UCHWAŁA NR 101/4716/26
ZARZĄDU WOJEWÓDZTWA KUJAWSKO-POMORSKIEGO

z dnia 8 kwietnia 2026 r.

w sprawie unieważnienia postępowania o udzielenie zamówienia publicznego w trybie z wolnej ręki

Na podstawie art. 2 ust. 1 pkt 1, art. 4 pkt 1, art. 255 pkt 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.[1)]) oraz art. 41 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581 i 1535 oraz z 2026 r. poz. 252 i 451), uchwala się, co następuje:

§ 1. Zatwierdza się protokół Komisji Przetargowej dotyczący postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest rozbudowa i modernizacja systemu cyfrowego repozytorium Wirtualnego Muzeum Kujaw i Pomorza w ramach projektu „Kultura w zasięgu 3.0" realizowanego ze środków Programu Regionalnego: Fundusze Europejskie dla Kujaw i Pomorza na lata 2021–2027.

§ 2. Unieważnia się przedmiotowe postępowanie, ponieważ wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć.

§ 3. Wykonanie uchwały powierza się Marszałkowi Województwa Kujawsko-Pomorskiego.

§ 4. Uchwała wchodzi w życie z dniem podjęcia.

[1)] Zmiany tekstu jednolitego wymienionej ustawy ogłoszono w Dz. U. z 2025 r. poz. 620, 769, 794, 1165, 1173 i 1235 oraz z 2026 r. poz. 252.

Uzasadnienie

1. Przedmiot regulacji:

Uchwała Zarządu Województwa Kujawsko-Pomorskiego w sprawie unieważnienia postępowania o udzielenie zamówienia publicznego w trybie z wolnej ręki.

2. Omówienie podstawy prawnej:

Zgodnie z art. 41 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, zarząd województwa wykonuje zadania należące do samorządu województwa, niezastrzeżone na rzecz sejmiku województwa i wojewódzkich samorządowych jednostek organizacyjnych. Zgodnie z art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej: ustawy Pzp) przepisy ustawy stosuje się do udzielania zamówień klasycznych oraz organizowania konkursów, których wartość jest równa lub przekracza kwotę 170 000 złotych, przez zamawiających publicznych. W myśl art. 4 pkt 1 ustawy Pzp, Województwo Kujawsko-Pomorskie, które wykonuje zadania przy pomocy Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego w Toruniu, jako jednostka sektora finansów publicznych w rozumieniu przepisów o finansach publicznych jest zobowiązana do stosowania ustawy Prawo zamówień publicznych. Na podstawie art. 255 pkt 5 ustawy Pzp, zamawiający unieważnia postępowanie o udzielenie zamówienia, jeżeli: wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć.

3. Konsultacje wymagane przepisami prawa (łącznie z przepisami wewnętrznymi):

Przepisy prawa nie wymagają konsultacji w przedmiocie niniejszej uchwały.

4. Uzasadnienie merytoryczne:

W dniu 2 kwietnia 2026 r. Województwo Kujawsko-Pomorskie (Zamawiający) opublikowało ogłoszenie o zamiarze zawarcia umowy w trybie zamówienia z wolnej ręki na usługę „Rozbudowa i modernizacja systemu cyfrowego repozytorium Wirtualnego Muzeum Kujaw i Pomorza". Zadanie to stanowi kluczowy element projektu dofinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego.

W toku czynności przygotowawczych do negocjacji, przeprowadzono ponowną weryfikację ryzyk projektowych w kontekście kwalifikowalności wydatków oraz spójności z dokumentami strategicznymi. W trakcie trwania procedury nastąpiła istotna zmiana stanu prawnego, który bezpośrednio determinuje standardy wdrażania systemów teleinformatycznych w administracji publicznej.

Zgodnie z obowiązującym od dnia 3 kwietnia 2026 r. art. 69 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, z późn. zm.):

„1. Strategia określa:

1) cele strategiczne i cele szczegółowe oraz środki organizacyjne i regulacyjne, służące ich realizacji;

2) mechanizm służący określeniu istotnych zasobów i szacowania ryzyka związanego z cyberbezpieczeństwem;

3) zasady współpracy między sektorem publicznym i prywatnym;

4) podmioty zaangażowane we wdrażanie i realizację Strategii;

5) środki służące koordynacji i wymianie informacji pomiędzy organami właściwymi w sprawach cyberbezpieczeństwa a właściwymi organami na podstawie dyrektywy 2022/2557 na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią ora wykonywania zadań nadzorczych;

6) działania w zakresie zwiększenia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie;

7) cele i sposób realizacji interesów cyberbezpieczeństwa krajowego w wymiarze międzynarodowym.

2. Przy opracowaniu strategii uwzględnia się:

1) rozwiązania dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT, usług ICT i procesów ICT wykorzystywanych przez podmioty do świadczenia usług;

2) rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT, usług ICT i procesów ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu;

3) rozwiązania dotyczące zarządzania podatnościami, obejmujące promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1 dyrektywy 2022/2555;

4) utrzymanie ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego Internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych;

5) promowanie rozwoju i integracji odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków zarządzania ryzykiem w cyberbezpieczeństwie;

6) kształcenie i szkolenia w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, rozwój i promocję kwalifikacji rynkowych w zakresie cyberbezpieczeństwa w przemyśle, podnoszenie świadomości oraz inicjatywy badawczo-rozwojowe, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie higieny cyfrowej;

7) wspieranie instytucji akademickich i naukowych, w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury sieciowej;

8) zapewnienie odpowiednich procedur oraz narzędzi służących wymianie informacji;

9) rozwiązania wzmacniające podstawowy poziom cyberodporności i higieny cyfrowej małych i średnich przedsiębiorstw;

10) rozwiązania wspierające aktywne działania w cyberprzestrzeni.”.

Zgodnie z pkt 7.1. Strategii: „7.1. *Podniesienie poziomu odporności systemów informacyjnych W zamówieniach publicznych będą uwzględniane wymogi związane z cyberbezpieczeństwem w odniesieniu do produktów ICT, usług ICT i procesów ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, obowiązku zastosowania mechanizmów kryptograficznych wykorzystujących powszechnie uznawane normy oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu.*

Z uwagi na rosnące znaczenie otwartego oprogramowania w infrastrukturze cyfrowej państwa będą wspierane inicjatywy zapewniające krajowe wsparcie techniczne, rozwój i utrzymanie kluczowych komponentów otwartoźródłowych wykorzystywanych w systemach administracji publicznej oraz podmiotów KSC. Wzmocnienie krajowego zaplecza oprogramowania otwartoźródłowego przyczyni się do zwiększenia niezależności technologicznej RP oraz odporności łańcucha dostaw na zagrożenia zewnętrzne.”.

W związku z powyższym, zaszła konieczność zmiany koncepcji rozbudowy i modernizacji systemu cyfrowego repozytorium Wirtualnego Muzeum Kujaw i Pomorza w ramach projektu „Kultura w zasięgu 3.0” na koncepcję opartą na otwartym oprogramowaniu. Zatem, bezcelowe jest kontynuowanie postępowania w trybie „z wolnej ręki” z Wykonawcą systemu.

Z uwagi na wieloletni cykl życia produktu oraz konieczność zachowania pełnej zgodności z aktualną strategią cyfryzacji państwa, Zamawiający w nowym postępowaniu otwartym uwzględni w OPZ poniższe aspekty:

· wzmocnienie odporności systemów informacyjnych:

konieczność implementacji rygorystycznych norm cyberbezpieczeństwa, w tym zastosowania zaawansowanych mechanizmów kryptograficznych opartych na powszechnie uznawanych standardach oraz wykorzystania certyfikowanych produktów zabezpieczających,

· wdrażanie otwartych standardów i budowanie niezależności technologicznej:

zgodnie z nowymi wytycznymi, system musi opierać się na otwartym oprogramowaniu, co ma na celu zapewnienie krajowego wsparcia technicznego, niezależności od dostawców zewnętrznych oraz zwiększenie odporności łańcucha dostaw.

Dalsze prowadzenie postępowania w obecnym kształcie wiązałoby się z ryzykiem utraty kwalifikowalności wydatków z EFRR oraz wdrożeniem systemu nieodpowiadającego aktualnym standardom bezpieczeństwa państwa.

Mając na uwadze powyższe, uzasadnione jest unieważnienie postępowania o udzielenie zamówienia w trybie z wolnej ręki na podstawie art. 255 pkt 5 ustawy Pzp, który stanowi, iż unieważnia postępowanie o udzielenie zamówienia, jeżeli: wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć.

5. Ocena skutków regulacji:

Zarezerwowane środki należy zwolnić spod rezerwacji.