

Projekt

z dnia 16 kwietnia 2026 r.
Druk Nr 8/04/26

**UCHWAŁA NR
RADY GMINY ORNONTOWICE**

z dnia 2026 r.

w sprawie rozpatrzenia skargi w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów

Na podstawie art. 18b ust. 1 Ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2025r., poz. 1153 z późn. zm.), art. 229 pkt 3 Ustawy z dnia 14 czerwca 1960r. Kodeks Postępowania Administracyjnego (Dz. U. z 2025 r. poz. 1691) oraz § 51 ust. 1 Statutu Gminy Ornontowice stanowiącego załącznik nr 1 do Uchwały Nr LV/460/23 Rady Gminy Ornontowice z dnia 27 kwietnia 2023 r. w sprawie: uchwalenia Statutu Gminy Ornontowice (Dz.Urz. Woj. Śl. z 2023 r. poz. 4105) na wniosek Komisji Skarg, Wniosków i Petycji uchwala się, co następuje:

§ 1. Uznaje się za bezzasadną skargę na Wójta Gminy Ornontowice w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów, która wpłynęła do Rady Gminy Ornontowice drogą mailową w dniu 10 marca 2026 r.

§ 2. Uzasadnienie dla sposobu rozpatrzenia skargi stanowi załącznik do niniejszej uchwały.

§ 3. Upoważnia się Przewodniczącą Rady Gminy Ornontowice do zawiadomienia wnoszącego skargę o sposobie jej załatwienia.

§ 4. Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Rady Gminy

Henryk Nieużyła

Uzasadnienie

W dniu 10.03.2026 r. drogą elektroniczną do Rady Gminy Ornontowice wpłynęło pismo zatytułowane „Skarga do Rady Gminy - w trybie art. 229 Ustawy Kodeks postępowania administracyjnego (t.j. Dz. U. z 2023 r.) w związku z art. 241 KPA”, w którego treści Skarżący zarzucił Wójtowi Gminy Ornontowice brak należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów w kierowanym przez niego Urzędzie Gminy.

W treści obszernego pisma wskazano, że:

- 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.)

- 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)

- W mniemaniu Skargodawcy - 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 .

- W mniemaniu Skargodawcy - 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.

- Firmy szkoleniowe, którym urzędy płacą - w ostatnim czasie setki milionów złotych z pieniędzy Podatników - dzięki programom takim jak „Cyberb. Samorząd.” i wcześniej „Cyf. Gm.” - przekazują jedynie wiedzę modelową, modelowe abstrakcyjne przykłady - niemalże książkowe przykłady cyberincydentów, etc. Reasumując - w opinii - Skargodawcy - niemal we wszystkich Urzędach w tym - u Adresata niniejszej skargi - zbyt małą wagę przywiązuje się do poznania empirycznych aspektów i uwarunkowań związanych z już potwierdzoną praktyką i rzeczywistymi przyczynami skutecznych włamań do Urzędów.

Ponadto w piśmie Skarżący przytoczył wiele przykładów negatywnych zjawisk związanych z cyberbezpieczeństwem na obszarze całej Polski.

Zgodnie z art. 223 § 1 Kodeksu postępowania administracyjnego organy państwowe, organy samorządu terytorialnego i inne organy samorządowe oraz organy organizacji społecznych - rozpatrują oraz załatwiają skargi i wnioski w ramach swojej właściwości. Art. 229 pkt 3 ww. ustawy wskazuje, że jeżeli przepisy szczególne nie określają innych organów właściwych do rozpatrywania skarg, organem właściwym do rozpatrzenia skargi dotyczącej zadań lub działalności wójta, z wyjątkiem spraw określonych w pkt 2, jest rada gminy. Art. 18b ust. 1 ustawy o samorządzie gminnym reguluje, że rada gminy rozpatruje skargi na działania wójta i gminnych jednostek organizacyjnych; wnioski oraz petycje składane przez obywateli; w tym celu powołuje komisję skarg, wniosków i petycji. Ponadto § 5 rozporządzenia Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków reguluje, że skargi i wnioski mogą być wnoszone również za pomocą poczty elektronicznej, co też miało miejsce w niniejszej sprawie.

Komisja Skarg, Wniosków i Petycji na posiedzeniu w dniu 30.03.2026 r. zapoznała się z przedmiotową skargą i zarekomendowała Radzie Gminy Ornontowice uznanie skargi za **bezzasadną**.

Jak wskazano wyżej, skarga zawiera wiele przykładów zagrożeń związanych z cyberbezpieczeństwem na obszarze całej Polski i w działalności różnych urzędów gmin ale nie sposób dopatrzeć się w jej treści konkretnych przykładów wskazujących na brak należytego nadzoru Wójta nad obszarem cyberbezpieczeństwa w Urzędzie Gminy Ornontowice lub w innych jednostkach organizacyjnych Gminy.

Problematyka cyberbezpieczeństwa stanowi coraz poważniejsze zagadnienie dla wszystkich jednostek samorządu terytorialnego. Dlatego też w strukturze organizacyjnej Urzędu Gminy Ornontowice przewidziano stanowiska informatyka, stanowiska ds. bezpieczeństwa i zarządzania kryzysowego oraz pełnomocnika ds. ochrony informacji niejawnej. Ponadto podjęto szereg działań mających odpowiednio zabezpieczać Gminę Ornontowice w omawianym obszarze.

W ocenie Komisji Skarg, Wniosków i Petycji w piśmie jest brak przekonujących argumentów, by w oparciu o podane w skardze przykłady nie dotyczące bezpośrednio Gminy Ornontowice, uznać za zasadną skargę z dnia 10.03.2026 r. na działalność Wójta Gminy Ornontowice w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów.

Należy podkreślić, iż Urząd Gminy Ornontowice w celu zapewnienia wysokiego poziomu bezpieczeństwa systemów informatycznych oraz ochrony danych wykorzystuje znane i ponad standardowe rozwiązania z zakresu cyberbezpieczeństwa.

Urząd Gminy Ornontowice wdrożył System Zarządzania Bezpieczeństwem Informacji w zgodności z ISO 27001 obejmujący swoim zakresem wymagania zdefiniowane w KRI. Zabezpieczenia dzielone są na kategorie zabezpieczeń organizacyjnych (polityki, procedury i zasady postępowania, audyty), technicznych (zabezpieczenia systemów informatycznych), fizycznych (zabezpieczenia infrastruktury IT, budynku oraz przetwarzanych informacji w formie papierowej) oraz zabezpieczeń ludzkich (uświadamianie, szkolenia). Gmina nie brała udziału w programie "Cyberbezpieczny Samorząd".

W miesiącu listopadzie został przeprowadzony audyt, raport z audytu wewnętrznego wydany został 17.12.2025 roku.

W Urzędzie koordynatorami ds. cyberbezpieczeństwa zgłoszonymi do CSIRT NASK są informatycy, Urząd współpracuje z firmą zewnętrzną w zakresie usług Pełnomocnika ds. cyberbezpieczeństwa. Incydenty wewnętrznie zgłaszane są do bezpośredniego przełożonego, IT oraz Pełnomocnika. Funkcjonuje adres mailowy cyberbezpieczenstwo@ornontowice.pl.

W Urzędzie funkcjonuje procedura zarządzania cyberbezpieczeństwem oraz procedura zarządzania incydentami określająca zasady postępowania w przypadku incydentu cyberbezpieczeństwa. Urząd zdefiniował politykę ciągłości działania, w trakcie opracowania są plany ciągłości działania. Dodatkowo w zakresie ochrony danych osobowych funkcjonuje procedura zgłaszania naruszeń, ich analizy oraz w przypadku identyfikacji wysokiego ryzyka, zgłaszania do organu nadzorczego - UODO. Całokształt niniejszej sprawy wskazuje, że działanie organu wykonawczego Gminy Ornontowice było zgodne z powrzechnie obowiązującymi w tej kwestii przepisami prawa.

W związku z powyższym Komisja podtrzymuje uznanie skargi za bezzasadną.

Zgodnie z art. 239 § 1 Kodeksu postępowania administracyjnego w przypadku, gdy skarga, w wyniku jej rozpatrzenia, została uznana za bezzasadną i jej bezzasadność wykazano w odpowiedzi na skargę, a skarżący ponowił skargę bez wskazania nowych okoliczności - organ właściwy do jej rozpatrzenia może podtrzymać swoje poprzednie stanowisko z odpowiednią adnotacją w aktach sprawy - bez zawiadamiania skarżącego.