zostać objęte wymaganiami z zakresu cyberbezpieczeństwa. Wynika to z tego, że na podmiotach kluczowych i podmiotach ważnych spoczywa obowiązek zapewnienia bezpiecznego łańcucha dostaw.

Ustawa to określiła także wymogi w zakresie audytów bezpieczeństwa systemu informacyjnego (art. 15), które zobowiązane są przeprowadzać podmioty KSC, a jak również uprawnienia nadzorcze i kontrole organów właściwych do spraw cyberbezpieczeństwa w poszczególnych sektorach (art. 41-42).

W kontekście tych wymogów należy zwrócić uwagę 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.

Jednocześnie Ministerstwo Cyfryzacji analizuje potencjalne uzupełnienie przepisów dotyczących cyberbezpieczeństwa i ochrony danych osobowych. 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 5) Czy Ministerstwo posiada dane dotyczące liczby poważnych incydentów cyberbezpieczeństwa dotyczących wycieku danych osobowych w latach 2024–2026?

Incydenty cyberbezpieczeństwa zgłaszane są do właściwych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSRIT). Statystyki w zakresie tych incydentów dostępne są w publicznych Sprawozdaniach Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Jednocześnie należy wyjaśnić, że ustawa o KSC nie rozróżnia incydentu dotyczącego danych osobowych.

Naruszenia dotyczące ochrony danych osobowych zgłaszane są zgodnie z unijnym rozporządzeniem 2016/679 (RODO) oraz ustawą o ochronie danych osobowych² - zgodnie z tą ustawą organem właściwym w sprawie ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (art. 34 ust. 1). Należy wyjaśnić, że Prezes UODO nie jest organem administracji rządowej podległym Radzie Ministrów, lecz niezależnym organem nadzorczym, wobec czego Minister Cyfryzacji nie posiada informacji na temat naruszeń zgłaszanych Prezesowi UODO. Statystyki dotyczące naruszeń danych osobowych udostępnione są w sprawozdaniach z działalności Prezesa UODO³. W 2024 r. liczba zgłoszeń naruszeń to 14 842, a w 2025 r. to 22 435. Dane z 2026 r. nie są jeszcze dostępne.

Ad 6) Jakie działania podejmowane są w celu zapewnienia, aby podmioty objęte nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa faktycznie wdrożyły wymagane zabezpieczenia, a nie ograniczały się do formalnego spełnienia obowiązków?

W celu zapewnienia, że podmioty objęte nowelizacją ustawy KSC wdrażają wymagane środki bezpieczeństwa w sposób rzeczywisty i efektywny, a nie wyłącznie w celu formalnego spełnienia obowiązków regulacyjnych, podejmowane są działania ukierunkowane na rozwój kompetencji, wymianę doświadczeń oraz praktyczną weryfikację zdolności organizacyjnych i operacyjnych.

W szczególności w ramach przedsięwzięć realizowanych w Programie Współpracy w Cyberbezpieczeństwie (PWCyber) prowadzone są specjalistyczne szkolenia skierowane do podmiotów krajowego systemu cyberbezpieczeństwa. Szkolenia prowadzą firmy technologiczne będące partnerami PWCyber, które dzielą się specjalistyczną wiedzą oraz najlepszymi praktykami stosowanymi w obszarze cyberbezpieczeństwa. Ich celem jest nie tylko przekazanie wiedzy na temat obowiązków wynikających z przepisów prawa, ale przede wszystkim rozwijanie umiejętności praktycznego wdrażania środków organizacyjnych i technicznych, zarządzania ryzykiem, reagowania na incydenty oraz budowania kultury cyberbezpieczeństwa w organizacjach.

Uzupełnieniem działań szkoleniowych są krajowe ćwiczenia cyberbezpieczeństwa KSC-EXE, które umożliwiają praktyczną weryfikację przygotowania organizacji do reagowania na incydenty oraz realizacji obowiązków wynikających z przepisów. Ćwiczenia prowadzone są w oparciu o realistyczne scenariusze zdarzeń i umożliwiają ocenę skuteczności funkcjonujących procedur, procesów decyzyjnych, mechanizmów komunikacji kryzysowej oraz współpracy z właściwymi CSIRT poziomu krajowego. Dzięki temu możliwe jest identyfikowanie obszarów wymagających poprawy oraz doskonalenie zdolności organizacyjnych i technicznych jeszcze przed wystąpieniem realnych zagrożeń.

Takie podejście, łączące podnoszenie kompetencji z praktycznym testowaniem zdolności operacyjnych, zwiększa prawdopodobieństwo rzeczywistego wdrożenia wymaganych

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 z późn. zm.)

³ <https://uodo.gov.pl/pl/487/2279>

środków bezpieczeństwa oraz wspiera budowanie trwałej odporności na zagrożenia podmiotów objętych regulacjami krajowego systemu cyberbezpieczeństwa.

Ponadto prowadzone są działania pod nazwą „KSCedu”, które mają na celu przygotowanie i realizację działań informacyjno-szkoleniowych oraz opracowanie materiałów edukacyjnych w zakresie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa na rzecz zwiększenia gotowości podmiotów krajowego systemu cyberbezpieczeństwa do wdrożenia wymogów ustawy. Zadanie realizowane w terminie od dnia 1 czerwca 2026 r. do dnia 31 grudnia 2027 r. Obejmuje działania informacyjne, opracowanie materiałów edukacyjnych oraz organizację i przeprowadzenie specjalistycznych szkoleń, ukierunkowanych na przygotowanie podmiotów krajowego systemu cyberbezpieczeństwa do wdrożenia wymogów wynikających z nowelizacji ustawy, która obowiązuje od kwietnia 2026 r.

Ministerstwo Cyfryzacji prowadzi także szereg innych działań informacyjnych i wspierających. Obejmują one publikowanie komunikatów i materiałów wyjaśniających zagadnienia związane z ustawą o krajowym systemie cyberbezpieczeństwa. Poza tym na bieżąco publikowane są komunikaty i informacje dotyczące wymagań i terminów, którymi objęte są podmioty kluczowe oraz podmioty ważne. Komunikaty można znaleźć w sekcji aktualności [Ministerstwa Cyfryzacji](#). Warto zwrócić uwagę w szczególności na ostatnie komunikaty⁴.

Poza komunikatami Ministerstwo Cyfryzacji przygotowało zbiór najczęściej zadawanych pytań w raz z odpowiedziami, które wspomagają podmioty objęte ustawą w samoidentyfikacji, zrozumieniu ustawy KSC i zwróceniu uwagi na pewne kwestie mogące budzić wątpliwości. Sama lista pytań zawiera 14 kategorii, a każda z nich jest szczegółowo rozbudowana, dodatkowo dla wygody podmiotów znajdują się też wyszukiwarka przyspieszająca wyszukanie potrzebnych im informacji. Kategorię dotyczą tematów takich jak: identyfikacja podmiotów kluczowych i podmiotów ważnych, wykaz podmiotów, obowiązki podmiotów, informację na temat CSIRT, zgłaszanie incydentów, System S46, przeprowadzanie audytów, nadzór nad podmiotami, kary pieniężne i wiele więcej. Pełną listę pytań możemy znaleźć pod adresem: [FAQ - Cyber.gov.pl](#). Poza tym Ministerstwo Cyfryzacji wspiera podmioty w procesie samoidentyfikacji odpowiadając na ich pytania, które trafiają drogą mailową. Szczególnie jest to pomocne dla podmiotów, które mają niepewną sytuację, nie posiadają działów prawnych lub ich sytuacja jest specyficzna i wymaga analizy ze strony urzędników.

Należy także zauważyć, że nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa przewiduje mechanizmy zapewniające, aby objęte nią podmioty kluczowe i podmioty ważne rzeczywiście wdrożyły wymagane zabezpieczenia. Organy właściwe do spraw cyberbezpieczeństwa, mogą monitorować wykonywanie obowiązków, prowadzić kontrole, w tym doraźne, żądać dokumentów, informacji oraz dowodów wdrożenia zabezpieczeń, a także zlecać właściwym CSIRT przeprowadzenie ocen bezpieczeństwa systemów informacyjnych, obejmujących testy służące identyfikacji podatności. Weryfikacji faktycznego stosowania zabezpieczeń służą również audyty bezpieczeństwa oraz dokumentacja operacyjna, w tym zapisy i logi potwierdzające wykonywanie wymaganych działań. W przypadku stwierdzenia nieprawidłowości organ może wydać zalecenia pokontrolne, nakazać usunięcie uchybień, zapewnienie zgodności z ustawą lub wdrożenie zaleceń audytowych, a wobec podmiotu kluczowego także wyznaczyć urzędnika monitorującego. Niewykonanie obowiązków może skutkować karami pieniężnymi

⁴ <https://www.gov.pl/web/cyfryzacja/novelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc--organy-wlasciwe-do-spraw-cyberbezpieczenstwa>; <https://www.gov.pl/web/cyfryzacja/miesiac-na-samorejestracje-w-wykazie-ksc-termin-mija-3-pazdziernika>

nakładanymi na podmiot, a w przypadkach określonych w ustawie również na kierownika podmiotu, w tym okresową karą za każdy dzień opóźnienia w wykonaniu decyzji.

Ad 8) Jakie działania państwo podejmuje w celu szybkiego informowania obywateli o wycieku ich danych oraz ograniczenia możliwości wykorzystania tych danych do kradzieży tożsamości, oszustw i wyłudzeń?

Ministerstwo Cyfryzacji, które zleca NASK-PIB prowadzenie serwisu bezpiecznedane.gov.pl, umożliwiło ustalenie obywatelom czy ich dane brały udział w wycieku poprzez ten serwis. 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.

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

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 elektronicznej⁵ (np. lista ostrzeżeń).

W zakresie wsparcia obywateli należy wskazać, że podstawowym kanałem informacji o naruszeniu pozostaje administrator danych, czyli placówka medyczna, na której zgodnie z art. 34 RODO spoczywa obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu powodującym wysokie ryzyko naruszenia jej praw lub wolności. Wyłącznie administrator dysponuje wiedzą o zakresie danych objętych naruszeniem w odniesieniu do konkretnego pacjenta.

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

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

⁵ Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. 2024 poz. 1803)