Gmina Świerklaniec
ul. Młyńska 3, 42-622 Świerklaniec
32 284 74 00, e-mail: kancelaria@ugswierklaniec.pl

BRG.1

SEKRETARIAT
URZĘDU GMINY ŚWIERKLANIEC
WPŁYNĘŁO
07. MAJ. 2026
Ilość załączników .....
Nr ..... podpis .....

Świerklaniec, dnia 7 maja 2026r.

BI.1510.1.2026

Komisja Skarg, Wniosków i Petycji

W nawiązaniu do pisma z dnia 4 maja 2026r. o nr BRG.0012.6.2026 przedkładam następujące wyjaśnienia w przedmiocie: **braku należytego nadzoru nad zamawianymi przez JST usługami dostarczanymi przez firmy zewnętrzne.**

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.

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, 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 tut. 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.

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 stoję na stanowisku, że skarga jest niezasadna.

WÓJT

mgr Grzegorz Zadecki