UCHWAŁA NR RG-XXVII/280/26
RADY GMINY NOWINY

z dnia 29 kwietnia 2026 r.

w sprawie załatwienia skargi na kierownika jednostki samorządu terytorialnego

Na podstawie art. 18 ust. 2 pkt. 15 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153 ze zm.), w związku z art. 229 pkt 3, art. 237 oraz art. 238 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego" (Dz. U. z 2025 r. poz. 1691), Rada Gminy Nowiny, po zapoznaniu się z wynikami badania skargi przeprowadzonego przez Komisję Skarg,Wniosków i Petycji Rady Gminy Nowiny, uchwala co następuje.

§ 1. Po rozpatrzeniu skargi złożonej przez Prezesa Zarządu firmy Szulc–Euphenics.com.p. S.A., na kierownika jednostki samorządu terytorialnego – Wójta Gminy Nowiny w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów, postanawia się uznać skargę za bezzasadną, z przyczyn określonych w uzasadnieniu niniejszej uchwały.

§ 2. 1. Niniejszą uchwałę wraz z uzasadnieniem przekazuje się osobie skarżącej tytułem zawiadomienia o sposobie załatwienia skargi.

2. Zobowiązuje się Przewodniczącego Rady Gminy Nowiny do powiadomienia osoby skarżącej o sposobie załatwienia skargi, z jednoczesnym upoważnieniem do zawiadomienia o treści niniejszej uchwały wraz z uzasadnieniem oraz pouczeniem o treści art. 239 Kodeksu postępowania administracyjnego.

§ 3. Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Rady Gminy

Marcin Wojcieszyński

Uzasadnienie

Do Rady Gminy w dniu 25 marca 2026 r za pomocą poczty e-mail została złożona skarga przez Prezesa Zarządu firmy Szulc–Euphenics.com.p. S.A., na kierownika jednostki samorządu terytorialnego– Wójta Gminy Nowiny w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów.

Skarga ta, zgodnie ze Statutem Gminy Nowiny (Dz. Urz. Woj. Św. z 2024 r. poz. 559,) została przekazana do Komisji Skarg, Wniosków i Petycji, celem jej rozpoznania i przygotowania stosownego projektu uchwały celem przedłożenia Radzie Gminy do jej załatwienia.

Komisja Skarg, Wniosków i Petycji na swoim posiedzeniu w dniu 10 kwietnia 2026 r. przeprowadziła analizę skargi.

W wyniku badania skargi ustalono co następuje.

Skarżący sformułował cztery zarzuty:

"Zarzut - 1.1) Jednostki organizacyjne nadzorowane przez Kierownika Jednostki nie posiadają zdefiniowanych i tworzonych kopii zapasowych w nawiązaniu do normy PN27001 oraz Rozporządzenia KRI-2024 (Dz. U. z 22 maja 2024 r.)

Wynika to z analizy stanu faktycznego - oraz odpowiedzi uzyskanych na nasze wnioski w trybie ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902, etc, etc)".

W odniesieniu do zarzutu – 1.1)

Odwołanie do normy ISO/IEC 27001:

Norma ISO 27001 (PN-EN ISO/IEC 27001) nie jest co do zasady obowiązkowa, ale jest powszechnie uznanym standardem należytej staranności.

Nie można zarzucić „naruszenia ISO 27001” jako prawa, można użyć jej jako benchmarku (wzorca dobrych praktyk). ISO 27001 to tylko punkt odniesienia, nie obowiązek prawny.

Rozporządzenie KRI faktycznie jest aktem obowiązującym jednostki publiczne i nakłada obowiązki w zakresie bezpieczeństwa informacji.

W praktyce obejmuje m.in.:

- zapewnienie bezpieczeństwa danych,

- stosowanie środków organizacyjnych i technicznych,

- zarządzanie ciągłością działania.

Choć nie zawsze literalnie mówi „musisz robić backup codziennie”, to: brak kopii zapasowych może być uznany za naruszenie obowiązku zapewnienia bezpieczeństwa i dostępności danych.

Zarzut dot. stwierdzenia, iż „Jednostki organizacyjne nadzorowane przez Kierownika Jednostki nie posiadają zdefiniowanych i tworzonych kopii zapasowych” jest niezasadny, nie poparty żadnymi dowodami. Jest to teza strony skarżącej, a nie ustalenie.

W Urzędzie funkcjonuje System Zarządzania Bezpieczeństwem Informacji (SZBI), w ramach którego:

·stosowane są mechanizmy zabezpieczenia danych przed utratą,

·wykonywane są kopie zapasowe,

·zapewniona jest możliwość odtworzenia danych.

Twierdzenia Skarżącego wynikają z błędnej interpretacji odpowiedzi udzielonych w trybie dostępu do informacji publicznej, które mają charakter zakresowy i nie odzwierciedlają całości funkcjonujących rozwiązań.

Ponadto należy wskazać, że:

·przepisy Rozporządzenie w sprawie Krajowych Ram Interoperacyjności wymagają zapewnienia bezpieczeństwa danych,

·nie narzucają jednak jednej, konkretnej formy realizacji kopii zapasowych.

Organ realizuje wymagania w sposób adekwatny i proporcjonalny do skali działania oraz zidentyfikowanych ryzyk.

"Zarzut 1.2) Naruszenie obowiązku nałożonego na Kierownika Jednostki w zakresie - art. 8 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222).(dalej KSC)".

W odniesieniu do zarzutu – 1.2)

Obowiązki wynikające z - art. 8 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa były realnie wykonywane. Została wprowadzona dokumentacja systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy opisująca w szczególności środki techniczne i organizacyjne wdrożone w celu zminimalizowania ryzyka naruszenia praw i wolności osób fizycznych, których dane przetwarzane są w Urzędzie.

Dokumentacja systemu zarządzania bezpieczeństwem informacji obejmuje Politykę bezpieczeństwa informacji oraz związaną z nią dokumentację bezpieczeństwa na którą składają się:

- Polityka Ochrony Danych Osobowych,

- Polityka Zarządzania Ciągłością Działania,

- Polityka Zarządzania Incydentami Cyberbezpieczeństwa,

- Polityka Zarządzania Systemem Teleinformatycznym.

Zarzut dotyczący rzekomego braku analizy incydentów w innych gminach ma charakter wyłącznie subiektywny i nie znajduje oparcia w obowiązujących przepisach prawa.

W szczególności:

·Ustawa o krajowym systemie cyberbezpieczeństwa,

·Rozporządzenie w sprawie Krajowych Ram Interoperacyjności

nie nakładają na Organ obowiązku systematycznego analizowania incydentów występujących w innych jednostkach samorządu terytorialnego.

Skarżący nie wskazał:

·konkretnych zdarzeń, które miałyby zostać przeanalizowane,

·ani działań, które Organ miałby obowiązek podjąć.

Zarzut stanowi próbę przypisania Organowi obowiązków niewynikających z przepisów prawa oraz utożsamienia dobrych praktyk z obowiązkiem prawnym.

"Zarzut 2)* W mniemaniu Skarżącego **-** Organ podlegający niniejszej skardze - per analogiam jak wiele innych Urzędów - przywiązuje zbyt małą wagę do analizy zaistniałych incydentów związanych z cyberbezpieczeństwem jakie miały miejsce w innych gminach .

Zaistniałe w innych gminach błędy związane z cyberbezpieczeństwem w obszarze Decydentów: Wójt/Burmistrz-Sekretarz-Skarbnik

W naszym mniemaniu taka analiza jest równie ważna jak zakup sprzętu, szkolenia, etc i warto mały ułamek percepcji w obszarze cyberbezpieczeństwa - poświęcić również na analizę tego obszaru".

W odniesieniu do zarzutu – 2)

W odniesieniu do Zarzutu 2, dotyczącego rzekomego „przywiązywania zbyt małej wagi do analizy incydentów cyberbezpieczeństwa w innych gminach”, Organ wskazuje, co następuje:

Zarzut ma charakter wyłącznie subiektywny i nie spełnia podstawowych wymogów zarzutu prawnego.

Zarzut został oparty wyłącznie na przekonaniu Skarżącego („w mniemaniu Skargodawcy”) i nie zawiera żadnych:

·konkretnych ustaleń faktycznych,

·dowodów,

·wskazania zdarzeń, które miałyby podlegać analizie,

·ani wykazania, że Organ zaniechał jakichkolwiek wymaganych działań.

W istocie zarzut ten stanowi opinię o charakterze publicystycznym, a nie zarzut naruszenia prawa lub obowiązku o charakterze administracyjnym.

Skarżący formułuje oczekiwanie, które nie znajduje oparcia w obowiązujących przepisach, w tym w:

- Ustawie o krajowym systemie cyberbezpieczeństwa,

- Rozporządzeniu w sprawie Krajowych Ram Interoperacyjności.

Żaden z powyższych aktów prawnych nie nakłada na kierownika jednostki obowiązku systematycznego analizowania incydentów w innych jednostkach samorządu terytorialnego, jak również prowadzenia odrębnych działań w tym zakresie jako samodzielnego obowiązku.

Próba przypisania Organowi naruszenia obowiązku, który nie istnieje w porządku prawnym, jest nieuprawniona.

Skarżący dokonuje nieuprawnionego rozszerzenia katalogu obowiązków poprzez utożsamienie:

- rekomendowanych działań (np. analiz incydentów zewnętrznych),

- z obowiązkami prawnymi.

Należy podkreślić, że nawet jeśli określone działania mogą być uznane za dobrą praktykę, ich brak nie stanowi naruszenia prawa, o ile Organ realizuje obowiązki wynikające z przepisów.

Organ realizuje obowiązki w zakresie cyberbezpieczeństwa poprzez:

·funkcjonujący w Urzędzie System Zarządzania Bezpieczeństwem Informacji,

·prowadzenie analizy ryzyka,

·stosowanie adekwatnych środków technicznych i organizacyjnych,

·monitorowanie zagrożeń oraz dostosowywanie zabezpieczeń.

W ramach tych działań uwzględniane są również ogólnodostępne informacje o zagrożeniach publikowane przez właściwe podmioty, w tym NASK, co czyni zarzut dodatkowo bezzasadnym.

Skarżący nie wykazał:

·aby brak postulowanych przez niego działań doprowadził do jakiegokolwiek incydentu,

·aby poziom bezpieczeństwa w Urzędzie był niewystarczający,

·ani aby istniało konkretne, zidentyfikowane ryzyko wynikające z rzekomego zaniechania.

Zarzut ma zatem charakter czysto hipotetyczny i nie odnosi się do rzeczywistego stanu bezpieczeństwa.

Skarżący opiera swoją tezę na „analogii do innych urzędów”, co jest metodologicznie i prawnie nieprawidłowe.

Ocena działalności konkretnego organu:

·musi opierać się na jego indywidualnej sytuacji,

·nie może wynikać z uogólnień ani przypuszczeń dotyczących innych podmiotów.

Zarzut 2 należy uznać za całkowicie bezzasadny, gdyż:

·nie wskazuje naruszenia konkretnego przepisu prawa,

·opiera się wyłącznie na subiektywnej opinii Skarżącego,

·próbuje przypisać Organowi obowiązki niewynikające z przepisów,

·nie został poparty żadnymi dowodami ani analizą stanu faktycznego.

W konsekwencji zarzut ten nie może stanowić podstawy do stwierdzenia jakichkolwiek uchybień w działalności Organu.

"Zarzut 3)* w mniemaniu Skarżącego - taki stan faktyczny - biorąc pod uwagę trudną sytuację geopolityczną - narusza zasady uczciwej konkurencji - poprzez inter alia - narażenie danych osób fizycznych oraz przedsiębiorców na kradzież danych".

W odniesieniu do zarzutu – 3)

W odniesieniu do Zarzutu 3, zgodnie z którym rzekomy stan faktyczny miałby „naruszać zasady uczciwej konkurencji poprzez narażenie danych osób fizycznych oraz przedsiębiorców na kradzież danych”, Organ wskazuje, co następuje:

Zarzut jest wewnętrznie niespójny i prawnie nieadekwatny.

Skarżący łączy w jednym zarzucie:

·kwestie bezpieczeństwa informacji,

·z zasadami uczciwej konkurencji,

co stanowi konstrukcję nieuprawnioną i pozbawioną podstaw prawnych.

Zasady uczciwej konkurencji odnoszą się do relacji rynkowych pomiędzy przedsiębiorcami, natomiast Organ jako jednostka samorządu terytorialnego nie działa na rynku w sposób konkurencyjny wobec przedsiębiorców w rozumieniu przepisów prawa konkurencji.

Skarżący nie wskazał:

·żadnego konkretnego incydentu naruszenia danych,

·żadnego przypadku kradzieży danych,

·ani dowodów na istnienie realnego zagrożenia.

Zarzut opiera się wyłącznie na przypuszczeniach oraz ogólnym odwołaniu do „sytuacji geopolitycznej”, co nie stanowi podstawy do formułowania zarzutów wobec konkretnego organu.

Organ realizuje obowiązki w zakresie ochrony danych oraz bezpieczeństwa informacji zgodnie z obowiązującymi przepisami, w tym:

·Rozporządzenie w sprawie Krajowych Ram Interoperacyjności,

·Ustawa o krajowym systemie cyberbezpieczeństwa,

·RODO.

W szczególności stosowane są środki organizacyjne i techniczne mające na celu:

·zapewnienie poufności, integralności i dostępności danych,

·minimalizację ryzyka nieuprawnionego dostępu,

·reagowanie na potencjalne incydenty.

Nie wykazano, aby:

·jakiekolwiek działanie lub zaniechanie Organu,

·mogło prowadzić do naruszenia zasad uczciwej konkurencji,

·ani aby istniał związek pomiędzy funkcjonowaniem systemu bezpieczeństwa w Urzędzie a sytuacją przedsiębiorców na rynku.

Zarzut 3 należy uznać za całkowicie bezzasadny, gdyż:

·opiera się na błędnym zastosowaniu przepisów o uczciwej konkurencji,

·ma charakter hipotetyczny i nie jest poparty dowodami,

·nie wskazuje żadnego rzeczywistego naruszenia,

·nie wykazuje związku przyczynowego pomiędzy działaniem Organu a rzekomymi skutkami.

W konsekwencji zarzut ten nie może stanowić podstawy do stwierdzenia jakichkolwiek uchybień w działalności Organu.

Mając na względzie dokonane przez Komisję Skarg, Wniosków i Petycji ustalenia, które to ustalenia Rada Gminy w pełni podziela i akceptuje, biorąc pod uwagę stan faktyczny, przytoczone przepisy, przedmiotowa skarga nie zasługuje na uwzględnienie.

Wobec powyższego podjęcie niniejszej uchwały, o uznaniu skargi za bezzasadną przez Radę Gminy Nowiny, jest zasadne.

Przewodniczący Rady Gminy

Marcin Wojcieszyński