



Piekary Śląskie, 21 września 2026 r.

BZP.271.29.2026

WYJAŚNIENIE I ZMIANA TREŚCI SPECYFIKACJI

dotyczy postępowania o udzielenie zamówienia publicznego pn.

Asysta techniczna i konserwacja systemu OTAGO 2026-2027

Zamawiający – Gmina Piekary Śląskie reprezentowana przez Prezydenta Miasta - na podstawie art. 284 ust. 1, 2, 6 i art. 286 ust. 1, 3, 5, 7 *ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych* informuje, że do treści specyfikacji wpłynęły pytania, na które udziela odpowiedzi i zmienia treść SWZ jak niżej:

Pytanie nr 7

Dotyczy § 4 ust. 6 pkt 1 w zw. z § 4 ust. 7–11 Umowy – zakres rekomendacji, o której mowa w art. 33 ust. 4 KSC

Czy Zamawiający potwierdza, że przez rekomendację, o której mowa w § 4 ust. 6 pkt 1 Umowy, rozumie rekomendację, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającą negatywny wpływ danego produktu ICT, usługi ICT lub procesu ICT na podstawowy interes bezpieczeństwa państwa, o której mowa w art. 226 ust. 1 pkt 17 ustawy Prawo zamówień publicznych, i w związku z tym dokona odpowiedniej zmiany § 4 ust. 6 pkt 1 Umowy?

W przypadku odpowiedzi twierdzącej Wykonawca wnosi o nadanie § 4 ust. 6 pkt 1 następującego brzmienia:

„1) produktu ICT, usługi ICT lub procesu ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;”.

W przypadku odpowiedzi przeczącej prosimy o wskazanie uzasadnienia dla objęcia skutkami określonymi w § 4 ust. 7–11 Umowy także rekomendacji, które nie spełniają przesłanki określonej w art. 226 ust. 1 pkt 17 Pzp.

Uzasadnienie

Zgodnie z § 4 ust. 6 pkt 1 projektu Umowy Wykonawca oświadcza, że na dzień zawarcia Umowy przedmiot Umowy w zakresie produktów ICT, usług ICT i procesów ICT nie obejmuje produktów ICT, usług ICT ani procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 KSC.

Jednocześnie art. 226 ust. 1 pkt 17 Pzp przewiduje obowiązek odrzucenia oferty obejmującej produkt ICT, usługę ICT lub proces ICT wskazane w rekomendacji, o

której mowa w art. 33 ust. 4 KSC, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa.

§ 4 ust. 6 pkt 1 projektu Umowy nie zawiera powyższego ograniczenia i literalnie obejmuje każdą rekomendację wydaną na podstawie art. 33 ust. 4 KSC.

Ma to istotne znaczenie wobec treści § 4 ust. 7–11 Umowy, ponieważ z objęciem rozwiązania zakresem § 4 ust. 6 związane zostały daleko idące konsekwencje, obejmujące w szczególności zakaz jego dalszego dostarczania, wdrażania, utrzymywania, aktualizowania i wykorzystywania, obowiązek zastąpienia rozwiązania na koszt i ryzyko Wykonawcy, możliwość odmowy odbioru lub wstrzymania wynagrodzenia, a także zakwalifikowanie naruszenia jako istotnego naruszenia Umowy.

Art. 226 ust. 1 pkt 17 Pzp określa przesłankę odrzucenia oferty i sam w sobie nie wyznacza maksymalnego dopuszczalnego zakresu zobowiązań umownych ustanawianych przez Zamawiającego. Niemniej zakres § 4 ust. 6 pkt 1 jest szerszy od zakresu rekomendacji, z którym ustawodawca w Pzp wiąże obligatoryjną przesłankę odrzucenia oferty.

Z tego względu zasadne jest jednoznaczne wyjaśnienie, czy Zamawiający świadomie zamierza objąć skutkami określonymi w § 4 ust. 7–11 także rekomendacje, które nie stwierdzają negatywnego wpływu danego produktu ICT, usługi ICT lub procesu ICT na podstawowy interes bezpieczeństwa państwa.

Odpowiedź:

Odpowiedź na pytanie stanowi zmodyfikowany § 4 ppu jak niżej i tym samym odpowiedź na pytanie udzielona 17 września staje się nieaktualna.

Pytanie nr 8

Dotyczy § 4 ust. 7–9 Umowy – rozróżnienie skutków rekomendacji i decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka oraz termin wycofania rozwiązania

Czy Zamawiający potwierdza, że w zakresie korzystania z Systemu OTAGO właściwym podmiotem po stronie Zamawiającego, tj. Urząd Miasta Piekary Śląskie, jest podmiotem kluczowym albo podmiotem ważnym, o którym mowa w art. 67b ust. 1 pkt 1 KSC, do którego znajdują zastosowanie obowiązki określone w art. 67c KSC?

Niezależnie od powyższego, czy Zamawiający wyrazi zgodę na zmianę § 4 ust. 7–9 Umowy poprzez:

1. jednoznaczne rozróżnienie skutków rekomendacji wydanej na podstawie art. 33 ust. 4 KSC od skutków decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 KSC;
2. wskazanie, że obowiązki określone w § 4 ust. 9 powstają w przypadku faktycznego objęcia danego rozwiązania odpowiednią rekomendacją lub decyzją, a nie już w przypadku wystąpienia okoliczności, która jedynie może w przyszłości skutkować niezgodnością;
3. uwzględnienie – w zakresie, w jakim właściwym podmiotem krajowego systemu cyberbezpieczeństwa jest Urząd Miasta Piekary Śląskie – w przypadku rekomendacji procedury określonej w art. 33 ust. 5–8 KSC, w tym możliwości wniesienia zastrzeżeń oraz wyniku ich rozpatrzenia;

4. wskazanie, że w przypadku decyzji, o której mowa w art. 67b ust. 15 KSC, wydanej po zawarciu Umowy, sposób i termin wycofania rozwiązania będą ustalane z uwzględnieniem terminów i zasad wynikających z art. 67c KSC – w zakresie, w jakim przepis ten znajduje zastosowanie do właściwego podmiotu po stronie Zamawiającego;
5. dopuszczenie, do czasu wycofania rozwiązania objętego decyzją, jego naprawy, modernizacji, wymiany elementu lub aktualizacji w zakresie przewidzianym w art. 67c ust. 3 KSC;
6. zastąpienie terminu „nie dłuższego niż 30 dni roboczych” terminem ustalonym z uwzględnieniem treści i skutków odpowiedniej rekomendacji lub decyzji, obowiązujących przepisów prawa, zakresu koniecznych prac, dostępności rozwiązania zastępczego, zakresu wymaganej migracji i integracji, konieczności przeprowadzenia testów oraz zapewnienia ciągłości działania Systemu OTAGO?

W przypadku nieuwzględnienia powyższej zmiany prosimy o wskazanie obiektywnych przyczyn, dla których Zamawiający wymaga zaprzestania korzystania z rozwiązania oraz jego zastąpienia w terminie nie dłuższym niż 30 dni roboczych także w sytuacji, gdy rozwiązanie zostało zgodnie z prawem nabyte i było wykorzystywane przed wydaniem decyzji, mimo że – w przypadku spełnienia przesłanek stosowania art. 67c KSC – przepisy te przewidują możliwość jego dalszego czasowego użytkowania.

Uzasadnienie

§ 4 ust. 7–9 projektu Umowy przewiduje zasadniczo jednakowe konsekwencje zarówno dla objęcia rozwiązania rekomendacją, o której mowa w art. 33 ust. 4 KSC, jak i decyzją w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 KSC.

Tymczasem KSC przewiduje dla tych dwóch instrumentów odmienne mechanizmy i skutki prawne.

W odniesieniu do rekomendacji art. 33 ust. 5 KSC przewiduje możliwość wniesienia przez podmiot krajowego systemu cyberbezpieczeństwa zastrzeżeń do rekomendacji dotyczących stosowania produktów ICT lub usług ICT, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, w terminie 14 dni od dnia publikacji rekomendacji.

Zgodnie z art. 33 ust. 6 KSC Pełnomocnik odnosi się do zastrzeżeń i podtrzymuje rekomendację albo wydaje zmienioną rekomendację. Art. 33 ust. 7–8 KSC reguluje natomiast dalsze następstwa sposobu uwzględnienia rekomendacji, w tym możliwość poinformowania organu sprawującego nadzór w razie jej nieuwzględnienia.

Przepisy te nie ustanawiają generalnego obowiązku zaprzestania korzystania z każdego rozwiązania objętego rekomendacją i jego wymiany w terminie 30 dni.

Odmienne mechanizmy ustawodawca przewidział w odniesieniu do decyzji, o której mowa w art. 67b ust. 15 KSC.

Zgodnie z art. 67c ust. 1 pkt 1 KSC podmioty, o których mowa w art. 67b ust. 1 KSC, nie wprowadzają do użytkowania rozwiązań objętych decyzją, natomiast zgodnie z art. 67c ust. 1 pkt 2 KSC rozwiązania już użytkowane wycofują nie później niż w terminie 7 lat od dnia ogłoszenia decyzji w Monitorze Polskim.

Oznacza to, że ustawodawca wyraźnie rozróżnia zakaz wprowadzania do użytkowania nowych rozwiązań od procesu wycofywania rozwiązań już użytkowanych. Okoliczności tej nie zmienia wynikająca z art. 67b ust. 18 KSC natychmiastowa wykonalność decyzji.

Ponadto zgodnie z art. 67c ust. 3 KSC do czasu wycofania dopuszczalne jest użytkowanie dotychczas posiadanych produktów ICT, usług ICT i konkretnych procesów ICT w zakresie objętym decyzją w celu ich naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonania niezbędnych napraw awarii lub uszkodzeń.

Dodatkowo art. 67c ust. 5 KSC przewiduje, że w przypadku gdy podmiot, o którym mowa w art. 67b ust. 1 KSC, do którego stosuje się Pzp, nabył w drodze zamówienia publicznego, przed dniem ogłoszenia decyzji, produkt ICT, usługę ICT lub proces ICT określone następnie w tej decyzji, może – w przypadku spełnienia przesłanek tego przepisu – korzystać z nich co do zasady nie dłużej niż 7 lat od dnia ogłoszenia decyzji. Termin ten ma charakter terminu maksymalnego i nie oznacza obowiązku korzystania z rozwiązania przez pełne 7 lat. Wskazuje jednak, że KSC nie ustanawia generalnego obowiązku wycofania prawidłowo nabytego i już użytkowanego rozwiązania w terminie 30 dni od ogłoszenia decyzji.

Na tym tle § 4 ust. 7–9 projektu Umowy ustanawia mechanizm istotnie bardziej rygorystyczny, przewidując w szczególności:

- zakaz utrzymywania i aktualizowania rozwiązania;
- obowiązek zaprzestania jego wykorzystywania;
- obowiązek przedstawienia rozwiązania zastępczego;
- obowiązek dokonania wymiany, rekonfiguracji lub migracji;
- wykonanie wszystkich powyższych czynności w terminie jednostronnie wyznaczonym przez Zamawiającego, nie dłuższym niż 30 dni roboczych.

Jednocześnie § 4 ust. 8 odnosi się do „każdej okoliczności, która może skutkować niezgodnością”, zaś § 4 ust. 9 uruchamia opisane wyżej obowiązki już w przypadku „wystąpienia okoliczności, o których mowa w ust. 8”.

Literalne brzmienie tych postanowień może zatem prowadzić do powstania obowiązku zaprzestania korzystania z rozwiązania, przedstawienia rozwiązania zastępczego oraz dokonania wymiany lub migracji nawet w sytuacji, w której doszło jedynie do wystąpienia okoliczności mogącej potencjalnie skutkować niezgodnością, lecz rozwiązanie nie zostało jeszcze faktycznie objęte odpowiednią rekomendacją albo decyzją.

Dodatkowo sformułowanie „w terminie wyznaczonym przez Zamawiającego, nie dłuższym niż 30 dni roboczych” nie określa żadnego terminu minimalnego. Zamawiający może zatem literalnie wyznaczyć termin istotnie krótszy niż 30 dni, niezależnie od rzeczywistego zakresu technicznego koniecznych prac.

Zastąpienie rozwiązania ICT może natomiast wymagać w szczególności:

- pozyskania nowego produktu lub usługi;
- uzyskania odpowiednich licencji;
- konfiguracji lub rekonfiguracji środowiska;

- wykonania integracji;
- migracji danych;
- dostosowania pozostałych komponentów Systemu;
- przeprowadzenia prac programistycznych;
- testów bezpieczeństwa;
- testów wydajnościowych;
- testów odbiorowych;
- zapewnienia ciągłości działania Systemu OTAGO.

Z tego względu maksymalny 30-dniowy termin, przy jednoczesnym braku terminu minimalnego i braku powiązania terminu z rzeczywistym zakresem koniecznych prac, może okazać się obiektywnie niewystarczający.

Odpowiedź:

Odpowiedź na pytanie stanowi zmodyfikowany § 4 ppu jak niżej

Pytanie nr 9

Dotyczy § 4 ust. 9 w zw. z § 14 ust. 2 pkt 2, 3 i 5 Umowy – koszt i ryzyko zastąpienia rozwiązania wskutek rekomendacji lub decyzji wydanej po zawarciu Umowy

Czy Zamawiający wyrazi zgodę na zmianę § 4 ust. 9 Umowy w taki sposób, aby obowiązek wykonania wymaganych czynności w całości na koszt i ryzyko Wykonawcy dotyczył przypadków, gdy niezgodność wynika z okoliczności leżących po stronie Wykonawcy, w szczególności gdy Wykonawca zaoferował, wdrożył lub wykorzystywał rozwiązanie pomimo tego, że w chwili dokonania tych czynności było ono już objęte odpowiednią rekomendacją albo decyzją?

Jednocześnie czy w przypadku wydania odpowiedniej rekomendacji albo decyzji dopiero po zawarciu Umowy, dotyczącej rozwiązania prawidłowo zaoferowanego i zgodnie z prawem wykorzystywanego, Zamawiający wyrazi zgodę na wprowadzenie klauzuli przeglądowej przewidującej – odpowiednio do rzeczywistych skutków danego zdarzenia – możliwość zmiany:

1. zakresu lub sposobu realizacji Umowy;
2. stosowanych produktów ICT, usług ICT lub procesów ICT;
3. terminów lub harmonogramu wykonania;
4. wynagrodzenia Wykonawcy – w zakresie uzasadnionych i udokumentowanych dodatkowych kosztów pozostających w bezpośrednim związku z koniecznością zastąpienia rozwiązania?

Wykonawca wnosi o wprowadzenie odpowiedniego mechanizmu zmiany Umowy zgodnego z art. 455 ust. 1 pkt 1 Pzp, tj. sformułowanego w sposób jasny, precyzyjny i jednoznaczny, określającego rodzaj, zakres i warunki zmiany oraz nieprowadzącego do zmiany ogólnego charakteru Umowy.

Uzasadnienie

Zgodnie z § 4 ust. 9 projektu Umowy Wykonawca jest obowiązany wykonać wszystkie czynności związane z zaprzestaniem wykorzystywania rozwiązania, przedstawieniem rozwiązania zastępczego oraz jego wymianą, rekonfiguracją, migracją lub wykonaniem innych czynności niezbędnych do zapewnienia zgodności realizacji Umowy – „na własny koszt i ryzyko”.

Postanowienie to nie rozróżnia sytuacji, w której określony produkt ICT, usługa ICT lub proces ICT był objęty odpowiednią rekomendacją albo decyzją już w chwili jego zaoferowania, wdrożenia lub wykorzystania, od sytuacji, w której rekomendacja albo decyzja zostanie wydana dopiero po zawarciu Umowy, a korzystanie z rozwiązania było wcześniej zgodne z prawem i wymaganiami Zamawiającego.

W pierwszym przypadku obciążenie Wykonawcy skutkami zastosowania rozwiązania już niedopuszczalnego może znajdować uzasadnienie.

W drugim przypadku konieczność zastąpienia rozwiązania wynikałaby natomiast ze zdarzenia przyszłego, którego wystąpienie, treść i moment pozostają poza kontrolą Wykonawcy oraz którego skutków technicznych i ekonomicznych Wykonawca nie jest w stanie precyzyjnie określić na etapie sporządzania oferty.

Ma to szczególne znaczenie w niniejszym postępowaniu, którego przedmiotem jest asysta techniczna i konserwacja istniejącego Systemu OTAGO. Obowiązek całkowitej wymiany, rekonfiguracji lub migracji rozwiązania może wiązać się z pracami i kosztami jakościowo i wartościowo odbiegającymi od typowego zakresu usług asysty technicznej i konserwacji.

Koszty te mogą obejmować w szczególności:

- nabycie nowych produktów lub usług;
- nabycie nowych licencji;
- integrację;
- migrację danych;
- konfigurację i rekonfigurację;
- prace programistyczne;
- zmianę lub dostosowanie innych komponentów Systemu;
- udział i usługi podmiotów trzecich;
- wykonanie testów;
- wdrożenie nowego rozwiązania;
- zapewnienie ciągłości działania Systemu.

Zgodnie z art. 99 ust. 1 Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. Z kolei art. 16 pkt 3 Pzp nakazuje Zamawiającemu przygotowanie i przeprowadzenie postępowania w sposób proporcjonalny.

Nałożenie na Wykonawcę pełnego ryzyka ekonomicznego skutków przyszłej rekomendacji albo decyzji powoduje konieczność uwzględnienia tego ryzyka w kalkulacji ceny już na etapie sporządzania oferty, mimo że nie jest wówczas możliwe określenie:

- czy takie zdarzenie w ogóle wystąpi;
- kiedy wystąpi;
- którego rozwiązania będzie dotyczyło;
- jaki będzie zakres wymaganej zmiany;
- czy i na jakich warunkach dostępne będzie rozwiązanie zastępcze;
- jaki będzie koszt jego nabycia i wdrożenia;
- jaki będzie zakres koniecznych prac migracyjnych i integracyjnych.

Zasadne jest zatem rozróżnienie ryzyka wynikającego z okoliczności leżących po stronie Wykonawcy od ryzyka wynikającego z rekomendacji lub decyzji wydanej dopiero po zawarciu Umowy, której wydanie, treść i moment pozostają poza kontrolą Wykonawcy.

Ogólne podstawy zmiany Umowy przewidziane w § 14 ust. 2 pkt 2, 3 i 5 nie określają w sposób jasny, precyzyjny i jednoznaczny rodzaju i zakresu dopuszczalnej zmiany wynagrodzenia, terminów oraz zakresu świadczenia w przypadku wydania po zawarciu Umowy rekomendacji albo decyzji, o których mowa w § 4 ust. 6.

Art. 455 ust. 1 pkt 1 Pzp pozwala Zamawiającemu przewidzieć już w dokumentach zamówienia jasne, precyzyjne i jednoznaczne postanowienia umowne określające rodzaj, zakres oraz warunki przyszłych zmian Umowy, w tym zasady zmiany wysokości ceny, pod warunkiem że zmiany nie prowadzą do zmiany ogólnego charakteru Umowy.

Przepis ten nie nakłada na Zamawiającego obowiązku ustanowienia takiej klauzuli, ale umożliwia uregulowanie już na etapie postępowania skutków przyszłego, niemożliwego obecnie do precyzyjnego oszacowania zdarzenia.

Odpowiedź:

Odpowiedź na pytanie stanowi zmodyfikowany § 4 ppu jak niżej

Pytanie nr 10

Dotyczy § 4 ust. 8, 10 i 11 Umowy /moment powstania obowiązku informacyjnego oraz proporcjonalność konsekwencji naruszenia/

Czy Zamawiający wyrazi zgodę na doprecyzowanie § 4 ust. 8 Umowy poprzez wskazanie, że w przypadku objęcia rozwiązania rekomendacją albo decyzją termin 2 dni roboczych biegnie od chwili powzięcia przez Wykonawcę informacji o oficjalnej publikacji rekomendacji albo ogłoszeniu decyzji?

Jednocześnie, mając na uwadze zasadę proporcjonalności wynikającą z art. 16 pkt 3 Pzp, czy Zamawiający wyrazi zgodę na zmianę § 4 ust. 10–11 Umowy poprzez:

1. wskazanie, że odmowa odbioru całości przedmiotu Umowy jest dopuszczalna wyłącznie w przypadku, gdy charakter lub zakres stwierdzonej niezgodności obiektywnie uniemożliwia odbiór całości świadczenia;
2. odstąpienie od automatycznego kwalifikowania każdego niewykonania albo nienależytego wykonania obowiązków określonych w § 4 ust. 6–10 jako istotnego naruszenia Umowy;
3. uzależnienie prawa odstąpienia albo wypowiedzenia Umowy od rzeczywiście istotnego charakteru naruszenia, ocenianego z uwzględnieniem jego rodzaju, zakresu, skutków oraz wpływu na cyberbezpieczeństwo, zgodność z prawem i możliwość prawidłowego wykonywania Umowy;
4. wprowadzenie, co do zasady, obowiązku uprzedniego wyznaczenia Wykonawcy odpowiedniego dodatkowego terminu na usunięcie naruszenia, z wyjątkiem przypadku, gdy dalsze wykonywanie Umowy jest niedopuszczalne na podstawie bezwzględnie obowiązujących przepisów prawa albo charakter naruszenia powoduje, że jego usunięcie nie jest możliwe?

Uzasadnienie

Zgodnie z § 4 ust. 8 projektu Umowy Wykonawca jest zobowiązany niezwłocznie, nie później niż w terminie 2 dni roboczych od powzięcia informacji, poinformować Zamawiającego na piśmie o każdej okoliczności, która może skutkować niezgodnością przedmiotu Umowy z § 4 ust. 6 lub 7.

W szczególności obowiązek ten dotyczy:

1. objęcia rozwiązania wykorzystywanego przy realizacji Umowy rekomendacją albo decyzją, o których mowa w § 4 ust. 6;
2. ujawnienia, że rozwiązanie oferowane albo wykorzystywane przy realizacji Umowy jest objęte zakresem rekomendacji albo decyzji, o których mowa w § 4 ust. 6.

Zgodnie z art. 33 ust. 4c KSC rekomendacje, o których mowa w art. 33 ust. 4 KSC, a także informacje o ich zmianie lub odwołaniu, Pełnomocnik publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej.

Natomiast zgodnie z art. 67b ust. 17 KSC decyzja w sprawie uznania dostawcy za dostawcę wysokiego ryzyka jest ogłaszana w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz publikowana na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra.

W celu uniknięcia wątpliwości interpretacyjnych dotyczących rozpoczęcia biegu bardzo krótkiego, dwudniowego terminu informacyjnego zasadne jest jednoznaczne określenie w Umowie zdarzenia, z którym związane jest rozpoczęcie biegu tego terminu.

Niezależnie od powyższego § 4 ust. 10 przewiduje, że do czasu usunięcia niezgodności Zamawiający ma prawo:

1. odmówić odbioru całości lub części przedmiotu Umowy;
2. wstrzymać zapłatę wynagrodzenia w części dotyczącej świadczenia dotkniętego niezgodnością;
3. żądać przedstawienia planu działań naprawczych wraz z harmonogramem.

Jednocześnie zgodnie z § 4 ust. 11 każde niewykonanie albo nienależyte wykonanie obowiązków określonych w § 4 ust. 6–10 stanowi „istotne naruszenie Umowy” i uprawnia Zamawiającego do:

1. odstąpienia od Umowy w całości albo w części w terminie 100 dni od dnia powzięcia wiadomości o naruszeniu albo
2. wypowiedzenia Umowy ze skutkiem natychmiastowym w zakresie świadczeń niewykonanych.

§ 4 ust. 11 nie różnicuje charakteru, przyczyny, zakresu ani skutków naruszenia.

W rezultacie również nieznaczne przekroczenie terminu informacyjnego określonego w § 4 ust. 8 albo inne uchybienie o charakterze formalnym, niemające wpływu na cyberbezpieczeństwo, zgodność Systemu z prawem ani możliwość jego dalszego prawidłowego funkcjonowania, jest literalnie kwalifikowane jako istotne naruszenie Umowy.

Takie naruszenie może następnie stanowić podstawę zastosowania najdalej idących sankcji kontraktowych – odstąpienia od Umowy albo jej wypowiedzenia ze skutkiem natychmiastowym.

Ponadto § 4 ust. 10 pkt 1 pozwala Zamawiającemu odmówić odbioru całości lub części przedmiotu Umowy niezależnie od zakresu stwierdzonej niezgodności.

Tymczasem § 4 ust. 10 pkt 2 prawidłowo ogranicza możliwość wstrzymania zapłaty wynagrodzenia do części dotyczącej świadczenia dotkniętego niezgodnością.

Analogiczny związek pomiędzy zakresem stwierdzonej niezgodności a zakresem zastosowanego środka powinien zostać zachowany również w przypadku odmowy odbioru.

Mając na uwadze zasadę proporcjonalności wynikającą z art. 16 pkt 3 Pzp, zasadne jest również rozróżnienie naruszeń rzeczywiście istotnych od uchybień nieistotnych oraz, co do zasady, zapewnienie Wykonawcy możliwości usunięcia naruszenia przed zastosowaniem najdalej idących sankcji kontraktowych.

Wyjątek powinny stanowić sytuacje, w których dalsze wykonywanie Umowy jest niedopuszczalne na podstawie bezwzględnie obowiązujących przepisów prawa albo naruszenie ze swej natury nie może zostać usunięte.

Odpowiedź:

Odpowiedź na pytanie stanowi zmodyfikowany § 4 ppu:

§ 4 PROJEKTOWANE POSTANOWIENIA UMOWNE

Zamawiający zmienia treść § 4 ppu, w taki sposób, że usuwa dotychczasową treść, a w jej miejsce wprowadzona zostaje następująca treść:

§ 4. Ogólne zobowiązania Wykonawcy i Zamawiającego

1. Wykonawca zobowiązuje się realizować Umowę z należytą starannością uwzględniającą zawodowy charakter prowadzonej działalności, zgodnie z zasadami wiedzy technicznej, wymaganiami cyberbezpieczeństwa, postanowieniami Umowy oraz przepisami prawa mającymi zastosowanie do przedmiotu Umowy.
2. Wykonawca zobowiązuje się współpracować z Zamawiającym w zakresie niezbędnym do prawidłowego wykonywania Umowy oraz realizacji przez Zamawiającego i Urząd Miasta Piekary Śląskie obowiązków w zakresie cyberbezpieczeństwa. W zakresie związanym z przedmiotem Umowy Wykonawca, na żądanie Zamawiającego, przekazuje informacje niezbędne do oceny ryzyka dotyczącego wykorzystywanych produktów ICT, usług ICT, procesów ICT i ich dostawców, a także niezwłocznie informuje o znanych mu podatnościach, cyberzagrożeniach lub zdarzeniach mogących istotnie wpłynąć na poufność, integralność, dostępność lub autentyczność Systemu OTAGO albo danych Zamawiającego.

3. Zamawiający zobowiązuje się do współpracy i współdziałania z Wykonawcą w zakresie niezbędnym do prawidłowego wykonania Umowy, w szczególności do:
 - 1) udostępnienia osobom wskazanym przez Wykonawcę zgodnie z § 7 ust. 2 możliwości zdalnego dostępu do zasobów, na których zainstalowany jest System OTAGO, za pośrednictwem bezpiecznego, szyfrowanego kanału telekomunikacyjnego i na zasadach określonych w Załącznikach nr 3 i 4 do Umowy,
 - 2) przekazywania Wykonawcy danych i informacji pozostających w dyspozycji Zamawiającego, niezbędnych do realizacji zobowiązań określonych w Umowie,
 - 3) wyznaczenia do współpracy osób posiadających odpowiednie upoważnienia i kompetencje.
4. Jeżeli niewykonanie przez Zamawiającego obowiązku określonego w ust. 3 pkt 1 lub 2 uniemożliwia albo rzeczywiście opóźnia wykonanie konkretnego zobowiązania Wykonawcy, termin wykonania tego zobowiązania ulega przedłużeniu wyłącznie o okres pozostawania tej przeszkody w bezpośrednim związku z opóźnieniem. Wykonawca jest obowiązany poinformować Zamawiającego o przeszkodzie niezwłocznie, nie później niż w terminie 2 Dni Roboczych od jej stwierdzenia, wskazać jej wpływ na realizację Umowy oraz podjąć dostępne działania ograniczające skutki opóźnienia.
5. Wykonawca oraz osoby, którymi posługuje się przy wykonywaniu Umowy, są obowiązani przestrzegać zasad określonych w Załącznikach nr 3 i 4 do Umowy, w szczególności zasady minimalnych uprawnień, korzystania wyłącznie z imiennych kont, ochrony danych uwierzytelniających oraz poleceń Zamawiającego dotyczących bezpieczeństwa dostępu zdalnego. Zamawiający może niezwłocznie ograniczyć albo zablokować dostęp, jeżeli jest to uzasadnione ochroną systemów lub danych. Takie działanie nie stanowi naruszenia Umowy przez Zamawiającego.
6. Wykonawca oświadcza, że na dzień złożenia oferty oraz na dzień zawarcia Umowy przedmiot Umowy, w zakresie rozwiązań objętych ofertą, dostarczanych, wdrażanych, wprowadzanych do użytkowania lub wykorzystywanych przez Wykonawcę przy realizacji Umowy, nie obejmuje:
 - 1) produktu ICT, usługi ICT ani procesu ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa, o której mowa w art. 226 ust. 1 pkt 17 ustawy - Prawo zamówień publicznych,
 - 2) typu produktu ICT, rodzaju usługi ICT ani konkretnego procesu ICT objętych decyzją w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy o krajowym systemie

cyberbezpieczeństwa oraz w art. 226 ust. 1 pkt 19 ustawy - Prawo zamówień publicznych.

7. Przez cały okres realizacji Umowy Wykonawca jest obowiązany:
 - 1) monitorować oficjalne publikacje rekomendacji, ich zmian i odwołań, o których mowa w art. 33 ust. 4c ustawy o krajowym systemie cyberbezpieczeństwa, oraz decyzji i list, o których mowa w art. 67b ust. 17 i art. 67f tej ustawy, w zakresie produktów ICT, usług ICT, procesów ICT i dostawców związanych z realizacją Umowy,
 - 2) nie dostarczać, nie wdrażać ani nie wprowadzać do użytkowania nowych rozwiązań, o których mowa w ust. 6, po opublikowaniu właściwej rekomendacji lub ogłoszeniu właściwej decyzji,
 - 3) nie zastępować rozwiązania wykorzystywanego przy realizacji Umowy innym produktem ICT, usługą ICT lub procesem ICT bez uprzedniego sprawdzenia go w zakresie, o którym mowa w pkt 1, oraz bez zgody Zamawiającego, jeżeli zastąpienie może wpływać na bezpieczeństwo, interoperacyjność, funkcjonalność lub koszty eksploatacji Systemu OTAGO,
 - 4) w odniesieniu do rozwiązań już użytkowanych stosować się do procedury określonej w ust. 8-10, z uwzględnieniem art. 33 ust. 5-8 oraz art. 67c ustawy o krajowym systemie cyberbezpieczeństwa.
8. Wykonawca poinformuje Zamawiającego na piśmie lub w postaci elektronicznej:
 - 1) niezwłocznie, nie później niż w terminie 2 Dni Roboczych od dnia, w którym powziął lub przy zachowaniu należytej staranności powinien był powziąć informację o oficjalnym opublikowaniu rekomendacji albo ogłoszeniu decyzji, o których mowa w ust. 6, jeżeli mogą one obejmować rozwiązanie dostarczane, utrzymywane lub wykorzystywane przy realizacji Umowy,
 - 2) niezwłocznie, nie później niż w terminie 3 Dni Roboczych od powzięcia informacji o wszczęciu postępowania, o którym mowa w art. 67b ustawy o krajowym systemie cyberbezpieczeństwa, wobec Wykonawcy, podmiotu z jego grupy kapitałowej, podwykonawcy albo dostawcy rozwiązania wykorzystywanego przy realizacji Umowy, jeżeli okoliczność ta może istotnie wpływać na bezpieczeństwo lub ciągłość realizacji Umowy,
 - 3) niezwłocznie po ujawnieniu, że złożone oświadczenie, o którym mowa w ust. 6, było nieprawdziwe albo stało się nieaktualne.
9. Informacja, o jakiej mowa w ust.8, powinna co najmniej identyfikować dane rozwiązanie i jego dostawcę, wskazywać podstawę i zakres możliwego objęcia rekomendacją lub decyzją, funkcje i środowiska Zamawiającego, na które zdarzenie może oddziaływać, przewidywane skutki oraz możliwe działania ograniczające ryzyko. Samo wszczęcie postępowania lub wystąpienie okoliczności mogącej prowadzić do wydania rekomendacji albo decyzji nie

uruchamia automatycznie obowiązku wymiany rozwiązania, lecz uprawnia Zamawiającego do żądania analizy ryzyka i działań zabezpieczających.

10. W przypadku objęcia rozwiązania wykorzystywanego przy realizacji Umowy rekomendacją albo decyzją, o których mowa w ust. 6, Strony stosują następującą procedurę:

- 1) Wykonawca niezwłocznie wstrzyma jego nowe wdrożenia i rozszerzenia oraz podejmie uzgodnione z Zamawiającym działania tymczasowe ograniczające ryzyko, Zamawiający może nakazać natychmiastowe zawieszenie określonego sposobu używania rozwiązania, jeżeli wymagają tego bezwzględnie obowiązujące przepisy prawa albo istnieje bezpośrednie i poważne zagrożenie dla bezpieczeństwa systemów, danych lub ciągłości realizacji zadań publicznych,
- 2) w terminie 5 Dni Roboczych od przekazania informacji, o której mowa w ust. 8 pkt 1, Wykonawca przedstawi analizę wpływu oraz plan postępowania zawierający co najmniej: zakres dotkniętych komponentów i funkcji, ocenę ryzyka, warianty dalszego działania, opis rozwiązania zastępczego, zakres migracji i integracji, wymagane testy, sposób zabezpieczenia danych i ciągłości działania, harmonogram, zasoby, zależności oraz wyszczególnienie kosztów,
- 3) Zamawiający, po analizie planu, wyznaczy sposób i termin wykonania działań, kierując się treścią rekomendacji lub decyzji, obowiązującymi przepisami, wynikiem oceny ryzyka, zakresem technicznym prac, dostępnością rozwiązania zastępczego, koniecznością migracji i testów oraz potrzebą zachowania ciągłości działania, termin nie może wykraczać poza termin dopuszczalny prawem,
- 4) w przypadku rekomendacji Zamawiający zachowuje prawo wniesienia zastrzeżeń w trybie art. 33 ust. 5 ustawy o krajowym systemie cyberbezpieczeństwa, a Wykonawca przekaze informacje potrzebne do ich przygotowania w terminie wskazanym przez Zamawiającego, nie krótszym niż 2 Dni Robocze, wniesienie zastrzeżeń nie wstrzymuje działań zabezpieczających wskazanych przez Zamawiającego,
- 5) w przypadku decyzji, o której mowa w art. 67b ust. 15 ustawy o krajowym systemie cyberbezpieczeństwa, sposób dalszego czasowego używania oraz wycofania rozwiązania ustala się z uwzględnieniem art. 67c tej ustawy, do czasu wycofania naprawa, modernizacja, wymiana elementu lub aktualizacja rozwiązania może następować wyłącznie w granicach dopuszczonych prawem, gdy jest niezbędna dla zapewnienia odpowiedniej jakości i ciągłości usług, oraz po akceptacji Zamawiającego.

11. Koszty i zmiany Umowy związane z wykonaniem ust. 9 i 10 rozlicza się według następujących zasad:

- 1) Wykonawca ponosi w całości koszty wykonania obowiązków informacyjnych, analizy wpływu, przygotowania planu oraz działań zabezpieczających mieszczących się w przedmiocie Umowy,
 - 2) Wykonawca ponosi w całości koszty usunięcia niezgodności, w tym wymiany, rekonfiguracji, migracji i testów, jeżeli niezgodność istniała w dniu złożenia oferty lub zawarcia Umowy, wynika z nieprawdziwości oświadczenia z ust. 6, naruszenia ust. 7 albo działania lub zaniechania Wykonawcy, jego podwykonawcy lub innego podmiotu, za który Wykonawca odpowiada,
 - 3) jeżeli rekomendacja albo decyzja została opublikowana lub ogłoszona po zawarciu Umowy i konieczność dodatkowych prac nie wynika z okoliczności określonych w pkt 2, Wykonawca w pierwszej kolejności wykorzysta czynności objęte wynagrodzeniem ryczałtowym oraz niewykorzystane Roboczogodziny, o których mowa w § 2 ust. 4,
 - 4) w zakresie, w jakim działania konieczne do zachowania zgodności wykraczają poza zakres określony w pkt 1-3, dopuszcza się zmianę zakresu lub sposobu świadczenia, dotkniętych terminów, zastosowanych rozwiązań oraz wynagrodzenia, pod warunkiem zawarcia aneksu i wykazania zgodności zmiany z art. 455 ustawy - Prawo zamówień publicznych; dodatkowe wynagrodzenie może obejmować wyłącznie zaakceptowaną przez Zamawiającego liczbę niezbędnych Roboczogodzin, rozliczanych według stawki za Roboczogodzinę wskazanej w ofercie, oraz udokumentowane i niezbędne koszty nabycia licencji lub usług podmiotów trzecich, bez dodatkowej marży Wykonawcy a łączny wzrost wynagrodzenia na tej podstawie nie może przekroczyć 10% pierwotnego maksymalnego wynagrodzenia brutto określonego w § 8 ust. 1,
 - 5) zmiana nie może modyfikować ogólnego charakteru Umowy i może dotyczyć wyłącznie świadczeń pozostających w bezpośrednim związku z rekomendacją (art.33 ust.4 uKSC) albo decyzją (art.67b uKSC) a zmniejszenie zakresu świadczeń powoduje odpowiednie zmniejszenie wynagrodzenia na podstawie cen określonych w Załączniku nr 1 albo, gdy nie jest to możliwe, na podstawie udokumentowanego udziału danego świadczenia w cenie,
 - 6) jeżeli zgodna z prawem i technicznie uzasadniona zmiana nie jest możliwa w ramach Umowy albo przekracza limit określony w pkt 4, Zamawiający może odstąpić od Umowy w części obejmującej dotknięte świadczenia, a gdy nie jest możliwe dalsze wykonywanie pozostałej części Umowy – odstąpić od Umowy w całości, bez obowiązku zapłaty odszkodowania lub utraconych korzyści.
12. W przypadku, o jakim mowa w ust. 11 pkt 6 Wykonawcy przysługuje wyłącznie wynagrodzenie za świadczenia prawidłowo wykonane do dnia zakończenia ich

realizacji, a Zamawiający może wykonać prawo do odstąpienia od Umowy w części lub całości w terminie do 7 dni od stwierdzenia podstaw do odstąpienia.

13. Do czasu zakończenia działań określonych w ust. 10 Zamawiający może, w zakresie adekwatnym do rodzaju i skutków niezgodności:

- 1) odmówić odbioru części świadczenia dotkniętej niezgodnością, a odbioru całości - wyłącznie wtedy, gdy niezgodność obiektywnie uniemożliwia bezpieczne i zgodne z prawem korzystanie z całości świadczenia,
- 2) żądać aktualizacji planu działań, dodatkowych wyjaśnień, dowodów wykonania działań oraz przeprowadzenia testów potwierdzających bezpieczeństwo i prawidłowość rozwiązania,
- 3) ograniczyć lub zawiesić dostęp Wykonawcy albo używanie rozwiązania, jeżeli jest to konieczne dla ochrony systemów, danych lub ciągłości realizacji zadań publicznych.

Pozostałe zmiany SWZ:

ZMIANA NR 1 - ROZDZIAŁ IV. OPIS PRZEDMIOTU ZAMÓWIENIA

Dotychczasowa treść ust. 4 zostaje usunięta, a w jej miejsce zostaje wprowadzona następująca treść:

4. Zamawiający wymaga, aby przedmiot Umowy, w zakresie rozwiązań objętych ofertą, dostarczanych, wdrażanych, wprowadzanych do użytkowania lub wykorzystywanych przez Wykonawcę przy realizacji Umowy, nie obejmował:
 - 1) produktu ICT, usługi ICT ani procesu ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa, o której mowa w art. 226 ust. 1 pkt 17 ustawy - Prawo zamówień publicznych,
 - 2) typu produktu ICT, rodzaju usługi ICT ani konkretnego procesu ICT objętych decyzją w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy o krajowym systemie cyberbezpieczeństwa oraz w art. 226 ust. 1 pkt 19 ustawy - Prawo zamówień publicznych.

ZMIANA NR 2 - ROZDZIAŁ XII. TERMIN ZWIĄZANIA OFERTĄ

Dotychczasowa treść zostaje usunięta, a w jej miejsce zostaje wprowadzona następująca treść:

Wykonawca składający ofertę jest nią związany od dnia upływu terminu składania ofert do dnia **23 października 2026 r.**

ZMIANA NR 3 – Rozdział XVI. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

Dotychczasowa treść pkt 1 zostaje usunięta, a w jej miejsce zostaje wprowadzona następująca treść:

1. Ofertę z załącznikami należy złożyć za pośrednictwem platformy przetargowej w terminie

do godziny 09:00 w dniu 24 września 2026 r.

ZMIANA NR 4 – Rozdział XX. TERMIN OTWARCIA OFERT

Dotychczasowa treść pkt 1 zostaje usunięta, a w jej miejsce zostaje wprowadzona następująca treść:

1. Otwarcie ofert nastąpi

o godzinie 09:15 w dniu 24 września 2026 r.

na komputerze zamawiającego na platformie przetargowej.

Ponadto Zamawiający modyfikuje formularz oferty - załącznik nr 1 do swz.(w załączeniu), w zakresie ust. 5 pkt 2 lit. a i b.

Przewodnicząca komisji przetargowej



Dokument podpisany elektronicznie przez:
Agnieszka Magdalena Strychalska
Data podpisu:
2026.09.21 13:53:11.