Fundusze Europejskie

Wpływ regulacji KSC na publiczne procesy zakupowe

Ewa Ropka

Warszawa, 7 września 2026

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

...od zamówień na cyberbezpieczeństwo
po cyberbezpieczeństwo
w zamówieniach ...

Relacja KSC do PZP

Kryterium wpływu: weryfikacja podmiotowa???

zamawiający ≠ podmioty kluczowe/podmioty ważne

- **podmioty kluczowe** – m.in. **podmioty publiczne** wskazane w załączniku nr 1 do ustawy w sektorze podmioty publiczne (art. 5 ust. 1 pkt 4 d uKSC) – załącznik nr 1 Sektory kluczowe – Podsektor: Podmioty publiczne (art. 9 pkt 1, 3, 5-6, 8-9 uFinPub)
- **podmioty ważne** – mi.n. **podmioty publiczne**, które nie są podmiotem kluczowym oraz jest samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką wykonującą zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), jeżeli realizują zadanie publiczne z wykorzystaniem systemów informacyjnych (art. 5 ust. 1 pkt 4 d uKSC)

- ogromna liczba podmiotów publicznych o statusie zamawiających (wg uPZP) uzyskało status podmiotów kluczowych lub ważnych (wg uKSC)

Relacja KSC do PZP

Kryterium wpływu: wartość zamówienia???

Zakres stosowania ustawy uKSC wobec zamawiających jest determinowany kryterium podmiotowym - zakres odziaływania uKSC:

- zamówienia publiczne podlegające stosowaniu ustawy uPZP
- zamówienia publiczne „podprogowe”

- wpływ uKSC na podmioty publiczne w kontekście procesów zakupowych nie zależy od wartości zamówienia determinującej reżim uPZP

Relacja KSC do PZP

Kryterium wpływu: etap procesu zakupowego???

Zakres stosowania ustawy uKSC obejmuje:

- etap przygotowania postępowania
- etap procedury zamówienia publicznego
- etap zawierania umowy
- etap realizacji umowy
- etap „wychodzenia” z umowy

- uKSC może wpływać na każdy etap procesu zakupowego = procesy zakupowe jako element *cybersecurity governance*

Decyzja HRV - uznanie za dostawcę wysokiego ryzyka - instrument KSC

Skutki decyzji (art. 67 uKSC):

- **zakaz wprowadzania do użytkowania** typów produktów ICT, rodzajów usług ICT, konkretnych procesów ICT w zakresie objętym decyzją przez dostawcę wysokiego ryzyka
- **wycofanie z użytkowania** typow produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka niepóźniej niż w terminie 7 lat od dnia ogłoszenia decyzji
- **zakaz nabywania** na podstawie uPZP typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji

Etap przygotowania postępowania

- **analiza potrzeb i wymagań**: analiza interesariuszy i skład zespołów, wpływ analizy ryzka cybersecurity zamawiającego na dokumenty zamówienia – wskaźniki ciągłości działania
- **wstępne konsultacje rynkowe**: polityki bezpieczeństwa wykonawców i zakres dostosowania do zamawiającego, wpływ podwyższonych wymagań na cenę, standardy SLA, analizy łańcucha dostawców
- **analiza rynku**: wpływ wymagań cybersecurity na poziom konkurencji i wartość zamówienia,
- **analiza doświadczeń i wnioski z ewaluacji umowy**: dotychczasowy zakres podwykonawstwa

Ryzyko → Wymaganie → Weryfikacja

Etap procedury zamówienia publicznego

- odrzucenie oferty (art. 226 ust.1 pkt 17) 19) uPZP

- produkt ICT, usługa ICT lub proces ICT wskazane w rekomendacji

- produkt ICT, usługę ICT lub proces ICT określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka,

- przedmiotowe środki dowodowe: certyfikaty (Common Criteria, SOC), raporty branżowe (Gartner, Forrester Wave, Mitre Engenuity), oświadczenia producenta, karty katalogowe, ankiety dot. cyberbezpieczeństwa
- kryteria oceny ofert: dodatkowe certyfikacje/autoryzacje związane z cyberbezpieczeństwem, dodatkowe funkcjonalności, wyniki audytów/testów np. penetracyjnych, zakres SLA, jakościowe parametrów
- badanie zdolności: warunki udziału/wymagania dla personelu wykonawcy
- unieważnienie postępowania (art. 255 pkt 5) uPZP

Etap zawierania umowy

- zabezpieczenie należytego wykonania umowy
- ankiety/oświadczenia dot. cyberbezpieczeństwa
- weryfikacja aktualności/dostarczenie dokumentów wymaganych na etapie proceduralnym: certyfikaty/raporty/oświadczenia
- dostosowanie do polityk bezpieczeństwa zamawiającego/weryfikacja personelu wykonawcy/zobowiązanie do zachowania poufności

Etap realizacji umowy

- cykliczność sposób weryfikacji wymagań dot. cyberbezpieczeństwa: wyniki audytów/testów, składania oświadczeń, samodzielna weryfikacja informacji, ciągłość aktualności dokumentów, ankiety cyberbezpieczeństwa,
- identyfikacja łańcucha ICT (uKSC) ≠ Identyfikacja podwykonawców (uPzp)
- warunki SLA: sposób weryfikacji wymagań, obsługa i raportowanie incydentów, poziom dostępności, zarządzanie podatnościami,
- zmiany umowy: komponentów/procesów/architektury/sposobu świadczenia
- transfer wiedzy: praktyka i materiały szkoleniowe, administratorzy/użytkownicy
- zapewnienie praw autorskich: kodów/dokumentacji technicznej
- kary umowne (dowody zgodności, logi, audyty)
- odstąpienie/odstąpienie częściowe – w odniesieniu do etapu realizacji/ wyodrębnionej składowej zamówienia – w kontekście produkt/usług/proces ICT HRV

Etap „wychodzenia” z umowy

- procedura przekazania dokumentacji technicznej/logów
- migracja danych
- procedura usunięcia danych i informacji

- jako elementy dostosowane do technologicznego „exit plan”

KSC vs.

- uwarunkowania organizacyjno - techniczne
- koszty
- potencjał rynku
- zasada proporcjonalności
- zasada uczciwej konkurencji