



**UCHWAŁA NR XXXI/275/26
RADY MIEJSKIEJ W GRODKOWIE**

z dnia 23 września 2026 r.

**w sprawie rozpatrzenia skargi na działalność Dyrektora Publicznej Szkoły Podstawowej nr 1 im.
Mikołaja Kopernika w Grodkowie**

Na podstawie art. 18 ust. 2 pkt 15 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662 ze zm.^[1]) oraz art. 229 pkt 3 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691) uchwala się, co następuje:

§ 1. Uznaje się za bezzasadną skargę złożoną w dniu 14 sierpnia 2026 r. na działalność Dyrektora Publicznej Szkoły Podstawowej nr 1 im. Mikołaja Kopernika w Grodkowie z przyczyn określonych w uzasadnieniu stanowiącym załącznik do niniejszej uchwały.

§ 2. Wykonanie uchwały powierza się Przewodniczącemu Rady Miejskiej w Grodkowie zobowiązując go do przesłania Skarżącemu niniejszej uchwały wraz z uzasadnieniem.

§ 3. Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Rady

Dariusz Gajewski

^[1] Dz. U. z 2026 r. poz. 912, Dz. U. z 2023 r. poz. 1688

Załącznik do uchwały nr XXXI/275/26

Rady Miejskiej w Grodkowie

z dnia 23 września 2026 r.

Uzasadnienie

W dniu 14 sierpnia 2026 r. za pośrednictwem poczty elektronicznej wpłynęła skarga na działalność Dyrektora Publicznej Szkoły Podstawowej nr 1 im. Mikołaja Kopernika w Grodkowie skierowana do Rady Miejskiej w Grodkowie.

Zarzuty wynikające z treści skargi dotyczą zakresu cyberbezpieczeństwa.

Zgodnie z art. 229 pkt 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, organem właściwym do rozpatrzenia skargi dotyczącej zadań lub działalności kierowników gminnych jednostek organizacyjnych, jest Rada Miejska.

Pismem z dnia 31 sierpnia 2026 r. Przewodniczący Rady Miejskiej w Grodkowie poinformował Skarżącego, że ww. skarga nie może być załatwiona w ustawowym terminie, wskazując termin rozpatrzenia skargi do dnia 30 września 2026 r.

Komisja Skarg, Wniosków i Petycji na posiedzeniu w dniu 8 września 2026 r. badając skargę zapoznała się z treścią wyjaśnień pisemnych złożonych przez dyrektora szkoły w omawianym zakresie, a także w wyniku przeprowadzonej analizy stwierdziła, co następuje:

Z treści niniejszej skargi wynika, że zarzuty w niej zawarte mają charakter ogólny i nie zostały poparte konkretnymi dowodami technicznymi ani szczegółową analizą, która wskazywałaby na rzeczywiste naruszenia bezpieczeństwa, ochrony danych lub obowiązujących przepisów prawa.

W skardze nie wskazano konkretnych podatności bezpieczeństwa, nie przedstawiono wyników audytów technicznych, nie załączono raportów potwierdzających naruszenia, nie wykazano przypadków wycieku danych lub kompromitacji systemów oraz nie wskazano konkretnych błędnych konfiguracji infrastruktury. Przesłane stwierdzenia mają charakter wyłącznie hipotetyczny.

Z wyjaśnień dyrektora szkoły wynika, że treść skarg kierowanych do jednostek samorządu terytorialnego może budzić wątpliwości co do intencji ich autorów. Pisma te wywołują niepotrzebną presję informacyjną oraz poczucie niepewności w kwestii zgodności z prawem i bezpieczeństwem stosowanych rozwiązań cyfrowych, mimo że nie zawierają konkretnych dowodów technicznych odnoszących się do dostawców.

Serwisy dostarczane przez podmiot w tym obszarze są projektowane, rozwijane oraz utrzymywane zgodnie z obowiązującymi wymaganiami dotyczącymi zarówno dostępności cyfrowej, jak i bezpieczeństwa cyfrowego. Strona internetowa oraz BIP Publicznej Szkoły Podstawowej nr 1 im. Mikołaja Kopernika w Grodkowie spełniają wymagania standardu WCAG 2.1, zgodnie z obowiązującymi przepisami dotyczącymi dostępności cyfrowej podmiotów publicznych.

Analiza dostępnych deklaracji dostępności, raportów samooceny oraz dokumentacji platformy wskazuje, że system zapewnia szereg mechanizmów wspierających dostępność i użyteczność serwisów internetowych szkół oraz innych jednostek publicznych.

W szczególności rozwiązania te obejmują m.in.:

- prawidłową i logiczną strukturę nagłówków, ułatwiającą orientację w treści zarówno użytkownikom, jak i technologiom asystującym,
- pełną obsługę serwisu przy użyciu samej klawiatury, bez konieczności korzystania z myszy,
- zachowanie odpowiedniego kontrastu treści oraz możliwość uruchomienia wersji kontrastowej strony,
- kompatybilność z technologiami wspomagającymi, w tym programami odczytu ekranu, takimi jak NVDA, JAWS czy Window-Eyes,
- możliwość zmiany wielkości czcionki oraz skalowania treści bez utraty funkcjonalności i czytelności,

- stosowanie opisów alternatywnych dla elementów graficznych oraz tekstowych odpowiedników dla treści multimedialnych,
- semantyczną strukturę dokumentów i stron internetowych, obejmującą poprawne oznaczanie list, tabel, formularzy i elementów nawigacyjnych,
- spójną i przewidywalną nawigację w całym serwisie, zgodną z zasadami użyteczności i dostępności,
- mechanizmy wspierające szybki dostęp do treści, takie jak mapa strony, wyszukiwarka czy linki do kluczowych sekcji,
- rozwiązania ograniczające ryzyko konfliktów z technologiami asystującymi, m.in. poprzez rezygnację z niestandardowych skrótów klawiaturowych.

Oprogramowanie stron www jest stale rozwijane i dostosowywane do aktualnych wymagań prawnych oraz standardów dostępności.

Infrastruktura oraz rozwiązania oferowane przez podmiot utrzymywane są z zachowaniem wysokich standardów bezpieczeństwa, z uwzględnieniem kierunków i dobrych praktyk wynikających z europejskich regulacji dotyczących cyberbezpieczeństwa, w tym dyrektywy NIS2.

Usługi utrzymywane są w środowisku OVHcloud – europejskiego dostawcy usług chmurowych i hostingowych, specjalizującego się w rozwiązaniach o podwyższonym poziomie dostępności i bezpieczeństwa.

W szczególności:

- systemy podlegają stałemu monitoringowi pod kątem dostępności, integralności oraz potencjalnych zagrożeń,
- regularnie wdrażane są aktualizacje bezpieczeństwa i poprawki systemowe ograniczające ryzyko wystąpienia podatności,
- stosowane są mechanizmy zabezpieczające przed nieautoryzowanym dostępem, obejmujące m.in. szyfrowanie transmisji danych oraz kontrolę dostępu,
- wykorzystywane są zabezpieczenia serwerowe i sieciowe chroniące usługi przed próbami włamań, złośliwym ruchem oraz atakami typu DDoS,
- infrastruktura OVHcloud objęta jest domyślną ochroną Anti-DDoS działającą w sposób ciągły, z globalnym systemem filtrowania ruchu i automatycznym wykrywaniem ataków,
- stosowane są mechanizmy Web Application Firewall (WAF), zabezpieczające aplikacje internetowe przed typowymi zagrożeniami, takimi jak SQL Injection czy XSS,
- realizowane są procedury związane z wykonywaniem kopii bezpieczeństwa, odtwarzaniem danych oraz zapewnieniem ciągłości działania usług,
- środowisko serwerowe korzysta z rozwiązań wysokiej dostępności oraz redundancji infrastruktury, ograniczających ryzyko przerw w działaniu serwisów,
- wykorzystywane są zabezpieczenia obejmujące szyfrowanie SSL/TLS, monitoring usług oraz automatyczne mechanizmy ochronne dostępne w infrastrukturze OVHcloud.

Produkty i rozwiązania spółki podlegają bieżącej weryfikacji oraz analizie przez podmioty specjalizujące się w obszarze bezpieczeństwa cyfrowego i cyberbezpieczeństwa, w tym instytucje zajmujące się reagowaniem na incydenty bezpieczeństwa, takie jak CERT Polska. Dotychczasowe analizy i kontrole nie wykazały zagrożeń podważających bezpieczeństwo oferowanych rozwiązań (ostatnia kontrola: marzec 2026).

Odnosząc się do podnoszonej kwestii płatności za usługi, należy zwrócić uwagę na fakt, że usługi świadczone w modelu darmowym, co do zasady oferują niższy poziom bezpieczeństwa, stabilności i odpowiedzialności niż rozwiązania komercyjne, co wynika przede wszystkim z ograniczonych zasobów przeznaczanych na utrzymanie i rozwój infrastruktury.

W przypadku usług komercyjnych dostawca ponosi natomiast realną odpowiedzialność kontraktową za utrzymanie systemów, bezpieczeństwo danych oraz ciągłość działania usług. Umożliwia to finansowanie

profesjonalnej infrastruktury, audytów bezpieczeństwa, monitoringu oraz mechanizmów ochronnych, zgodnych z aktualnymi standardami cyberbezpieczeństwa i wymaganiami regulacyjnymi.

Z tego względu rozwiązania płatne, szczególnie wykorzystywane przez podmioty publiczne, są co do zasady bardziej przewidywalne, stabilne i bezpieczne niż rozwiązania oparte na darmowych lub hobbystycznych modelach świadczenia usług.

Podkreślić należy, że w skardze nie wskazano żadnych konkretnych incydentów bezpieczeństwa, dotyczących systemów dostarczanych przez podmiot, ani nie wykazano faktycznych naruszeń bezpieczeństwa infrastruktury.

Przedstawione w skardze zarzuty nie znajdują potwierdzenia w przedstawionym stanie faktycznym.

W świetle powyższego Komisja Skarg, Wniosków i Petycji postanowiła uznać skargę za bezzasadną.

Rada Miejska w Grodkowie uznaje za własne ustalenia Komisji Skarg, Wniosków i Petycji. Mając na uwadze powyższe Rada Miejska w Grodkowie w oparciu o stanowisko Komisji Skarg, Wniosków i Petycji uznaje skargę za bezzasadną.

Niniejsza uchwała stanowi zawiadomienie o sposobie załatwienia skargi w rozumieniu art. 237 § 3 w związku z art. 238 § 1 kpa.