



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.97.2026
Warszawa, 29 czerwca 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 21 maja br. Posłów na Sejm RP Panów Łukasza Osmalaka, Adama Gomoły, Pań Bożenny Hołowni, Ewy Schädler, Pana Piotra Pawła Stracha, Pani Wiolety Tomczak oraz Pana Kamila Wnuka w sprawie włączenia pracowników jednostek samorządu terytorialnego do systemu świadczeń teleinformatycznych przewidzianych w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (interpelacja nr 17187)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytania.

Ad 1) Czy Ministerstwo Cyfryzacji dostrzega zagrożenie wynikające z odpływu kadr ds. cyberbezpieczeństwa z jednostek samorządu terytorialnego do sektora prywatnego oraz innych instytucji publicznych objętych dodatkami?

Ministerstwo Cyfryzacji monitoruje cyberzagrożenia w jednostkach samorządu terytorialnego oraz dostrzega trudności, z którymi mierzą się samorządy, w szczególności w obszarze zasobów finansowych i kadrowych. Deficyt wykwalifikowanych ekspertów z zakresu cyberbezpieczeństwa jest problemem występującym zarówno na poziomie krajowym, jak i w skali całej Unii Europejskiej. Niedobór wykwalifikowanych kadr stanowi istotne wyzwanie dla funkcjonowania administracji rządowej oraz administracji samorządowej.

Prowadzimy również rozmowy z przedstawicielami administracji samorządowej w ramach realizowanych inicjatyw, jak obecnie realizowanych spotkań z samorządami w ramach „Cyfrowego Samorządu”, podczas których prezentujemy rozwiązania wspierające cyfryzację oraz cyberbezpieczeństwo samorządów, czy w ramach spotkań z Komisją Wspólną Rządu i Samorządu Terytorialnego, m.in. w procesie prac legislacyjnych.

Należy w tym miejscu przypomnieć, że z uwagi na zidentyfikowane potrzeby samorządów dot. wzmacniania cyberodporności podmiotów oraz rozwijania kompetencji, Ministerstwo Cyfryzacji uruchomiło konkursy grantowe pn. „Cyberbezpieczny Samorząd” oraz „Cyberbezpieczne Wodociągi”, w ramach których do jednostek samorządu terytorialnego w latach 2024-2026 przekazywane są środki finansowe na ww. cele.

Konkurs grantowy pn. „**Cyberbezpieczny Samorząd**” to projekt współfinansowany ze środków UE oraz budżetu państwa, w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Łączna kwota grantów w tym projekcie wynosi ok. 1,5 mld zł, z czego do dnia 5 czerwca 2026 r., samorządom wypłacono już ponad 1 440 mln zł na budowanie odporności na cyberzagrożenia w obszarach organizacji, technicznym i kompetencyjnym.

Z kolei konkurs grantowy „**Cyberbezpieczne Wodociągi**”, to projekt współfinansowany ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO). Nabór wniosków o granty w ramach niniejszego konkursu został uruchomiony w dniu 1 września 2025 r. i zakończył się 2 października 2025 r. W jego wyniku 759 wnioskodawców, których wnioski

zostały pozytywnie zaopiniowane otrzyma wsparcie o łącznej wartości ponad 624 mln zł. Celem tego przedsięwzięcia jest wzmocnienie cyberodporności przedsiębiorstw działających w sektorze zbiorowego zaopatrzenia w wodę, w szczególności poprzez: modernizację systemów IT/OT, audyty bezpieczeństwa oraz szkolenia pracowników. Przedsięwzięcie to pozwoli wzmocnić ochronę infrastruktury wodociągowej przed cyberatakami, zapewniając ciągłość dostaw wody poprzez wsparcie we wdrażaniu środków organizacyjnych i technicznych oraz rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

Ponadto, w celu ograniczania skutków deficytu specjalistów z obszaru cyberbezpieczeństwa w jednostkach samorządu terytorialnego jeszcze w tym roku planowane jest uruchomienie projektu pn. „Lokalne Centra Cyberbezpieczeństwa (LCC)”. LCC będą realizowane w formie zbliżonej do Centrów Usług Wspólnych w obszarze IT. Dofinansowanie skierowane będzie do samorządów, które dzięki połączeniu sił będą wspólnie realizować zadania z obszaru cyberbezpieczeństwa dla wielu instytucji działających na poziomie samorządu terytorialnego. Na realizację tego projektu Ministerstwo Cyfryzacji planuje przeznaczyć kwotę ok. 270 mln zł. Projekt będzie współfinansowany ze środków UE oraz budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Planowany termin ogłoszenia naboru wniosków o wsparcie to przełom II i III kwartału 2026 r.

Planowane jest również kolejne wsparcie finansowe z Funduszu Bezpieczeństwa i Odporności adresowane do samorządów, w ramach którego ok. 2,46 mld zł w formie preferencyjnych pożyczek przeznaczone zostanie na zwiększenie poziomu bezpieczeństwa i niezawodności infrastruktury cyfrowej, w tym usług publicznych realizowanych przez JST¹.

Ad 2) Jak Ministerstwo uzasadnia fakt, że ustawa o KSC nakłada na samorządy obowiązki równe administracji rządowej, podczas gdy ustawa o szczególnych zasadach wynagradzania odmawia im analogicznego wsparcia finansowego?

Na wstępie należy zauważyć, że obowiązki wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa nie stanowią całkowicie nowych wymagań dla podmiotów publicznych. W istotnym zakresie rozwijają i uszczegóławiają ustanowione w 2012 r. obowiązki wynikające z ówczesnego §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych². Obowiązki te zostały powtórzone w nadal obowiązującym §19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych³. Zgodnie z tymi przepisami podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Ponadto nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa nie nakłada takich samych obowiązków na wszystkie podmioty publiczne, a różnicuje te obowiązki mając na uwadze specyfikę danej instytucji publicznej. Nie można zatem zgodzić się z tezą, że obowiązki te są równe. W przypadku administracji samorządowej inne obowiązki mają

¹ <https://funduszeuropejskie.gov.pl/aktualnosci/mfipr-i-bgk-uruchamiaja-inwestycje-w-bezpieczenstwo-i-obronnosc/>

² Dz.U. z 2017 r. poz. 2247

³ Dz. U. poz. 773

urzędy gminy zatrudniające co najmniej 50 osób, a inne obowiązki mają urzędy gminy, w których zatrudnienie jest mniejsze, jak również samorządowe jednostki budżetowe, samorządowe zakłady budżetowe, samorządowe instytucje kultury oraz spółki komunalne, dla których ustawodawca – wspólnie ze stroną samorządową – przygotował uproszczoną listę obowiązków, która stanowi odrębny załącznik do ustawy, tj. załącznik nr 4.

Ad 3) Czy zostaną podjęte pilne prace legislacyjne mające na celu nowelizację art. 5 przedmiotowej ustawy, aby umożliwić dopłacanie do wynagrodzeń kluczowych specjalistów cyberbezpieczeństwa w samorządach ze środków Funduszu Cyberbezpieczeństwa?

Ministerstwo Cyfryzacji prowadzi działania mające na celu zwiększenie przychodów Funduszu, co w przyszłości mogłoby stworzyć warunki do objęcia wsparciem szerszego katalogu beneficjentów.

Ministerstwo Cyfryzacji zachęca jednocześnie jednostki samorządu terytorialnego do aktywnego uczestnictwa w realizowanych przez Ministerstwo projektach tych finansowych, jak i pozafinansowych jak: szkolenia, udostępnianie narzędzi wspomagających realizację obowiązków z obszaru cyberbezpieczeństwa, które stanowią istotne wsparcie i umożliwiają pozyskanie wiedzy oraz kompetencji niezbędnych do skutecznego wykonywania zadań z zakresu cyberbezpieczeństwa.

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

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych