NUMER 7:
NOWE REGULACJE, NOWE RYZYKA:
CYBERBEZPIECZEŃSTWO W ZAMÓWIENIACH PUBLICZNYCH

WPROWADZENIE

Cyberbezpieczeństwo przestaje być wyłącznie zagadnieniem technicznym. Zmiany w Prawie zamówień publicznych wprowadziła ustawa z 23.01.2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, ogłoszona w Dzienniku Ustaw 2.03.2026 r. pod poz. 252. Przepisy te obowiązują od 3 kwietnia i powodują, że cyberbezpieczeństwo staje się realnym elementem oceny dopuszczalności ofert, zarządzania ryzykiem kontraktowym i odpowiedzialności compliance. Zamawiający muszą uwzględniać nowe przesłanki odrzucenia ofert, a wykonawcy powinni być gotowi wykazać bezpieczeństwo i przejrzystość swoich łańcuchów dostaw ICT.

Zmiany te dotyczą nie tylko typowych zamówień informatycznych. Ryzyko może pojawić się również w projektach infrastrukturalnych, budowlanych, energetycznych, utrzymaniowych i usługowych, jeżeli ich elementem są systemy ICT, usługi chmurowe, infrastruktura sieciowa, rozwiązania cyberbezpieczeństwa, platformy komunikacyjne albo procesy utrzymania i aktualizacji.

CYBERBEZPIECZEŃSTWO A OCENA OFERT

Nowelizacja Pzp wprowadza istotne konsekwencje na etapie badania i oceny ofert. Zmieniony art. 226 ust. 1 pkt 17 Pzp przewiduje obowiązek odrzucenia oferty obejmującej produkt, usługę lub proces ICT objęte rekomendacją Pełnomocnika Rządu ds. Cyberbezpieczeństwa, jeżeli rekomendacja stwierdza ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa. Nowy art. 226 ust. 1 pkt 19 Pzp obejmuje natomiast rozwiązania powiązane z decyzją w sprawie dostawcy wysokiego ryzyka.

W centrum nowych obowiązków znajdują się dwa mechanizmy ustawy z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (KSC). Pierwszy wynika z art. 33 KSC i dotyczy rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Rekomendacje te mogą być wydawane po badaniu produktu ICT, usługi ICT lub procesu ICT przez właściwe zespoły CSIRT, jeżeli zidentyfikowana podatność może zagrozić m.in. poufności, integralności, dostępności, rozliczalności albo autentyczności danych, a w konsekwencji bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa. W szczególnym trybie art. 33 ust. 4a KSC rekomendacja może być wydana w razie możliwości wystąpienia incydentu krytycznego.

Drugi mechanizm wynika z art. 67b KSC i dotyczy postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Postępowanie prowadzi minister właściwy ds. informatyzacji w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Decyzja nie musi obejmować całej działalności dostawcy — może odnosić się do określonych typów produktów, rodzajów usług ICT albo procesów ICT. Jej znaczenie dla zamówień publicznych jest istotne, ponieważ oferta oparta na rozwiązaniach objętych taką decyzją może podlegać odrzuceniu, a zamawiający powinien umieć powiązać treść decyzji z konkretnym przedmiotem zamówienia i zakresem oferty.

To właśnie rekomendacje i decyzje wydawane na podstawie KSC uruchamiają po stronie zamawiającego obowiązek oceny, czy zachodzi

jedna z nowych przesłanek odrzucenia oferty przewidzianych w Pzp. Dla zamawiających oznacza to konieczność bieżącego monitorowania tych aktów oraz przełożenia ich na opis przedmiotu zamówienia, wymagania przedmiotowe oraz w zakresie podwykonawstwa technologicznego i projektowane postanowienia umowy. Dla wykonawców oznacza to potrzebę stałej kontroli, czy oferowane rozwiązanie w tym komponenty pochodzące od producentów, integratorów, dostawców chmury lub podwykonawców serwisowych – nie są objęte rekomendacją albo decyzją dotyczącą dostawcy wysokiego ryzyka.

W praktyce oznacza to jedno: oferta może być najkorzystniejsza cenowo, zgodna funkcjonalnie z SWZ i technicznie poprawna, a mimo to podlegać odrzuceniu, jeżeli obejmuje komponent, usługę lub proces ICT objęty ryzykiem regulacyjnym. Cyberbezpieczeństwo staje się więc elementem dopuszczalności oferty, a nie wyłącznie wymaganiem eksploatacyjnym.

Przykład: zamawiający prowadzi postępowanie na wdrożenie systemu monitoringu infrastruktury lub platformy zarządzania usługami miejskimi. Oferta wykonawcy obejmuje rozwiązanie technicznie zgodne z SWZ i atrakcyjne cenowo, ale jeden z kluczowych komponentów systemu – np. element infrastruktury sieciowej, usługa chmurowa albo moduł cyberbezpieczeństwa – jest objęty rekomendacją wydaną na podstawie ustawy z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (KSC) albo jest objęty decyzją dotyczącą dostawcy wysokiego ryzyka bądź pozostaje z nią funkcjonalnie powiązany. W takiej sytuacji zamawiający powinien zbadać, czy zachodzi obowiązek odrzucenia oferty na podstawie nowych przesłanek Pzp, a wykonawca musi liczyć się z koniecznością wykazania, że oferowane rozwiązanie nie narusza tych wymogów albo że zaproponował bezpieczny i dopuszczalny wariant równoważny.

Jak wynika z przykładu, analiza cyberbezpieczeństwa nie może ograniczać się do głównego systemu lub dostawcy. Powinna obejmować cały technologiczny łańcuch rozwiązania – od produktów i usług ICT po procesy utrzymania, aktualizacji i integracji.

ZAKRES RYZYKA

Kluczowe znaczenie ma odejście od zawężonego rozumienia „urządzeń informatycznych" i „oprogramowania". Nowe przepisy posługują się pojęciami produktu ICT, usługi ICT i procesu ICT. To znacząco rozszerza obszar weryfikacji. Ryzyko może dotyczyć nie tylko głównego sytemu lub urządzenia, lecz także usługi chmurowej, hostingu, utrzymania, integracji, aktualizacji, administrowania systemem, procesu projektowania albo komponentów bezpieczeństwa.

Szczególnej uwagi wymagają m.in. firewalle, systemy EDR/XDR, IAM, SIEM, systemy pocztowe, platformy CMS, rozwiązania komunikacyjne, komponenty infrastruktury sieciowej oraz usługi serwisowe i utrzymaniowe. W praktyce przedmiot zamówienia może być regulacyjnie wrażliwy nawet wtedy, gdy ICT nie jest jego głównym elementem, lecz jedynie częścią architektury rozwiązania.

Dla zamawiających oznacza to potrzebę bardziej precyzyjnego opisu wymagań i mechanizmów weryfikacji. Dla wykonawców – konieczność znajomości własnego łańcucha dostaw i gotowość przedstawienia dowodów zgodności już na etapie postępowania.

OBOWIĄZKI ZAMAWIAJĄCYCH A CYBERBEZPIECZEŃSTWO

Zamawiający powinni już na etapie planowania postępowania ustalić, czy jego przedmiot obejmuje produkty, usługi lub procesy ICT. Jeżeli tak, dokumenty zamówienia powinny umożliwiać realną ocenę ryzyka cyberbezpieczeństwa. W praktyce należy rozważyć obowiązek wskazania kluczowych komponentów ICT, producentów, dostawców usług chmurowych, integratorów oraz podwykonawców technologicznych.

Zasadne jest również żądanie oświadczeń potwierdzających, że oferowane rozwiązania nie są objęte rekomendacją wydaną na podstawie KSC ani decyzją dotyczącą dostawcy wysokiego ryzyka. Takie wymogi powinny być proporcjonalne, powiązane z przedmiotem zamówienia

i sformułowane w sposób pozwalający na ich późniejszą weryfikację.
Z perspektywy praktycznej dobrze przygotowane SWZ może być dziś jednym z najważniejszych narzędzi ograniczania ryzyka. Pozwala uniknąć sytuacji, w której problem cyberbezpieczeństwa ujawnia się dopiero po wyborze oferty albo na etapie realizacji umowy.

WYKONAWCY POTRZEBUJĄ DOWODÓW, A NIE DEKLARACJI

Po stronie wykonawców ogólne oświadczenie o zgodności z prawem może okazać się niewystarczające. W przypadku rozwiązań ICT standardem powinno stać się udokumentowane due diligence łańcucha dostaw. Powinno ono obejmować producentów, dystrybutorów, resellerów, integratorów, dostawców usług chmurowych, podwykonawców wdrożeniowych i serwisowych oraz producentów komponentów bezpieczeństwa.

Przed złożeniem oferty warto przygotować rejestr kluczowych elementów rozwiązania, obejmujący co najmniej nazwę produktu, producenta, funkcję w architekturze, dostawcę usługi, kraj pochodzenia oraz podmioty odpowiedzialne za utrzymanie lub aktualizacje. Następnie warto zestawić rejestr z aktualnymi rekomendacjami i decyzjami wydawanymi na podstawie KSC.

Dobrą praktyką jest pozyskanie od kluczowych partnerów technologicznych pisemnych oświadczeń compliance oraz zobowiązań do niezwłocznego informowania o zmianie statusu produktu, usługi, procesu ICT albo dostawcy. Taki pakiet dowodowy może mieć znaczenie przy wyjaśnieniach, kontroli, sporze odwoławczym lub negocjacjach dotyczących zmiany umowy.

CO WARTO ZROBIĆ JUŻ TERAZ?

Zamawiający powinni przejrzeć wzory SWZ, projektowane postanowienia umów i procedury badania ofert pod kątem produktów, usług i procesów ICT. W szczególności warto wprowadzić mechanizmy identyfikacji komponentów technologicznych, obowiązki informacyjne wykonawców, zasady akceptacji rozwiązań równoważnych oraz procedurę reagowania na nową rekomendację lub decyzję organu.

Wykonawcy powinni uporządkować dokumentację łańcucha dostaw, przygotować matrycę zgodności z KSC oraz powiązanymi standardami cyberbezpieczeństwa, pozyskać oświadczenia od partnerów technologicznych i przewidzieć w umowach z dostawcami obowiązki aktualizacyjne, notyfikacyjne oraz odpowiedzialność za zmianę statusu produktu lub dostawcy.

PODSUMOWANIE

Cyberbezpieczeństwo staje się jednym z tych obszarów, w których przewaga będzie należała do podmiotów przygotowanych wcześniej. Dobrze zaprojektowane postępowanie, rzetelna dokumentacja compliance i przemyślane klauzule umowne mogą ograniczyć ryzyko odrzucenia oferty, sporu odwoławczego, opóźnień oraz dodatkowych kosztów realizacji zamówienia.

Jeżeli chcą Państwo sprawdzić, czy planowane postępowanie, oferta lub dokumentacja kontraktowa są dostosowane do nowych wymogów cyberbezpieczeństwa, zapraszamy do kontaktu z SDZLEGAL Schindhelm.
Przeanalizujemy ryzyka, wskażemy praktyczne działania zabezpieczające oraz pomożemy przygotować rozwiązania zgodne z Pzp, KSC i standardami compliance – zanim problem stanie się podstawą odrzucenia oferty, sporu odwoławczego albo przysporzy trudności na etapie realizacji umowy.

r.pr. Martyna Wójcik-Szydełko
Wrocław, 10.08.2026 r.

SDZLEGAL Schindhelm
Kancelaria Prawna
Schampera, Dubis, Zając i Wspólnicy
ul. Kazimierza Wielkiego 3
50-077 Wrocław
tel.: +48 71 326 51 40
e-mail: wroclaw@sdzlegal.pl
pl.schindhelm.com