UCHWAŁA NR XXIV/188/2026
RADY GMINY DOBRE

z dnia 26 czerwca 2026 r.

w sprawie rozpatrzenia skargi

Na podstawie art.18b ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662) oraz art. 223 § 1, art. 227 i 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. Po rozpatrzeniu skargi z dnia 5 maja 2026 r. na Kierownika Jednostki Samorządu Terytorialnego – Wójta Gminy Dobre w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa uznaje się skargę za bezzasadną.

§ 2. Zobowiązuje się Przewodniczącą Rady Gminy Dobre do powiadomienia wnoszącego skargę o sposobie jej rozpatrzenia oraz przesłania wnoszącemu skargę treści uchwały wraz z uzasadnieniem.

§ 3. 1. Uchwała wchodzi w życie z dniem podjęcia.

2. Uchwała podlega ogłoszeniu w Biuletynie Informacji Publicznej Urzędu Gminy Dobre.

Przewodnicząca Rady

Teresa Wiśniewska

UZASADNIENIE

W dniu 5 maja 2026 r. do Rady Gminy Dobre wpłynęła skarga złożona przez osobę prawną – Spółkę Szulc-Euphenics.com p. Spółka Akcyjna. Pismem z dnia 2 czerwca 2026 r. poinformowano Skarżącego o przedłużeniu rozpatrzenia skargi do dnia 30 czerwca 2026 r. w celu zebrania dodatkowych wyjaśnień i materiału dowodowego. Wniesiona przez osobę prawną – Spółkę Szulc-Euphenics.com p. Spółka Akcyjna skarga została skierowana przeciwko Wójtowi Gminy Dobre, działającemu jako kierownik jednostki samorządu terytorialnego i dotyczyła zarzutu braku należytej kontroli nad wydatkowaniem środków publicznych przez kierowników podległych JO oraz na przestrzeganiu przez tychże kierowników zasad zawiązanych cyberbezpieczeństwem w zakresie bezpieczeństwa stron Biuletynów Informacji Publicznych oraz oficjalnych stron internetowych jednostek podległych.

Skarżący wskazał, iż organ, którego dotyczy skarga, miał naruszyć obowiązek wynikający z 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 teleinformatycznych (Dz.U. z 2024 r., poz. 773), a także pogwałcać dyspozycję ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2025. poz. 1483 z późn. zm.)

Komisja Skarg, Wniosków i Petycji, rozpatrując skargę na posiedzeniu 9 czerwca 2026 r., dokonała szczegółowej analizy jej treści, a także zapoznała się z wyjaśnieniami przedstawionymi przez Wójta Gminy Dobre. Po analizie treści skargi, obowiązujących przepisów prawa oraz stanu faktycznego należy stwierdzić, że zarzuty podniesione w piśmie nie znajdują potwierdzenia ani w obowiązujących regulacjach, ani w realiach technicznych funkcjonowania systemów teleinformatycznych jednostki.

W pierwszej kolejności wskazać należy, że sam fakt korzystania przez jednostkę samorządu terytorialnego z komercyjnego systemu BIP lub komercyjnej strony WWW nie stanowi naruszenia prawa. Żaden przepis ustawy o dostępie do informacji publicznej, ustawy o krajowym systemie cyberbezpieczeństwa ani rozporządzenia w sprawie Krajowych Ram Interoperacyjności nie nakłada na gminę obowiązku korzystania wyłącznie z rozwiązań oferowanych w ramach systemów rządowych. Obowiązek organu dotyczy zapewnienia zgodności z wymaganiami prawa, bezpieczeństwa przetwarzania informacji, dostępności cyfrowej oraz ciągłości działania usług publicznych. Sposób realizacji tych obowiązków może następować zarówno przy użyciu rozwiązań publicznych, jak i komercyjnych, pod warunkiem że spełniają one wymagania techniczne, organizacyjne i prawne. Tym samym sama okoliczność, że na rynku istnieją bezpłatne rozwiązania oferowane przez administrację rządową, nie przesądza automatycznie o bezprawności, niegospodarności ani nieracjonalności wyboru innego systemu.

Odnosząc się do zarzutu, jakoby komercyjny BIP był z definicji mniej bezpieczny niż rozwiązania rządowe, należy wskazać, że takie twierdzenie ma charakter generalny, uproszczony i nie znajduje technicznego uzasadnienia. Bezpieczeństwo konkretnego systemu teleinformatycznego nie wynika z samego faktu, czy jest on bezpłatny, komercyjny, rządowy albo prywatny, lecz z jego architektury, sposobu utrzymania, częstotliwości aktualizacji, modelu autoryzacji, monitoringu, reagowania na incydenty, zarządzania podatnościami oraz jakości konfiguracji. W praktyce nie ma podstaw do kategorycznego stwierdzenia, że system rządowy i system komercyjny są zawsze tak samo bezpieczne albo, że jeden z nich jest z definicji bezpieczniejszy. Tego rodzaju ocena wymagałaby przeprowadzenia porównawczego audytu technicznego, testów bezpieczeństwa, analizy architektury, sposobu zarządzania incydentami, polityki aktualizacji oraz zgodności z wymaganiami KRI i dobrymi praktykami cyberbezpieczeństwa. Bez takich ustaleń nie można przyjąć, że każdy komercyjny system BIP pozostaje w gorszej pozycji bezpieczeństwa względem systemu rządowego.

Jednocześnie należy zwrócić uwagę na istotny aspekt bezpieczeństwa systemowego, jakim jest dywersyfikacja stosowanych rozwiązań. Powszechne wykorzystywanie przez bardzo dużą liczbę podmiotów jednej, centralnej platformy zwiększa ryzyko skutków ewentualnej podatności typu wspólnego. W przypadku ujawnienia krytycznej luki, błędu konfiguracyjnego albo skutecznego przełamania zabezpieczeń w systemie używanym masowo przez wiele jednostek, potencjalny skutek incydentu może objąć równocześnie znaczną liczbę podmiotów. Z punktu widzenia zarządzania ryzykiem oznacza to zwiększone ryzyko efektu skali oraz powstania jednego punktu koncentracji zagrożeń. W systemach rozproszonych, opartych o różnych dostawców, architektury i modele utrzymania, skala jednoczesnego oddziaływania tej samej podatności może być istotnie mniejsza. Nie oznacza to, że rozwiązanie komercyjne jest automatycznie

bezpieczniejsze, lecz że teza, jakoby jednolite rozwiązanie rządowe musiało być zawsze lepsze z punktu widzenia cyberbezpieczeństwa, nie znajduje jednoznacznego potwierdzenia. Z perspektywy bezpieczeństwa infrastruktury publicznej różnorodność technologiczna może ograniczać ryzyko masowego incydentu.

W odniesieniu do kwestii dostępności i zgodności z wymaganiami prawnymi należy wskazać, że zarówno systemy rządowe, jak i systemy komercyjne mogą spełniać wymagania dostępności cyfrowej, standardy publikacji informacji publicznej oraz wymogi wynikające z Krajowych Ram Interoperacyjności. O zgodności z prawem nie przesądza bowiem marka, model licencyjny ani źródło pochodzenia rozwiązania, lecz faktyczne spełnienie określonych parametrów technicznych i organizacyjnych. To, czy dany BIP zapewnia odpowiedni poziom dostępności, bezpieczeństwa oraz poprawności funkcjonowania, wymaga każdorazowo oceny konkretnego wdrożenia. Z tego względu twierdzenie, że system bip.gov lub inne rozwiązanie rządowe jest co do zasady bardziej dostępne i bezpieczne od systemu komercyjnego, w tym systemów w naszych jednostkach, nie może zostać uznane za oczywiste bez odniesienia do konkretnych danych z audytu, testów lub oceny zgodności.

W zakresie argumentacji technicznej należy również podkreślić, że producenci wykorzystywanych przez nas platform BIP deklarują stosowanie rozwiązań odpowiadających aktualnym standardom bezpieczeństwa. Wskazywane są między innymi nowoczesne wersje środowiska uruchomieniowego, takie jak PHP 8.2, mechanizmy ograniczające ryzyko ataków słownikowych i siłowych, w tym rate limiting oraz blokady po błędnych logowaniach, możliwość wdrożenia wieloskładnikowego uwierzytelniania, stały monitoring incydentów, ukrywanie informacji technicznych przed osobami postronnymi, blokowanie i logowanie podejrzanych zapytań oraz utrzymywanie systemu zgodnie z procedurami reagowania na incydenty i wytycznymi CERT Polska. Tego rodzaju rozwiązania mieszczą się w katalogu standardowych, uznanych środków ochrony stosowanych w nowoczesnych systemach teleinformatycznych. Jeżeli są rzeczywiście wdrożone, utrzymywane i aktualizowane, nie ma podstaw, by przyjmować, że rozwiązanie takie narusza wymagania bezpieczeństwa wyłącznie z uwagi na komercyjny charakter.

Skarga zawiera również twierdzenie, że ponoszenie wydatków na komercyjne rozwiązania przy istnieniu rozwiązań bezpłatnych stanowi przejaw rażącej niegospodarności. Także ten zarzut nie zasługuje na uwzględnienie. Ocena gospodarności wydatku publicznego nie może być dokonywana wyłącznie przez porównanie ceny zakupu lub informacji, że na rynku istnieje produkt bezpłatny. Należy uwzględnić całkowity koszt użytkowania, koszty wdrożenia, migracji danych, integracji z obecnymi systemami, parametry wsparcia serwisowego, dostępność indywidualnej obsługi, czas reakcji na awarie, możliwość dostosowania funkcjonalnego do potrzeb jednostki, odpowiedzialność kontraktową wykonawcy, poziom gwarancji utrzymania, zgodność z już działającą architekturą teleinformatyczną urzędu, a także ryzyka organizacyjne związane ze zmianą systemu. System bezpłatny nie musi być rozwiązaniem najkorzystniejszym ekonomicznie w całym cyklu życia usługi. Również odpłatne rozwiązanie nie jest z tego powodu automatycznie niegospodarne. O prawidłowości wydatku rozstrzyga jego celowość, legalność, oszczędność i efektywność oceniane w konkretnych uwarunkowaniach organizacyjnych i technicznych jednostki.

Nie można także podzielić stanowiska skarżącego, jakoby wybór rozwiązania komercyjnego sam w sobie oznaczał naruszenie zasad uczciwej konkurencji. Wręcz przeciwnie, korzystanie z rozwiązań rynkowych, nabywanych zgodnie z obowiązującymi procedurami i z zachowaniem zasad wydatkowania środków publicznych, mieści się w mechanizmach konkurencji gospodarczej przewidzianych przez przepisy prawa. Gmina nie ma obowiązku rezygnowania z rozwiązań komercyjnych wyłącznie dlatego, że dostępne są także usługi oferowane przez sektor publiczny. O ile wybór wykonawcy albo modelu usługi został dokonany zgodnie z prawem i uwzględniał potrzeby jednostki, nie sposób uznać tego za działanie sprzeczne z interesem publicznym.

W części odnoszącej się do bezpieczeństwa obiegu dokumentów i nadzoru nad cyberbezpieczeństwem należy wskazać, że obowiązki jednostki w tym zakresie realizowane są na bieżąco w ramach systemu organizacyjnego urzędu, procedur wewnętrznych, utrzymania infrastruktury teleinformatycznej, szkoleń, aktualizacji oraz stosowania środków technicznych i organizacyjnych adekwatnych do poziomu ryzyka. Sama okoliczność przywoływania w skardze incydentów występujących w innych jednostkach samorządu terytorialnego, nawet medialnie nagłośnionych, nie może być utożsamiana z wykazaniem konkretnego zaniedbania po stronie tutejszego organu. Przykłady z innych gmin, miast albo urzędów mają charakter ogólny i publicystyczny. Mogą one uzasadniać potrzebę ciągłego doskonalenia standardów cyberbezpieczeństwa w administracji publicznej, lecz nie dowodzą automatycznie, że w danej

gminie doszło do naruszenia obowiązków nadzorczych albo, że wykorzystywany system BIP jest niebezpieczny.

Należy również zaznaczyć, że odpowiedzialne zarządzanie cyberbezpieczeństwem nie polega wyłącznie na wyborze jednej kategorii dostawcy usług, lecz na stałej analizie ryzyka, utrzymywaniu aktualności systemów, egzekwowaniu właściwych mechanizmów autoryzacji, prowadzeniu monitoringu, kontroli dostępu, wykonywaniu kopii bezpieczeństwa, nadzorze nad publikacją treści i reagowaniu na nieprawidłowości. W tym kontekście redukowanie całego zagadnienia do prostego twierdzenia, że „bezpłatny BIP rządowy jest bezpieczny, a komercyjny jest niebezpieczny", nie odpowiada rzeczywistemu stanowi wiedzy technicznej i nie może stanowić samodzielnej podstawy uznania skargi za zasadną.

Ponad to dodać należy, iż Gmina Dobre realizowała i zakończyła projekt grantowy „Cyfrowa Gmina" w ramach, którego zakupiono sprzęt i oprogramowanie, wykonano modernizację infrastruktury informatycznej, przeprowadzono diagnozę stanu cyberbezpieczeństwa systemów Gminy, zidentyfikowano potencjalne słabości oraz obszary wymagające wzmocnienia. Gmina Dobre realizuje również projekt „Cyberbezpieczny Samorząd", który obejmuje działania w zakresie opracowania dokumentacji dotyczącej cyberbezpieczeństwa, audytów, zakupu sprzętu sieciowego zabezpieczającego, organizację szkoleń dla pracowników i kadry zarządzającej. Na tej podstawie Komisja przyjmuje, że Skarżony Organ tj. Kierownik JST działający za zgodą i w ramach kompetencji gminy uczestniczy aktywnie w projektach służących podnoszeniu poziomu bezpieczeństwa teleinformatycznego Gminy.

Mając na względzie powyższe, należy stwierdzić, że zarzut dotyczący rzekomego braku należytego nadzoru nad obszarem cyberbezpieczeństwa, wynikający z korzystania z komercyjnego rozwiązania BIP, nie został wykazany. Nie przedstawiono dowodów potwierdzających, że użytkowane przez gminę rozwiązanie nie spełnia obowiązujących wymogów prawnych, wymagań bezpieczeństwa lub standardów dostępności. Nie wykazano również, aby rozwiązania rządowe były w sposób oczywisty i bezwzględny bardziej bezpieczne od rozwiązań komercyjnych ani aby sam wybór systemu komercyjnego stanowił przejaw niegospodarności. Z technicznego punktu widzenia należy przyjąć, że poziom bezpieczeństwa systemu zależy od całokształtu przyjętej architektury, utrzymania i nadzoru, a nie od samego faktu jego komercyjnego albo publicznego pochodzenia. Co więcej, przy dużej skali wykorzystania jednego wspólnego rozwiązania rządowego należy uwzględniać ryzyko skumulowanego oddziaływania incydentu na znaczną liczbę podmiotów, podczas gdy zróżnicowanie stosowanych platform może ograniczać skutki masowych zdarzeń.

Mając na uwadze zgromadzony materiał dowodowy, stanowisko Komisji Skarg, Wniosków i Petycji oraz analizę przedstawionych zarzutów, Rada Gminy Dobre nie znajduje podstaw do uznania skargi za zasadną i z tej właśnie przyczyny uznaje ją za bezzasadną. Na podstawie art. 239 § 1 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, w przypadku ponowienia skargi bez wskazania nowych okoliczności, organ właściwy do jej rozpatrzenia może podtrzymać swoje dotychczasowe stanowisko, dokonując odpowiedniej adnotacji w aktach sprawy, bez obowiązku zawiadamiania skarżącego.