

Katowice 15 stycznia 2026r.

Zamawiający publikuje otrzymane pytania wraz ze swoją odpowiedzią.

PYTANIA DO TREŚCI ZAPYTANIA OFERTOWEGO

Pytanie 1

na podstawie postanowienia pkt. 9.2 ppkt. 4 Zapytania Ofertowego z dnia 22 grudnia 2025 r. zwracam się z prośbą o zmianę treści Zapytania Ofertowego, tj.

wykreślenie wymogu posiadania certyfikatu ISO/IEC 27701 z warunków udziału w postępowaniu.

Uzasadnienie:

Niniejsze uzasadnienie przedstawia argumenty przemawiające za wykreśleniem z warunków udziału w postępowaniu wymogu posiadania certyfikatu ISO/IEC 27701, przy jednoczesnym pozostawieniu wymogów certyfikacji ISO/IEC 27001 (dla obszaru świadczenia usług SOC/monitorowania cyberbezpieczeństwa lub usług pokrewnych) oraz ISO 22301.

1) Brak proporcjonalności warunku do przedmiotu zamówienia (SOC)

Warunki udziału w postępowaniu powinny być określone w sposób proporcjonalny do przedmiotu zamówienia oraz umożliwiające ocenę zdolności wykonawcy do należytego wykonania zamówienia. Wymóg ISO/IEC 27701, przy jednoczesnym wymaganiu ISO/IEC 27001 oraz ISO 22301, może stanowić warunek ponad poziom niezbędny do weryfikacji zdolności wykonawcy do świadczenia usługi SOC (monitorowanie, analiza zdarzeń, obsługa incydentów, zarządzanie ryzykiem, nadzór nad dostawcami, utrzymanie ciągłości działania).

2) ISO/IEC 27001 obejmuje kluczowe wymagania istotne dla ochrony danych (w tym osobowych) oraz zgodności prawnej

Certyfikat ISO/IEC 27001 (ISMS) – jako wynik niezależnej oceny zgodności – obiektywnie potwierdza wdrożenie i skuteczność systemowego podejścia do bezpieczeństwa informacji. Obejmuje ono m.in. identyfikację wymagań prawnych i ich uwzględnienie w systemie zarządzania, zarządzanie ryzykiem, dobór i utrzymanie zabezpieczeń, obsługę incydentów oraz kontrolę dostępu.

W szczególności, w strukturze ISO/IEC 27001 znajdują się wymagania i zabezpieczenia związane z: zrozumieniem potrzeb i oczekiwań stron zainteresowanych (w tym wymagań prawnych i regulacyjnych), oceną ryzyka i postępowaniem z ryzykiem oraz doбором środków zaradczych, identyfikacją obowiązujących przepisów i zobowiązań, prywatnością i ochroną danych osobowych, klasyfikacją informacji, kontrolą dostępu, bezpieczeństwem w relacjach z dostawcami, zarządzaniem bezpieczeństwem w trakcie incydentów oraz zapewnieniem ciągłości działania i dostępności informacji. Z perspektywy przedmiotu zamówienia (SOC), certyfikacja ISO/IEC 27001 z zakresem obejmującym usługi SOC jest wystarczającym i adekwatnym potwierdzeniem dojrzałości procesowej oraz organizacyjno-technicznej w zakresie bezpieczeństwa informacji, w tym danych osobowych przetwarzanych w ramach realizacji usługi.

3) Ochrona danych osobowych wynika przede wszystkim z obowiązku prawnego (RODO), a nie z dobrowolnej certyfikacji

Ochrona danych osobowych jest obowiązkiem wynikającym z przepisów RODO, w szczególności w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa

adekwatny do ryzyka. Podejście oparte na ryzyku (risk-based approach) oraz zasada adekwatności zabezpieczeń są zbieżne z metodyką zarządzania bezpieczeństwem informacji realizowaną w ramach ISO/IEC 27001.

4) ISO/IEC 27701 ma charakter rozszerzenia PIMS i nie stanowi autonomicznego, koniecznego „podwyższenia” poziomu bezpieczeństwa SOC

ISO/IEC 27701 opisuje wymagania dla systemu zarządzania prywatnością (PIMS) jako rozszerzenie ISMS. Nie jest standardem autonomicznym – nie można uzyskać certyfikacji ISO/IEC 27701 bez spełnienia wymagań ISO/IEC 27001. W konsekwencji, posiadanie ISO/IEC 27001 stanowi warunek bazowy dla ISO/IEC 27701, a żądanie dodatkowej certyfikacji ISO/IEC 27701 nie jest jedynym ani koniecznym sposobem wykazania zdolności do prawidłowej realizacji usługi SOC, zwłaszcza gdy wymagane jest również ISO 22301.

5) ISO 22301 wzmacnia wiarygodność wykonawcy w obszarach krytycznych dla SOC Certyfikacja ISO 22301 (BCMS) potwierdza dojrzałość organizacji w zakresie planowania, utrzymania i doskonalenia ciągłości działania. W usługach SOC – świadczonych w trybie ciągłym (24/7) – odporność operacyjna, gotowość na zakłócenia oraz zdolność do działania w sytuacjach incydentowych mają znaczenie kluczowe. Wymóg ISO 22301 stanowi zatem silny i adekwatny dowód należytej organizacji procesów krytycznych.

6) Ryzyko ograniczenia konkurencji i wątpliwości co do neutralności warunku (informacje publiczne o ISO/IEC 27701 na rynku SOC) przy wykorzystaniu publicznych środków pochodzących z KPO

Weryfikacja informacji publicznie dostępnych (np. sekcje „certyfikaty”, deklaracje zgodności, materiały ofertowe) wskazuje, że certyfikacja ISO/IEC 27701 jest wśród podmiotów świadczących usługi SOC komunikowana relatywnie rzadko. W ramach przeglądu źródeł publicznych jednoznacznie informację o posiadaniu certyfikatu ISO/IEC 27701 przez dostawcę SOC zidentyfikowano m.in. na stronie StillSec (sekcja „Certyfikaty”). Wprowadzenie wymogu, który w praktyce może być spełniany przez bardzo ograniczoną liczbę wykonawców, może rodzić uzasadnione wątpliwości co do zachowania zasady uczciwej konkurencji, równego traktowania oraz przejrzystości, a także budzić podejrzenie preferowania konkretnego dostawcy.

Źródła i odniesienia

1. Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (PZP): art. 16 oraz art. 112.
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO): w szczególności art. 5, 24, 25, 32 oraz art. 42.
3. Strona StillSec – sekcja „Certyfikaty” (informacja o ISO 27701): <https://stillsec.com/#certificates>
4. Normy: ISO/IEC 27001, ISO 22301, ISO/IEC 27701.

Odpowiedź:

Zamawiający wyjaśnia, że w Zapytaniu Ofertowym nie wymaga posiadania certyfikatu ISO/IEC 27701 z warunków udziału w postępowaniu.

Zgodnie z warunkami zapytania ofertowego Zamawiający wymaga, aby Wykonawca wykazał, że „Posiada wdrożony System Zarządzania Prywatnością Informacji zgodny z normą ISO 27701”

Na potwierdzenie spełnienia tego warunku Wykonawca powinien przedstawić „**Oświadczenie Wykonawcy** o posiadaniu wdrożonego Systemu Zarządzania Prywatnością Informacji zgodnego z normą ISO 27701”