

ODPOWIEDZI NA PYTANIA WYKONAWCÓW

dotyczy: zaproszenia do składania ofert na świadczenie usługi hostingu dedykowanego serwisu SOP wraz z usługami serwisowymi, konserwacyjnymi i administracyjnymi

W związku z wnioskami o wyjaśnienie treści zaproszenia do składania ofert, które wpłynęły do Zamawiającego w dniach 20–22 lipca 2026 r. (dwa pisma oraz pytania przekazane pocztą elektroniczną), Zamawiający przekazuje poniższe odpowiedzi. Odpowiedzi udzielane są łącznie, bez wskazywania źródła zapytania, i zostają opublikowane w miejscu publikacji zaproszenia. Treść pytań przytoczono w brzmieniu nadesłanym przez wykonawców, z pominięciem uzasadnień.

Odpowiedzi stanowią integralną część dokumentacji postępowania i są wiążące dla Zamawiającego i wykonawców. W zakresie, w jakim doprecyzowują lub zmieniają treść zaproszenia (w tym Opisu przedmiotu zamówienia) lub wzoru umowy, mają one pierwszeństwo przed pierwotnym brzmieniem dokumentacji i zostaną odzwierciedlone w treści umowy zawieranej z wybranym wykonawcą.

Zamawiający przypomina, że termin składania ofert został przedłużony do dnia **30 lipca 2026 r., do godz. 12:00** (komunikaty z 23 i 27 lipca 2026 r.). Wykonawcy, którzy złożyli oferty przed publikacją niniejszych odpowiedzi, mogą je zmienić lub wycofać przed upływem terminu składania ofert.

Numeracja pytań w Częściach I–III odpowiada numeracji zastosowanej w poszczególnych pismach wykonawców. Pismo drugie nie zawiera pytania nr 13 — zachowano oryginalną numerację nadawcy.

Część I. Odpowiedzi na pytania z pisma pierwszego (wpływ: 20.07.2026)

Pytanie 1 — termin rozpoczęcia świadczenia usługi

Treść pytania: „Czy Zamawiający może potwierdzić, że rozpoczęcie świadczenia usługi planowane jest na 16 sierpnia 2026 r., oraz wskazać przewidywany termin zawarcia umowy? Jak należy stosować 14-dniowy termin na konfigurację i uruchomienie środowiska, jeżeli umowa zostanie zawarta później niż 2 sierpnia 2026 roku?”

Odpowiedź: Zamawiający potwierdza, że planowane rozpoczęcie świadczenia usługi to 1 września 2026 r. Zamawiający planuje zawarcie umowy niezwłocznie po wyborze najkorzystniejszej oferty, orientacyjnie do 5 sierpnia br. Czynności przygotowawcze, o których mowa w § 2 ust. 6 wzoru umowy, wykonywane są w terminie 14 dni od dnia zawarcia umowy. Jeżeli zawarcie umowy nastąpi w terminie uniemożliwiającym rozpoczęcie świadczenia usługi 1 września 2026 r., rozpoczęcie świadczenia nastąpi po wykonaniu czynności przygotowawczych i podpisaniu Protokołu zdawczo-odbiorczego, a usługa będzie świadczona przez 12 miesięcy od dnia rozpoczęcia realizacji przedmiotu umowy (§ 2 ust. 2 wzoru umowy).

Pytanie 2 — termin uruchomienia a współdziałanie Zamawiającego

Treść pytania: „Czy Zamawiający może rozważyć przyjęcie, że termin uruchomienia usługi będzie liczony od dnia przekazania Wykonawcy kompletnych danych, kopii systemu, dokumentacji, dostępów administracyjnych i informacji konfiguracyjnych potrzebnych do wykonania migracji, a opóźnienia wynikające z nieterminowego współdziałania Zamawiającego albo obecnego dostawcy nie będą traktowane jako zwłoka Wykonawcy?”

Odpowiedź: Zamawiający potwierdza, że opóźnienia wynikające z przyczyn leżących po stronie Zamawiającego — w tym z nieterminowego przekazania danych, kopii systemu, dostępów, dokumentacji lub informacji konfiguracyjnych niezbędnych do migracji — nie stanowią zwłoki Wykonawcy i nie mogą być podstawą naliczenia kar umownych (zob. § 5 ust. 16 wzoru umowy). Na potrzeby oceny dochowania terminów opóźnienia w przekazaniu danych przez dotychczasowego operatora traktowane są jak przyczyny leżące po stronie Zamawiającego. W takim przypadku termin wykonania czynności przygotowawczych ulega odpowiedniemu przesunięciu.

Pytanie 3 — zakres i organizacja migracji

Treść pytania: „Czy Zamawiający może wskazać, czy zakres migracji obejmuje: system plików, bazę danych, konfigurację systemów i usług, prywatną instancję GitLab, serwer pocztowy, rekordy DNS, konfigurację certyfikatów oraz dane środowiska testowego? Czy obecny dostawca hostingu będzie uczestniczył w przekazaniu środowiska i czy Zamawiający dopuszcza uzgodnione okno niedostępności na przełączenie produkcyjne?”

Odpowiedź: Zakres migracji obejmuje: bazę danych, system plików wraz z załącznikami, konfiguracje usług niezbędne do uruchomienia serwisu, prywatną instancję GitLab oraz dane środowiska testowego. Konfigurację usługi wysyłki powiadomień odtwarza Wykonawca (migracji podlega konfiguracja, nie skrzynki pocztowe). Certyfikat SSL dostarcza Zamawiający (§ 2 ust. 11); zmiany rekordów DNS wykonuje Zamawiający na podstawie danych przekazanych przez Wykonawcę. Zamawiający zapewni przekazanie danych z obecnego środowiska (przy udziale dotychczasowego operatora) w formie uzgodnionej z wybranym wykonawcą (w szczególności rzut bazy danych oraz archiwum plików). Zamawiający dopuszcza uzgodnione okno niedostępności na przełączenie produkcyjne. Migracja próbna nie jest wymagana; przed przełączeniem Wykonawca przedstawi plan migracji obejmujący weryfikację danych oraz możliwość powrotu do poprzedniego środowiska. Testy funkcjonalne serwisu po migracji oraz potwierdzenie kompletności danych wykonuje Zamawiający.

Pytanie 4 — wielkość i dynamika danych

Treść pytania: „Czy Zamawiający może podać aktualne wykorzystanie przestrzeni przez serwer aplikacyjny, bazę danych, środowisko testowe, repozytorium GitLab, załączniki i serwer pocztowy, a także średni miesięczny przyrost danych, orientacyjną liczbę plików oraz wielkość bazy danych?”

Odpowiedź: Zamawiający nie udostępnia szczegółowej inwentaryzacji środowiska na etapie postępowania. Na potrzeby przygotowania oferty należy przyjąć następujące wiążące wartości graniczne: wolumen danych środowiska produkcyjnego (baza danych, pliki i załączniki, w tym repozytoria GitLab) nie przekracza pojemności przestrzeni dyskowych określonych w OPZ (łącznie 700 GB) i nie przekroczy ich w okresie realizacji umowy; wolumen środowiska testowego nie przekracza łącznie 350 GB. Rozbudowa przestrzeni ponad wartości z OPZ wykracza poza przedmiot zamówienia. Zapotrzebowanie na przestrzeń backupu należy wymiarować na podstawie powyższych wolumenów, cykli kopii wskazanych w § 2 ust. 8 wzoru umowy oraz retencji wskazanej w odpowiedzi na pytanie 16.

Pytanie 5 — charakter hostingu dedykowanego i sposób przydziału zasobów

Treść pytania: „Czy Zamawiający może potwierdzić, że określenie „hosting dedykowany” odnosi się do wydzielonego i logicznie odseparowanego środowiska wirtualnego przeznaczonego dla systemu SOP, a nie do fizycznych hostów używanych wyłącznie przez Zamawiającego? Czy dopuszczalne jest uruchomienie maszyn wirtualnych na współdzielonym klastrze centrum danych, przy zapewnieniu wymaganej wydajności, bezpieczeństwa i dostępności? Czy Zamawiający oczekuje rezerwacji zasobów CPU i RAM albo ograniczenia overcommitmentu tych zasobów?”

Odpowiedź: Zamawiający potwierdza, że „hosting dedykowany” oznacza logicznie wydzielone i odseparowane środowisko wirtualne przeznaczone dla systemu SOP; fizyczne serwery użytkowane wyłącznie przez Zamawiającego nie są wymagane. Dopuszczalne jest uruchomienie maszyn wirtualnych na współdzielonym klastrze centrum danych, pod warunkiem zapewnienia separacji, bezpieczeństwa oraz wymaganej wydajności i dostępności. Pamięć RAM i przestrzeń dyskowa w parametrach określonych w OPZ muszą być gwarantowane (zarezerwowane) dla środowiska SOP. Zamawiający nie określa sztywnego wskaźnika overcommitment vCPU — Wykonawca odpowiada za przydział zasobów zapewniający prawidłową wydajność serwisu i dotrzymanie SLA.

Pytanie 6 — wymaganie dotyczące procesorów vCPU

Treść pytania: „Czy Zamawiający może potwierdzić, że zapis „Intel Xeon 2.10Mhz” należy rozumieć jako odniesienie do procesora Intel Xeon o częstotliwości 2,10 GHz? Czy dopuszczalne są procesory równoważne lub nowszej generacji, zapewniające co najmniej porównywalną wydajność, bez wymagania stałej częstotliwości pojedynczego rdzenia na poziomie 2,10 GHz?”

Odpowiedź: Zamawiający potwierdza, że zapis „Intel Xeon 2.10Mhz” stanowi oczywistą omyłkę pisarską i oznacza procesor klasy serwerowej o taktowaniu referencyjnym 2,10 GHz. Dopuszczalne są procesory równoważne lub nowszych generacji, w tym innych producentów (architektura x86-64), zapewniające co

najmniej porównywalną wydajność. Częstotliwość zegara pojedynczego rdzenia nie jest samodzielnym kryterium oceny równoważności.

Pytanie 7 — parametry środowiska testowego

Treść pytania: „Czy Zamawiający może podać minimalne parametry vCPU, RAM i przestrzeni dyskowej dla serwera aplikacyjnego oraz serwera bazy danych w środowisku testowym? Czy środowisko testowe ma być objęte takim samym SLA, monitoringiem 24/7, backupem i aktualizacjami jak środowisko produkcyjne?”

Odpowiedź: Minimalne parametry środowiska testowego: serwer aplikacyjny — 4 vCPU, 16 GB RAM, 250 GB przestrzeni dyskowej; serwer bazy danych — 4 vCPU, 16 GB RAM, 100 GB przestrzeni dyskowej; wersje systemu operacyjnego i komponentów odpowiadające środowisku produkcyjnemu. Środowisko testowe ma być stale dostępne oraz objęte ochroną firewall i aktualizacjami bezpieczeństwa. Środowisko testowe nie jest objęte gwarancją dostępności 99,4%, monitoringiem 24/7 ani karami umownymi właściwymi dla środowiska produkcyjnego; wymagany jest backup bazy danych i konfiguracji środowiska testowego wykonywany co najmniej raz w tygodniu, z retencją 4 tygodni. Powyższe stanowi uzupełnienie OPZ.

Pytanie 8 — zasoby i przestrzeń dla prywatnej instancji GitLab

Treść pytania: „Czy Zamawiający przewiduje uruchomienie prywatnej instancji GitLab jako odrębnej maszyny wirtualnej lub usługi? Czy zasoby CPU, RAM i przestrzeń dyskowa dla GitLab mają stanowić dodatkowe zasoby ponad parametry wskazane dla serwera aplikacyjnego, serwera bazy danych i środowiska testowego, czy GitLab może korzystać z zasobów jednego z tych serwerów? Czy Zamawiający może również podać liczbę użytkowników i projektów, aktualną oraz przewidywaną wielkość repozytoriów, oczekiwany przyrost danych, wymaganą edycję GitLab, zapotrzebowanie na GitLab Runner, zakres backupu, retencję oraz wymagania dotyczące SLA?”

Odpowiedź: Zamówienie obejmuje przeniesienie istniejącej prywatnej instancji GitLab (min. edycja Community). Liczba użytkowników nie przekracza 30, a łączny rozmiar repozytoriów mieści się w wolumenie wskazanym w odpowiedzi na pytanie 4. GitLab Runner, CI/CD oraz Container Registry nie są wymagane. GitLab może zostać uruchomiony na zasobach serwera aplikacyjnego albo jako odrębna maszyna — decyzja architektoniczna należy do Wykonawcy, przy czym nie może to pomniejszać minimalnych zasobów przewidzianych w OPZ dla serwerów SOP. GitLab objęty jest backupem (repozytoria, konfiguracja i metadane) na zasadach jak pozostałe komponenty; nie jest objęty gwarancją dostępności 99,4%.

Pytanie 9 — serwer pocztowy do wysyłania powiadomień

Treść pytania: „Czy Zamawiający może podać przewidywaną liczbę wiadomości wysyłanych na dobę i w godzinie szczytu, liczbę domen i adresów nadawczych, maksymalny rozmiar wiadomości oraz informację, czy wymagany jest dedykowany publiczny adres IP? Która ze Stron będzie odpowiadała za konfigurację rekordów SPF, DKIM i DMARC oraz utrzymanie reputacji domeny i adresu IP?”

Odpowiedź: Zamawiający wyjaśnia, że wymaganie dotyczy wyłącznie usługi wysyłania powiadomień z aplikacji SOP (SMTP). Skrzynki pocztowe, odbieranie i przechowywanie wiadomości oraz webmail nie są wymagane. Zamawiający nie prowadzi statystyk wysyłki; wysyłka ma charakter transakcyjny — są to powiadomienia generowane przez aplikację obsługującą ok. 15 tys. kont użytkowników, o natężeniu podwyższonym w okresach naborów. Wysyłka realizowana jest z jednej domeny nadawczej; maksymalny rozmiar wiadomości: 50 MB. Wykonawca zapewnia konfigurację serwera wysyłkowego (w tym DKIM i PTR) oraz utrzymanie reputacji infrastruktury wysyłkowej; Zamawiający publikuje wskazane przez Wykonawcę rekordy DNS (SPF, DKIM, DMARC). Dla usługi wysyłki powiadomień wymagany jest dedykowany publiczny adres IP, uwzględniony w cenie oferty. Wykonawca nie odpowiada za odrzucenie lub klasyfikację wiadomości przez zewnętrzne systemy odbiorców, jeżeli wysyłka, konfiguracja i reputacja po jego stronie są prawidłowe.

Pytanie 10 — łącze internetowe i transfer danych

Treść pytania: „Czy Zamawiający może wyjaśnić, czy wymagane 1 Gbps oznacza przepustowość portu, czy gwarantowane pasmo symetryczne dostępne dla systemu SOP? Czy Zamawiający może również podać aktualny średni i szczytowy transfer, miesięczny wolumen danych oraz potwierdzić, czy usługa ma być świadczona bez limitu transferu?”

Odpowiedź: Parametr „1 Gbps” oznacza przepustowość portu, z którego korzysta środowisko; nie jest wymagane gwarantowane pasmo symetryczne zarezerwowane wyłącznie dla systemu SOP. Usługa ma być świadczona bez limitu transferu. Zamawiający nie prowadzi statystyki transferu; serwis obsługuje nabory wniosków (formularze i załączniki), a jego ruch nie ma charakteru masowego ani streamingowego.

Pytanie 11 — adresacja publiczna IPv4 i IPv6

Treść pytania: „Czy Zamawiający może wskazać oczekiwaną liczbę publicznych adresów IPv4 i IPv6 oraz sposób ich wykorzystania przez poszczególne elementy środowiska? Czy wystarczający jest jeden publiczny adres IPv4 dla całej usługi z wykorzystaniem NAT lub reverse proxy, czy przewidywane są odrębne adresy dla aplikacji, poczty, GitLab i innych usług?”

Odpowiedź: Wymagany jest co najmniej jeden publiczny adres IPv4 oraz adresacja IPv6; dopuszczalne jest zastosowanie NAT i reverse proxy. Liczbę adresów dobiera Wykonawca w ilości niezbędnej do prawidłowego działania usług (§ 2 ust. 4 pkt 2 wzoru umowy), z uwzględnieniem odpowiedzi na pytanie 9 (dedykowany adres dla usługi wysyłki powiadomień).

Pytanie 12 — redundancja infrastruktury hostingowej

Treść pytania: „Czy Zamawiający może potwierdzić, czy poza redundantnym systemem firewall oczekuje również redundancji platformy wirtualizacyjnej, hostów obliczeniowych, pamięci masowej, przełączników i łącz internetowych oraz automatycznego uruchomienia maszyn wirtualnych na innym hoście w przypadku awarii? Jeżeli tak, czy może wskazać minimalne wymagania w tym zakresie?”

Odpowiedź: Poza redundantnym systemem firewall (§ 2 ust. 7 wzoru umowy) Zamawiający nie narzuca poziomu ani technologii redundancji poszczególnych warstw infrastruktury. Wykonawca dobiera architekturę tak, aby zapewnić gwarantowaną dostępność 99,4% w skali miesiąca oraz wymagania dotyczące backupu i odtwarzania; mechanizmy wysokiej dostępności należy przedstawić w opisie planowanego środowiska hostingowego składanym wraz z ofertą.

Pytanie 13 — sposób realizacji i zakres funkcjonalny firewalla

Treść pytania: „Czy Zamawiający może potwierdzić, że wymaganie redundantnego systemu firewall może być spełnione przez centralny klaster wysokiej dostępności, fizyczny lub wirtualny, obsługujący całe centrum danych i wielu klientów, pod warunkiem wydzielenia dla systemu SOP odrębnych stref, interfejsów lub kontekstów logicznych, polityk bezpieczeństwa oraz zapewnienia wymaganej wydajności i dostępności? Czy Zamawiający oczekuje dedykowanej pary urządzeń albo dedykowanego kontekstu firewall przeznaczonego wyłącznie dla systemu SOP? Czy wymagany zakres funkcji obejmuje tylko filtrowanie ruchu L3/L4, czy również IPS/IDS, WAF, filtrowanie reputacyjne, ochronę anty-DDoS, inspekcję ruchu szyfrowanego i raportowanie zdarzeń?”

Odpowiedź: Wymaganie redundantnego systemu firewall może zostać spełnione przez centralny klaster wysokiej dostępności (fizyczny lub wirtualny) obsługujący wielu klientów, pod warunkiem wydzielenia dla systemu SOP odrębnych stref, interfejsów lub kontekstów logicznych oraz odrębnych polityk bezpieczeństwa. Dedykowana para urządzeń nie jest wymagana. Minimalny wymagany zakres funkcji to kontrola całego ruchu przychodzącego i wychodzącego z przepuszczaniem wyłącznie ruchu niezbędnego dla działania serwisu (filtrowanie L3/L4). Funkcje IPS/IDS, WAF, filtrowanie reputacyjne i inspekcja ruchu szyfrowanego nie są wymagane. Odrębna usługa ochrony anty-DDoS nie jest wymagana; jednocześnie ataki DDoS nie są wyłączone z SLA (zob. odpowiedź na pytanie 28) — sposób zabezpieczenia środowiska w tym zakresie pozostaje decyzją projektową Wykonawcy.

Pytanie 14 — bezpieczne połączenie z infrastrukturą Zamawiającego

Treść pytania: „Czy Zamawiający przewiduje zestawienie stałego tunelu site-to-site IPsec albo innego szyfrowanego połączenia pomiędzy centrum danych Wykonawcy a infrastrukturą Zamawiającego? Jeżeli takie połączenie jest wymagane, czy Zamawiający może wskazać liczbę zakończeń tunelu, oczekiwaną redundancję, przepustowość, sposób routingu, używaną adresację oraz podział odpowiedzialności za konfigurację urządzeń brzegowych i zarządzanie kluczami? Czy wymaganie dotyczące VPN odnosi się wyłącznie do dostępu administracyjnego osób obsługujących środowisko?”

Odpowiedź: Wymaganie dotyczące VPN (§ 2 ust. 12d wzoru umowy) odnosi się wyłącznie do zabezpieczenia dostępu administracyjnego osób obsługujących środowisko (alternatywnie: ograniczenie dostępu do wskazanych adresów IP). Stały tunel site-to-site pomiędzy centrum danych Wykonawcy a siecią Zamawiającego nie jest wymagany. Na potrzeby przygotowania oferty należy przyjąć wiążące założenie, że integracje zewnętrzne aplikacji realizowane są wyłącznie ruchem wychodzącym za pośrednictwem publicznej sieci Internet i nie wymagają dodatkowych łącz, urządzeń ani licencji po stronie Wykonawcy; szczegóły konfiguracyjne (adresy, porty, certyfikaty) zostaną przekazane wybranemu wykonawcy na etapie uzgodnień, o których mowa w § 2 ust. 6.

Pytanie 15 — zakres danych objętych backupem

Treść pytania: „Czy Zamawiający może potwierdzić, czy backup ma obejmować wszystkie maszyny i komponenty środowiska, tj. serwer aplikacyjny, bazę danych, środowisko testowe, GitLab, serwer pocztowy, konfigurację firewall oraz konfiguracje usług systemowych? Czy kopie mają być wykonywane na poziomie maszyn wirtualnych, systemu plików i bazy danych, czy przewidywane jest równoległe stosowanie kilku metod?”

Odpowiedź: Backup obejmuje wszystkie komponenty środowiska pozostające w administracji Wykonawcy: produkcyjną bazę danych i system plików (zgodnie z cyklami określonymi w § 2 ust. 8), instancję GitLab (repozytoria, konfiguracja, metadane), konfiguracje usług systemowych i firewalla oraz — w zakresie wskazanym w odpowiedzi na pytanie 7 — środowisko testowe. Usługa wysyłki powiadomień wymaga backupu konfiguracji, nie treści wiadomości. Kopie mogą być wykonywane na poziomie maszyn wirtualnych, systemu plików lub bazy danych, także z równoległym stosowaniem kilku metod — wybór technologii należy do Wykonawcy, pod warunkiem spełnienia wymaganych cykli, retencji, szyfrowania i skuteczności odtwarzania.

Pytanie 16 — retencja kopii zapasowych

Treść pytania: „Czy Zamawiający może wskazać wymagany okres retencji kopii przyrostowych i pełnych oraz minimalną liczbę przechowywanych punktów odtworzenia? Czy przewidywana jest również retencja miesięczna lub roczna?”

Odpowiedź: Wymagana retencja: kopie przyrostowe wykonywane co 6 godzin — co najmniej 14 dni; pełne kopie tygodniowe — co najmniej 4 tygodnie. Retencja miesięczna i roczna nie jest wymagana. Powyższe stanowi uzupełnienie OPZ.

Pytanie 17 — niezależna geograficznie lokalizacja kopii

Treść pytania: „Czy Zamawiający może wskazać, jak należy rozumieć pojęcie „niezależnej geograficznie lokalizacji”, w tym ewentualną minimalną odległość od podstawowego centrum danych? Czy dopuszczalne jest przechowywanie kopii w drugim centrum danych należącym do tego samego Wykonawcy lub przez niego kolokowanym, przy zachowaniu odrębnego budynku, zasilania i infrastruktury telekomunikacyjnej?”

Odpowiedź: Przez „niezależną geograficznie lokalizację” rozumie się odrębny fizyczny obiekt (budynek) o niezależnym zasilaniu i niezależnej infrastrukturze telekomunikacyjnej względem podstawowego centrum danych. Dopuszczalne jest przechowywanie kopii w drugim centrum danych należącym do tego samego Wykonawcy lub przez niego kolokowanym. Minimalna odległość nie jest określona. Dane i kopie zapasowe muszą być przetwarzane wyłącznie na terytorium EOG.

Pytanie 18 — parametry RPO i RTO

Treść pytania: „Czy Zamawiający może potwierdzić, że wymagany parametr RPO wynosi maksymalnie 6 godzin? Czy może również wskazać wymagane wartości RTO dla odtworzenia bazy danych, systemu plików, pojedynczej maszyny wirtualnej oraz całego środowiska po awarii?”

Odpowiedź: Maksymalne RPO dla bazy danych i systemu plików wynosi 6 godzin i wynika z wymaganego cyklu kopii przyrostowych. RTO: przywrócenie działania usługi (w tym odtworzenie danych z kopii w przypadku, o którym mowa w § 2 ust. 10) — do 10 godzin, spójnie z § 4 ust. 2 wzoru umowy; odtworzenie pełnego środowiska po rozległej awarii — do 24 godzin. Przez odtworzenie pełnego środowiska rozumie się odbudowę wszystkich maszyn i usług od podstaw (np. w przypadku utraty podstawowego centrum danych); nie uchybia to terminowi 10 godzin na przywrócenie działania serwisu produkcyjnego w pozostałych przypadkach.

Pytanie 19 — zakres testów odtworzeniowych

Treść pytania: „Czy Zamawiający może określić wymagany zakres testu odtworzeniowego: pojedynczy plik, bazę danych, wybraną maszynę wirtualną czy pełne uruchomienie całego systemu SOP? Czy test może zostać wykonany w odizolowanym środowisku testowym i jakie kryteria będą stosowane przy jego odbiorze?”

Odpowiedź: Test odtworzeniowy obejmuje odtworzenie bazy danych i systemu plików produkcyjnego serwisu w izolowanym środowisku Wykonawcy wraz z uruchomieniem usług niezbędnych do działania aplikacji. Zakres i termin testu Wykonawca uzgadnia z Zamawiającym; zasoby tymczasowe niezbędne do przeprowadzenia testu zapewnia Wykonawca w ramach wynagrodzenia. Kryterium pozytywnego wyniku jest poprawne uruchomienie aplikacji na danych z kopii oraz zgodność danych z wybranym punktem odtworzenia; weryfikację funkcjonalną wykonuje Zamawiający. Test przed rozpoczęciem świadczenia usługi (§ 2 ust. 12e) zostanie przeprowadzony po przekazaniu Wykonawcy kompletnej i poprawnej kopii danych.

Pytanie 20 — szyfrowanie kopii i zarządzanie kluczami

Treść pytania: „Czy Zamawiający może potwierdzić, czy kopie zapasowe mają być szyfrowane w transmisji i w spoczynku? Jeżeli tak, czy klucz szyfrujący ma pozostawać wyłącznie w dyspozycji Zamawiającego, czy może być zarządzany przez Wykonawcę zgodnie z jego procedurami bezpieczeństwa?”

Odpowiedź: Kopie zapasowe mają być szyfrowane w transmisji i w spoczynku. Kluczami szyfrującymi zarządza Wykonawca zgodnie z udokumentowaną procedurą bezpieczeństwa, zapewniając ich rozdzielanie od danych, kontrolę dostępu oraz możliwość odtworzenia danych przez cały okres umowy i przy przekazaniu danych po jej zakończeniu. Zamawiający nie wymaga, aby klucze pozostawały w jego wyłącznej dyspozycji.

Pytanie 21 — podział odpowiedzialności za warstwę systemową i aplikacyjną

Treść pytania: „Czy Zamawiający może wskazać planowany podział odpowiedzialności pomiędzy Stronami? Czy Wykonawca odpowiada za system operacyjny, usługi systemowe i infrastrukturę, czy również za aktualizację PHP, MariaDB, frameworka Yii, kodu aplikacji SOP, zależności aplikacyjnych oraz migracje schematu bazy danych? Która Strona będzie odpowiadała za testy zgodności aplikacji po aktualizacjach?”

Odpowiedź: Wykonawca odpowiada za warstwę infrastrukturalną i systemową: wirtualizację, systemy operacyjne, usługi systemowe (w tym Nginx, środowisko wykonawcze PHP i MariaDB jako usługi), firewall, backup, monitoring, techniczne działanie usługi wysyłki powiadomień oraz aktualizacje komponentów pozostających w jego administracji (§ 2 ust. 12f). Kod aplikacji SOP, framework Yii i zależności aplikacyjne, struktura i zapytania bazy danych, procesy wdrażania kodu, integracje na poziomie aplikacji oraz testy aplikacyjne po aktualizacjach i zmianach pozostają po stronie Zamawiającego. Naprawa i modyfikacje kodu aplikacji, optymalizacja zapytań oraz dostosowanie aplikacji do nowych wersji komponentów nie są objęte przedmiotem zamówienia ani wynagrodzeniem ryczałtowym.

Pytanie 22 — aktualizacje krytyczne w terminie 72 godzin

Treść pytania: „Czy Zamawiający może wskazać klasyfikację, według której będzie ustalana krytyczność aktualizacji, oraz moment, od którego będzie liczony termin 72 godzin? Czy w przypadku potrzeby przeprowadzenia testów kompatybilności lub uzyskania akceptacji Zamawiającego termin może zostać zawieszony do czasu uzgodnienia wdrożenia i okna serwisowego?”

Odpowiedź: Za aktualizację krytyczną uznaje się poprawkę bezpieczeństwa oznaczoną przez producenta lub dystrybutora jako krytyczna albo usuwającą podatność o ocenie CVSS 9,0 lub wyższej (według oceny producenta lub bazy NVD) lub podatność, której aktywne wykorzystywanie zostało publicznie potwierdzone. Termin 72 godzin biegnie od udostępnienia poprawki w oficjalnym kanale aktualizacji stosowanego systemu (dla komercyjnie wspieranego buildu PHP — w kanale jego dostawcy). Jeżeli instalacja wymaga wcześniejszych uzgodnień z Zamawiającym (§ 2 ust. 12f) lub testów kompatybilności, Wykonawca niezwłocznie przedstawia ocenę ryzyka i plan wdrożenia; czas oczekiwania na akceptację Zamawiającego nie jest wliczany do terminu 72 godzin, o ile Wykonawca przekazał komplet informacji i zastosował dostępne zabezpieczenia tymczasowe.

Pytanie 23 — zakres rejestrowania i retencji logów

Treść pytania: „Czy Zamawiający może doprecyzować, czy 90-dniowa retencja dotyczy wyłącznie logów działań administracyjnych, czy również logów systemowych, aplikacyjnych, bazy danych, firewall, reverse proxy, poczty i GitLab? Czy może również wskazać oczekiwaną formę dostępu Zamawiającego do logów oraz potwierdzić, czy wymagany jest centralny system SIEM lub syslog?”

Odpowiedź: Retencja 90 dni obejmuje: logi działań administracyjnych, logi systemowe (w tym uwierzytelniania), logi firewalla oraz logi dostępowe serwera WWW/reverse proxy; dla bazy danych, usługi wysyłki powiadomień i GitLab — logi zdarzeń istotnych dla bezpieczeństwa. Logi aplikacyjne serwisu SOP prowadzone są zgodnie z konfiguracją aplikacji i nie są objęte tym wymogiem. Centralny system SIEM ani syslog nie jest wymagany. Zamawiający otrzymuje wyciąg z logów na żądanie: w związku z incydem — w terminie 1 dnia roboczego, w pozostałych przypadkach — w terminie 3 dni roboczych.

Pytanie 24 — zakres monitoringu 24/7

Treść pytania: „Czy Zamawiający może wskazać minimalny zakres monitorowanych parametrów i usług, w szczególności czy monitoring ma obejmować jedynie dostępność maszyn i usług, czy także parametry wydajnościowe, zajętość przestrzeni, stan backupu, ważność certyfikatów, zdarzenia bezpieczeństwa oraz funkcjonalny test działania aplikacji? Czy Zamawiający oczekuje dostępu do panelu monitoringu?”

Odpowiedź: Minimalny zakres monitoringu obejmuje: dostępność maszyn i usług (w tym zewnętrzną odpowiedź HTTP/HTTPS serwisu, bazę danych, usługę wysyłki powiadomień, GitLab), wykorzystanie zasobów (CPU, RAM, przestrzeń dyskową), poprawność wykonania kopii zapasowych oraz ważność certyfikatów. Funkcjonalne testy biznesowe aplikacji nie są wymagane. Zamawiający nie wymaga dostępu do panelu monitoringu; wystarczające jest miesięczne zestawienie dostępności i zdarzeń w raporcie, o którym mowa w odpowiedzi na pytanie 29.

Pytanie 25 — kanały przyjmowania zgłoszeń

Treść pytania: „Czy Zamawiający może potwierdzić, czy Wykonawca musi zapewnić wszystkie trzy kanały przyjmowania zgłoszeń wskazane we wzorze umowy, czy wystarczające jest zapewnienie telefonu oraz jednego z kanałów elektronicznych, zgodnie z warunkiem udziału w postępowaniu?”

Odpowiedź: Wystarczające jest zapewnienie całodobowej obsługi zgłoszeń przez telefon oraz co najmniej jeden kanał elektroniczny (system zgłoszeniowy albo e-mail), zgodnie z warunkiem udziału w postępowaniu. Katalog kanałów w § 4 ust. 1 wzoru umowy zostanie dostosowany do kanałów faktycznie oferowanych przez wybranego wykonawcę, z zachowaniem powyższego minimum. Zgłoszenie telefoniczne wymaga potwierdzenia drogą elektroniczną.

Pytanie 26 — kategorie zgłoszeń oraz czas reakcji i usunięcia

Treść pytania: „Czy Zamawiający może określić kategorie lub priorytety zgłoszeń oraz oczekiwane czasy reakcji, przywrócenia usługi i rozwiązania dla każdej kategorii? Czy termin 10 godzin dotyczy wszystkich zgłoszeń, wyłącznie awarii powodujących częściowy lub zmniejszony dostęp, czy także zgłoszeń konfiguracyjnych, konsultacyjnych i problemów wynikających z działania aplikacji?”

Odpowiedź: Termin 10 godzin (§ 4 ust. 2 wzoru umowy) dotyczy usuwania nieprawidłowości w świadczeniu usługi hostingu powodujących częściowy lub zmniejszony dostęp, a także — tym bardziej — całkowitą niedostępność usługi, z zastrzeżeniem terminu 24 godzin przewidzianego w odpowiedzi na pytanie 18 dla odtworzenia pełnego środowiska po rozległej awarii. Nie dotyczy on konsultacji, zapytań ani prac konfiguracyjnych zleczanych przez Zamawiającego, które realizowane są w terminach uzgodnionych przez Strony, ani błędów kodu aplikacji pozostającej poza administracją Wykonawcy. Wykonawca potwierdza przyjęcie zgłoszenia niezwłocznie, nie później niż w ciągu 1 godziny, i niezwłocznie rozpoczyna prace. Zamawiający nie wprowadza dodatkowej formalnej kategoryzacji zgłoszeń.

Pytanie 27 — sposób pomiaru SLA

Treść pytania: „Czy Zamawiający może doprecyzować punkt i metodę pomiaru dostępności, w tym narzędzie referencyjne, częstotliwość pomiaru oraz warunki uznania usługi za niedostępną? Czy częściowe ograniczenie funkcjonalności, niedostępność pojedynczego komponentu lub problem po stronie aplikacji będą traktowane jako niedostępność całej usługi?”

Odpowiedź: Dostępność mierzona jest z zewnętrznego punktu monitoringu na poziomie produkcyjnego serwisu (HTTP/HTTPS), w odstępach nie dłuższych niż 1 minuta. Niedostępność stwierdza się po trzech kolejnych nieudanych pomiarach, przy czym za jej początek przyjmuje się chwilę pierwszego nieudanego pomiaru w tej serii; niedostępność kończy się po trzech kolejnych pomiarach prawidłowych, a za jej koniec przyjmuje się chwilę pierwszego prawidłowego pomiaru w tej serii. Monitoring pozostałych usług (baza danych, usługa wysyłki powiadomień, GitLab) ma charakter diagnostyczny i nie stanowi odrębnego miernika SLA. Podstawą rozliczenia są dane monitoringu Wykonawcy, z prawem weryfikacji przez Zamawiającego (w razie sporu zastosowanie ma § 4 ust. 5). Ograniczenie funkcjonalności lub niedostępność pojedynczego komponentu pomocniczego nie stanowi niedostępności całej usługi, o ile serwis pozostaje dostępny dla użytkowników; niedostępność wynikająca wyłącznie z błędów aplikacji pozostającej poza administracją Wykonawcy nie stanowi niedostępności usługi hostingu.

Pytanie 28 — okna serwisowe i wyłączenia z SLA

Treść pytania: „Czy Zamawiający może potwierdzić, że do czasu niedostępności nie będą wliczane przerwy wynikające z: uzgodnionych okien serwisowych, awarii lub błędów aplikacji pozostającej poza zakresem administracji Wykonawcy, działań lub zaniechań Zamawiającego, niedostępności usług i łączy podmiotów trzecich niezależnych od Wykonawcy, ataków DDoS przekraczających uzgodniony poziom ochrony oraz zdarzeń siły wyższej? Jaką procedurę należy stosować w przypadku pilnych prac bezpieczeństwa, których nie można zgłosić z 24-godzinym wyprzedzeniem?”

Odpowiedź: Do czasu niedostępności nie wlicza się: uzgodnionych okien serwisowych (§ 4 ust. 4), innych przerw zaakceptowanych przez Zamawiającego, przerw z przyczyn leżących po stronie Zamawiającego, siły wyższej (§ 5 ust. 16) oraz niedostępności wynikającej wyłącznie z błędów aplikacji pozostającej poza administracją Wykonawcy. Zamawiający nie wprowadza automatycznego wyłączenia dla awarii poddostawców wybranych przez Wykonawcę ani dla ataków DDoS. Pilne prace bezpieczeństwa, których nie można zgłosić z 24-godzinym wyprzedzeniem, mogą być prowadzone po niezwłocznym powiadomieniu Zamawiającego, z późniejszym raportem, jeżeli zwłoka zwiększałaby ryzyko dla bezpieczeństwa serwisu; czas takich prac, zgłoszonych przed ich rozpoczęciem, traktowany jest jak uzgodniona przerwa serwisowa, o ile konieczność ich niezwłocznego przeprowadzenia była obiektywnie uzasadniona, co Wykonawca wykaże w raporcie — Zamawiający może zakwestionować zasadność, a w razie sporu stosuje się § 4 ust. 5.

Pytanie 29 — raport ze świadczenia usługi

Treść pytania: „Czy Zamawiający może wskazać oczekiwany zakres i format raportu oraz maksymalną częstotliwość żądania jego przygotowania? Czy przewidywany jest również cykliczny raport miesięczny obejmujący dostępność SLA, zgłoszenia, kopie zapasowe, wykorzystanie zasobów, aktualizacje i zdarzenia bezpieczeństwa?”

Odpowiedź: Standardowy raport miesięczny obejmujący dostępność (SLA), zgłoszenia, kopie zapasowe i testy odtworzeniowe, aktualizacje, wykorzystanie zasobów oraz zdarzenia bezpieczeństwa spełnia wymóg § 2 ust. 12 wzoru umowy. Zamawiający będzie żądał raportu nie częściej niż raz w miesiącu kalendarzowym, z zastrzeżeniem odrębnych raportów dotyczących konkretnych incydentów. Forma elektroniczna.

Pytanie 30 — miesięczny protokół i podstawa wystawienia faktury

Treść pytania: „Czy Zamawiający może potwierdzić, że brak przekazania przez Zamawiającego miesięcznego protokołu w terminie 3 dni roboczych od zakończenia miesiąca nie będzie wstrzymywał możliwości wystawienia faktury? Czy Zamawiający dopuści mechanizm, zgodnie z którym w przypadku braku zgłoszenia zastrzeżeń w określonym terminie usługa zostanie uznana za odebraną?”

Odpowiedź: Zamawiający potwierdza, że jeżeli w terminie 3 dni roboczych od zakończenia miesiąca nie prześle protokołu ani zastrzeżeń co do wykonania usługi, usługę uznaje się za wykonaną należycie w danym okresie rozliczeniowym, co uprawnia Wykonawcę do wystawienia faktury. Wady nieistotne, niewpływające na dostępność, bezpieczeństwo ani możliwość korzystania z usługi, nie stanowią podstawy odmowy potwierdzenia wykonania usługi za cały miesiąc — są wskazywane w protokole wraz z terminem ich usunięcia. Powyższe nie dotyczy Protokołu zdawczo-odbiorczego uruchomienia usługi (§ 3 ust. 21) i nie wyłącza uprawnień Zamawiającego z tytułu nieprawidłowości ujawnionych po upływie terminu ani rozliczenia SLA za dany okres.

Pytanie 31 — podwykonawcy i dalsze podmioty przetwarzające

Treść pytania: „Czy Zamawiający może wyjaśnić relację pomiędzy obowiązkiem uprzedniego poinformowania o zmianie podwykonawcy a wymogiem uzyskania uprzedniej pisemnej zgody Administratora na dalsze powierzenie danych? Czy może również wskazać termin udzielenia zgody lub zgłoszenia sprzeciwu oraz potwierdzić, czy dostawcy kolokacji, telekomunikacji i narzędzi, którzy nie posiadają dostępu do danych, także mają być wykazywani jako dalsze podmioty przetwarzające?”

Odpowiedź: Obowiązek poinformowania (§ 6 ust. 3–4 wzoru umowy) dotyczy wszystkich podwykonawców uczestniczących w realizacji usługi. Uprzednia pisemna zgoda Administratora (§ 9 ust. 5) jest wymagana dla dalszego powierzenia przetwarzania danych osobowych. Zamawiający rozpatrzy wniosek o zgodę w terminie 14 dni od otrzymania kompletnej informacji o podmiocie, zakresie czynności i państwie przetwarzania; brak odpowiedzi w tym terminie nie oznacza zgody. Dostawcy kolokacji, telekomunikacji i narzędzi, którzy nie mają dostępu do danych i nie wykonują na nich operacji, nie są dalszymi podmiotami przetwarzającymi — podlegają wyłącznie obowiązkowi informacyjnemu z § 6 ust. 3.

Pytanie 32 — zasady audytów i inspekcji RODO

Treść pytania: „Czy Zamawiający może doprecyzować zasady prowadzenia audytów i inspekcji, w szczególności termin wcześniejszego powiadomienia, częstotliwość, godziny prowadzenia audytu, obowiązek zachowania poufności przez audytorów oraz zasady pokrywania kosztów? Czy audyt może zostać zastąpiony przedstawieniem aktualnych raportów, certyfikatów lub wyników niezależnych audytów bezpieczeństwa, jeżeli dokumenty te potwierdzają spełnienie wymagań?”

Odpowiedź: Audyt planowy poprzedzony będzie powiadomieniem z wyprzedzeniem co najmniej 7 dni roboczych i będzie prowadzony w dni robocze, w sposób zapewniający bezpieczeństwo i poufność danych innych klientów Wykonawcy; osoby audytujące zobowiązane będą do zachowania poufności; każda Strona ponosi własne koszty. Ograniczenia te nie dotyczą audytu związanego z incydemem ani działań organu nadzorczego. Zamawiający może w pierwszej kolejności wykorzystać przedstawione certyfikaty, raporty lub wyniki niezależnych audytów bezpieczeństwa, co nie wyłącza uprawnień Administratora wynikających z art. 28 RODO.

Pytanie 33 — przekazanie danych po zakończeniu umowy

Treść pytania: „Czy Zamawiający może wskazać przewidywany format i sposób przekazania danych po zakończeniu umowy? Która ze Stron dostarcza zewnętrzny dysk twardy, jaka ma być jego minimalna pojemność, czy dane mają być zaszyfrowane oraz jaki jest termin ich przekazania? Czy termin usunięcia wszystkich kopii danych może rozpocząć bieg po potwierdzeniu przez Zamawiającego kompletności i poprawności przekazanych danych?”

Odpowiedź: Zewnętrzny dysk dostarcza Wykonawca w ramach wynagrodzenia ryczałtowego (§ 3 ust. 4 wzoru umowy); nośnik ma być zaszyfrowany, o pojemności odpowiadającej wolumenowi danych. Pakiet przekazania obejmuje co najmniej: zrzut bazy danych (SQL), pliki i załączniki serwisu, eksport instancji GitLab, konfiguracje niezbędne do odtworzenia środowiska oraz ostatnią pełną, poprawną kopię zapasową. Przekazanie nastąpi w terminie 7 dni od zakończenia umowy; Zamawiający zweryfikuje kompletność pakietu w terminie 7 dni od jego otrzymania; klucz do zaszyfrowanego nośnika zostanie przekazany odrębnym kanałem. Usunięcie pozostałych kopii danych nastąpi w terminie 7 dni od potwierdzenia kompletności przez Zamawiającego, z zastrzeżeniem kopii niezmiennych, które wygasają zgodnie z retencją — nie później niż 4 tygodnie od zakończenia umowy (zob. Część II, odpowiedź na pytanie 19).

Pytanie 34 — przesłanki natychmiastowego wypowiedzenia umowy

Treść pytania: „Czy Zamawiający może rozważyć doprecyzowanie, że do liczby zgłoszeń stanowiącej przesłankę wypowiedzenia będą zaliczane zgłoszenia uzasadnione, dotyczące przyczyn leżących po stronie Wykonawcy i potwierdzone po zakończeniu analizy incydentu, z pominięciem zgłoszeń powielonych lub odnoszących się do tego samego zdarzenia?”

Odpowiedź: Zamawiający doprecyzowuje, że do liczby zgłoszeń, o której mowa w § 10 ust. 1 pkt 1 wzoru umowy, wliczane będą wyłącznie zgłoszenia zasadne, dotyczące przyczyn leżących po stronie Wykonawcy, potwierdzone po zakończeniu analizy zdarzenia; zgłoszenia powielone lub dotyczące tego samego zdarzenia traktowane będą jako jedno zgłoszenie.

Pytanie 35 — kumulacja kar i odpowiedzialność odszkodowawcza

Treść pytania: „Czy Zamawiający może rozważyć przyjęcie, że za to samo zdarzenie lub naruszenie nie będą naliczane równocześnie różne kary umowne, a łączna odpowiedzialność Wykonawcy z tytułu kar i odszkodowań zostanie ograniczona do ustalonego poziomu całkowitego wynagrodzenia, z wyjątkiem szkód wyrządzonych umyślnie oraz przypadków, w których takie ograniczenie nie jest dopuszczalne na mocy prawa?”

Odpowiedź: Zamawiający potwierdza, że za to samo zdarzenie (to samo naruszenie) nie będzie naliczana więcej niż jedna kara umowna — w przypadku zbiegu podstaw zastosowanie znajdzie kara wyższa. Przed naliczeniem kary Wykonawca może przedstawić wyjaśnienia; kara za naruszenie innych obowiązków (§ 5 ust. 6) naliczana będzie wyłącznie w przypadku naruszeń istotnych, nieusuniętych mimo wezwania i wyznaczenia odpowiedniego terminu. Łączna wysokość kar umownych pozostaje ograniczona zgodnie z § 5 ust. 14 wzoru umowy. Zamawiający nie wyraża zgody na ograniczenie łącznej odpowiedzialności odszkodowawczej Wykonawcy do wysokości wynagrodzenia; § 5 ust. 17 pozostaje bez zmian.

Pytanie 36 — przedłużenie terminu składania ofert

Treść pytania: „Czy Zamawiający rozważy przedłużenie terminu składania ofert w taki sposób, aby Wykonawcy dysponowali co najmniej 3 dniami roboczymi od dnia przekazania odpowiedzi na pytania na przygotowanie i złożenie oferty?”

Odpowiedź: Termin składania ofert został przedłużony do dnia 30 lipca 2026 r., do godz. 12:00 (komunikaty z 23 i 27 lipca 2026 r.). Zob. także Część II, odpowiedź na pytanie 21.

Część II. Odpowiedzi na pytania z pisma drugiego (wptyw: 22.07.2026)

Pismo drugie w przeważającej mierze dotyczy zagadnień objętych pismem pierwszym; w takim zakresie Zamawiający odsyła do odpowiedzi z Części I, które pozostają wiążące. Poniżej wskazano odpowiedzi na elementy nowe oraz stanowisko wobec wniosków o zmianę dokumentacji.

Pytanie 1 — termin rozpoczęcia usługi i warunki uruchomienia

Treść pytania: „Prosimy o jednoznaczne wskazanie przewidywanego terminu zawarcia umowy oraz potwierdzenie, czy usługa ma być świadczona od 16 sierpnia 2026 r. do 16 sierpnia 2027 r., czy przez 12 miesięcy od podpisania protokołu zdawczo-odbiorczego. Jak należy stosować 14-dniowy termin uruchomienia, jeżeli zawarcie umowy albo przekazanie danych, dostępów lub dokumentacji nastąpi w terminie uniemożliwiającym rozpoczęcie usługi 16 sierpnia 2026 r.?”

Wniosek o zmianę: „Prosimy o przyjęcie, że termin uruchomienia będzie od dnia przekazania Wykonawcy kompletnych i prawidłowych danych, kopii systemu, dostępów, dokumentacji oraz informacji konfiguracyjnych, a opóźnienia wynikające z braku współdziałania Zamawiającego lub dotychczasowego operatora odpowiednio przedłużają termin i nie stanowią zwłoki Wykonawcy.”

Odpowiedź: Zob. odpowiedzi na pytania 1 i 2 w Części I. Wniosek o zmianę: Zamawiający nie wprowadza zmiany umowy w tym zakresie — skutek, o który wnosi wykonawca, zapewniają § 5 ust. 16 wzoru umowy oraz potwierdzenie zawarte w odpowiedzi na pytanie 2 (Część I).

Pytanie 2 — stan obecny, wolumen danych i organizacja migracji

Treść pytania: „Prosimy o przekazanie opisu aktualnego środowiska i migracji, obejmującego co najmniej: liczbę i parametry wszystkich maszyn lub usług oraz dokładne wersje systemów i komponentów; aktualne wykorzystanie przestrzeni przez bazę danych, pliki i załączniki, środowisko testowe, GitLab oraz pocztę, wraz ze średnim miesięcznym przyrostem danych; średni i maksymalny transfer, liczbę użytkowników równoczesnych oraz okresy szczytowego obciążenia; format przekazania maszyn, baz, plików, konfiguracji, repozytoriów, rekordów DNS i certyfikatów; zakres udziału dotychczasowego operatora, dostęp administracyjny dla nowego Wykonawcy, dopuszczalne okno niedostępności, migrację próbną oraz procedurę powrotu do poprzedniego środowiska; podmiot odpowiedzialny za testy funkcjonalne i potwierdzenie kompletności oraz poprawności danych po migracji.”

Odpowiedź: Zob. odpowiedzi na pytania 3 i 4 w Części I. Uzupełniająco: migracja próbna nie jest wymagana; wymagany jest plan migracji obejmujący weryfikację danych i możliwość powrotu do poprzedniego środowiska; testy funkcjonalne po migracji oraz potwierdzenie kompletności danych wykonuje Zamawiający; format przekazania danych zostanie uzgodniony z wybranym wykonawcą (w szczególności zrzut bazy danych i archiwum

plików). W pozostałym zakresie Zamawiający nie udostępnia inwentaryzacji stanu obecnego środowiska; wycenę należy oprzeć wyłącznie na wiążących parametrach docelowych oraz wartościach granicznych wskazanych w OPZ i niniejszych odpowiedziach, jednakowo dla wszystkich wykonawców.

Pytanie 3 — podział odpowiedzialności za infrastrukturę, system i aplikację

Treść pytania: „Prosimy o jednoznaczne wskazanie, czy odpowiedzialność Wykonawcy obejmuje wyłącznie infrastrukturę, wirtualizację, system operacyjny i usługi systemowe, czy również kod aplikacji SOP, framework Yii, zależności aplikacyjne, strukturę i zapytania bazy danych, procesy CI/CD, integracje zewnętrzne oraz dostarczalność wiadomości e-mail. Która Strona odpowiada za testy aplikacyjne po aktualizacjach, migracjach i zmianach konfiguracji?”

Wniosek o zmianę: „Prosimy o potwierdzenie, że naprawa kodu aplikacji, optymalizacja zapytań, modyfikacje funkcjonalne oraz dostosowanie aplikacji do nowych wersji komponentów nie są objęte wynagrodzeniem ryczałtowym, chyba że zostaną wyraźnie zlecone i odrębnie wycenione.”

Odpowiedź: Zob. odpowiedź na pytanie 21 w Części I. Wniosek o zmianę: Zamawiający potwierdza, że naprawa kodu aplikacji, optymalizacja zapytań, modyfikacje funkcjonalne oraz dostosowanie aplikacji do nowych wersji komponentów nie są objęte wynagrodzeniem ryczałtowym ani przedmiotem zamówienia.

Pytanie 4 — znaczenie hostingu dedykowanego i sposób przydziału zasobów

Treść pytania: „Prosimy o potwierdzenie, że pojęcie „hosting dedykowany” oznacza wydzielone logicznie środowisko wirtualne przeznaczone dla systemu SOP, a nie fizyczne serwery użytkowane wyłącznie przez Zamawiającego. Czy dopuszczalne jest uruchomienie maszyn wirtualnych na współdzielonym klastrze centrum danych przy zachowaniu separacji, wymaganej wydajności, bezpieczeństwa i dostępności? Czy Zamawiający wymaga rezerwacji CPU i RAM albo określonego limitu overcommitmentu?”

Odpowiedź: Zob. odpowiedź na pytanie 5 w Części I.

Pytanie 5 — parametry serwerów produkcyjnych, równowaga CPU, storage i skalowanie

Treść pytania: „Prosimy o potwierdzenie, że zapis „2.10Mhz” oznacza 2,10 GHz oraz że dopuszczalne jest zastosowanie dowolnego procesora x86-64, w tym AMD EPYC, zapewniającego wydajność nie niższą niż wymagana, niezależnie od producenta i częstotliwości taktowania. Prosimy także o wskazanie minimalnych parametrów storage: IOPS, przepustowości, maksymalnego opóźnienia i wymaganego poziomu redundancji. Czy wymóg NVMe dotyczy fizycznych nośników, czy wymaganej wydajności warstwy dyskowej?”

Wniosek o zmianę: „Prosimy o podanie maksymalnego przewidywanego zwiększenia CPU, RAM i przestrzeni dyskowej oraz wprowadzenie cennika jednostkowego lub zasad zmiany wynagrodzenia za zasoby uruchamiane ponad wartości minimalne.”

Odpowiedź: Zob. odpowiedź na pytanie 6 w Części I. Uzupełniająco: wymóg NVMe oznacza zastosowanie nośników NVMe lub rozwiązania o wydajności warstwy dyskowej nie niższej; Zamawiający nie określa minimalnych wartości IOPS, przepustowości ani opóźnień — Wykonawca odpowiada za wydajność zapewniającą prawidłowe działanie serwisu i dotrzymanie SLA. Wniosek o zmianę (cennik zasobów dodatkowych): Zamawiający nie wprowadza cennika jednostkowego. Parametry określone w OPZ wyznaczają zakres objęty wynagrodzeniem ryczałtowym; zwiększenie zasobów ponad te parametry nie jest objęte przedmiotem zamówienia i może nastąpić wyłącznie na podstawie odrębnego, zgodnego z przepisami uzgodnienia Stron.

Pytanie 6 — parametry i zakres środowiska testowego

Treść pytania: „Prosimy o podanie minimalnych parametrów obu serwerów testowych: vCPU, RAM, przestrzeni dyskowej, wydajności storage, adresacji oraz wersji oprogramowania. Czy środowisko testowe ma być stale uruchomione i objęte tym samym SLA, monitoringiem 24/7, backupem, aktualizacjami, firewallem i ochroną anty-DDoS co produkcja?”

Odpowiedź: Zob. odpowiedź na pytanie 7 w Części I.

Pytanie 7 — prywatna instancja GitLab

Treść pytania: „Prosimy o wskazanie, czy należy przenieść istniejącą instancję, czy uruchomić nową, oraz czy GitLab ma działać na odrębnej maszynie. Prosimy o podanie wymaganej edycji i wersji, liczby użytkowników i projektów, aktualnej wielkości repozytoriów i przyrostu danych, wykorzystywania GitLab Runner, CI/CD, Container Registry, artefaktów i pakietów, minimalnych zasobów, wymagań SLA oraz zakresu i retencji backupu.”

Odpowiedź: Zob. odpowiedź na pytanie 8 w Części I.

Pytanie 8 — zakres usługi pocztowej, skrzynki i wolumen wysyłki

Treść pytania: „Prosimy o jednoznaczne wskazanie, czy wymaganie dotyczy wyłącznie usługi SMTP relay lub dedykowanego serwera SMTP do wysyłania powiadomień, czy pełnego systemu pocztowego umożliwiającego odbieranie i przechowywanie wiadomości. Jeżeli wymagane są skrzynki pocztowe, prosimy o podanie ich liczby, pojemności pojedynczej i łącznej, aktualnej zajętości, przewidywanego przyrostu, retencji, liczby aliasów i list dystrybucyjnych, wymaganych protokołów, webmaila oraz wymagań backupu i odtwarzania.”

Wniosek o zmianę: „Niezależnie od powyższego prosimy o podanie średniej i maksymalnej liczby wiadomości na godzinę i dobę, maksymalnego rozmiaru wiadomości, liczby domen i adresów nadawczych, wymogu dedykowanego IP oraz podziału odpowiedzialności za SPF, DKIM, DMARC, PTR i reputację. Prosimy o potwierdzenie, że Wykonawca nie odpowiada za odrzucenie lub klasyfikację wiadomości przez zewnętrzne systemy odbiorców, jeżeli wysyłka i konfiguracja po jego stronie są prawidłowe.”

Odpowiedź: Zob. odpowiedź na pytanie 9 w Części I, która potwierdza również kwestie objęte wnioskiem o zmianę (wolumen, podział odpowiedzialności za SPF/DKIM/DMARC/PTR i reputację oraz brak odpowiedzialności Wykonawcy za klasyfikację wiadomości przez systemy odbiorców przy prawidłowej wysyłce i konfiguracji).

Pytanie 9 — łącze, transfer, adresacja, VPN i integracje

Treść pytania: „Prosimy o wskazanie, czy 1 Gbps oznacza przepustowość portu, czy gwarantowane pasmo symetryczne dla systemu SOP, czy transfer ma być nielimitowany oraz jakie są aktualne i prognozowane wolumeny transferu. Prosimy o podanie wymaganej liczby publicznych adresów IPv4 i IPv6 dla aplikacji, GitLab, poczty i pozostałych usług oraz potwierdzenie, czy dopuszczalne są NAT i reverse proxy. Czy wymagane jest stałe połączenie site-to-site VPN z siecią Zamawiającego, a jeżeli tak — z jaką przepustowością, redundancją, adresacją i routingiem? Prosimy również o wykaz integracji zewnętrznych, wymaganych portów, adresów i certyfikatów.”

Odpowiedź: Zob. odpowiedzi na pytania 10, 11 i 14 w Części I.

Pytanie 10 — zakres, technologia, retencja, RPO i RTO kopii zapasowych

Treść pytania: „Prosimy o określenie: komponentów objętych backupem (produkcja, test, GitLab, poczta, konfiguracje systemowe, firewall i inne usługi); wymaganego RPO oraz RTO dla bazy, plików, pojedynczej maszyny i całego środowiska; retencji kopii wykonywanych co 6 godzin i kopii tygodniowych, minimalnej liczby punktów odtworzenia oraz ewentualnej retencji miesięcznej lub rocznej; wymagania point-in-time recovery dla bazy danych; dopuszczalności backupu obrazowego, agentowego, kopii syntetycznej pełnej, deduplikacji, kompresji, szyfrowania i niezmienności kopii; znaczenia „niezależnej geograficznie lokalizacji”, w tym minimalnej odległości i dopuszczenia drugiego centrum danych tego samego Wykonawcy z odrębnym budynkiem, zasilaniem i telekomunikacją.”

Odpowiedź: Zob. odpowiedzi na pytania 15–18 w Części I. Uzupełniająco: odtwarzanie point-in-time bazy danych ponad wymagany cykl kopii co 6 godzin nie jest wymagane; dopuszcza się backup obrazowy i agentowy, kopie syntetyczne pełne, deduplikację, kompresję oraz kopie niezmiennicze.

Pytanie 11 — zakres i kryteria testów odtworzeniowych

Treść pytania: „Prosimy o wskazanie, czy test ma obejmować pojedynczy plik, bazę danych, wybraną maszynę czy kompletne uruchomienie systemu. Kto wybiera zakres danych, zapewnia zasoby tymczasowe, wykonuje testy funkcjonalne aplikacji i zatwierdza wynik? Jakie są mierzalne kryteria pozytywnego odbioru i czy test może być przeprowadzony w izolowanym środowisku Wykonawcy? Prosimy o potwierdzenie, że test przed rozpoczęciem usługi nastąpi po przekazaniu kompletnej, poprawnej kopii danych.”

Odpowiedź: Zob. odpowiedź na pytanie 19 w Części I.

Pytanie 12 — cykl życia oprogramowania i aktualizacje bezpieczeństwa

Treść pytania: „PHP 8.1 nie jest już objęte oficjalnym wsparciem bezpieczeństwa, a Debian 12 jest obecnie wydaniem oldstable objętym LTS. Prosimy o wskazanie, czy przed rozpoczęciem lub w trakcie umowy przewidywana jest aktualizacja PHP, Debiana i pozostałych komponentów oraz która Strona odpowiada za dostosowanie i testy aplikacji. Prosimy również o zdefiniowanie „aktualizacji krytycznej”, źródła klasyfikacji i poziomu CVSS oraz momentu rozpoczęcia terminu 72 godzin.”

Wniosek o zmianę: „Prosimy o przyjęcie, że termin 72 godzin ulega zawieszeniu na czas testów, oczekiwania na zgodę lub współdziałanie Zamawiającego, a Wykonawca nie odpowiada za brak poprawek producenta ani za skutki odmowy lub opóźnienia akceptacji aktualizacji przez Zamawiającego.”

Odpowiedź: System SOP jest istniejącą aplikacją zbudowaną w środowisku Yii 2.0.49 / PHP 8.1 i wymagane jest uruchomienie środowiska zgodnego z aplikacją. Zamawiający wyjaśnia, że: (a) bazową wymaganą wersją środowiska PHP jest 8.1, przy czym Wykonawca zapewni aktualizacje bezpieczeństwa tego środowiska — dopuszcza się zastosowanie komercyjnie wspieranych buildów PHP 8.1 zgodnych z systemem Debian 12, ze wskazaniem w ofercie dostawcy i okresu wsparcia; (b) Zamawiający dopuszcza aktualizację środowiska do PHP 8.3 lub nowszej wersji objętej wsparciem — zarówno w trakcie trwania umowy, jak i od rozpoczęcia świadczenia usługi — pod warunkiem pozytywnego wyniku testów aplikacji w środowisku testowym przed przełączeniem produkcyjnym i uzgodnienia z Zamawiającym; dostosowanie i testy aplikacji pozostają po stronie Zamawiającego; wersja PHP 8.2 nie jest wersją docelową, ponieważ jej wsparcie bezpieczeństwa kończy się przed upływem okresu umowy; (c) wymagany system operacyjny to Debian 12 (objęty wsparciem bezpieczeństwa LTS) lub — po uzgodnieniu z Zamawiającym — nowsze stabilne wydanie systemu Debian; zmiana rodziny dystrybucji (w tym CloudLinux OS, AlmaLinux) nie jest dopuszczalna. Za dostosowanie i testy aplikacji po aktualizacjach komponentów odpowiada Zamawiający, zgodnie z podziałem odpowiedzialności wskazanym w odpowiedzi na pytanie 21 (Część I). W zakresie definicji aktualizacji krytycznej, biegu terminu 72 godzin i jego zawieszenia — zob. odpowiedź na pytanie 22 w Części I; w zakresie tam wskazanym wniosek o zmianę zostaje uwzględniony. Wykonawca nie odpowiada za brak poprawki producenta dla komponentu, dla którego poprawka nie została udostępniona, o ile spełnia wymagania określone w lit. a powyżej.

Pytanie 14 — dostęp administracyjny, monitoring, logi i incydenty bezpieczeństwa

Treść pytania: „Prosimy o wskazanie minimalnego zakresu monitoringu, w tym dostępności, parametrów wydajności, przestrzeni dyskowej, backupu, certyfikatów i testów funkcjonalnych aplikacji, oraz informacji, czy Zamawiający oczekuje dostępu do panelu. Prosimy o określenie, czy 90-dniowa retencja dotyczy wyłącznie działań administracyjnych, czy również logów systemowych, aplikacyjnych, bazodanowych, firewall, reverse proxy, poczty i GitLab. Prosimy także o określenie maksymalnego czasu zgłoszenia incydentu bezpieczeństwa i wymaganego zakresu raportu.”

Odpowiedź: Zob. odpowiedzi na pytania 23 i 24 w Części I. Uzupełniając: Wykonawca zgłasza Zamawiającemu incydent bezpieczeństwa bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od jego stwierdzenia (termin 24 godzin stanowi maksimum kontraktowe; w przypadku naruszenia ochrony danych osobowych zgłoszenie następuje bez zbędnej zwłoki, zgodnie z § 9 ust. 4 lit. j wzoru umowy); zgłoszenie wstępne może być uzupełniane i obejmuje co najmniej charakter incydentu, czas wystąpienia, dotknięte usługi i dane, przewidywany wpływ oraz podjęte działania.

Pytanie 15 — kanały, priorytety oraz czasy reakcji i przywrócenia

Treść pytania: „Prosimy o potwierdzenie, czy wymagane są wszystkie trzy kanały: system zgłoszeniowy, telefon i e-mail, czy telefon oraz jeden kanał elektroniczny. Prosimy o wprowadzenie kategorii zgłoszeń co najmniej dla awarii krytycznej, wysokiej, zwykłej i konsultacji oraz określenie dla każdej kategorii czasu potwierdzenia, reakcji, rozpoczęcia prac, przywrócenia usługi i docelowego rozwiązania. Czy termin 10 godzin dotyczy wyłącznie awarii powodujących częściowy dostęp, czy także całkowitej niedostępności, konsultacji i problemów aplikacyjnych?”

Odpowiedź: Zob. odpowiedzi na pytania 25 i 26 w Części I. Termin 10 godzin obejmuje także całkowitą niedostępność usługi, z zastrzeżeniem terminu 24 godzin dla odtworzenia pełnego środowiska po rozległej awarii (Część I, odpowiedź na pytanie 18).

Pytanie 16 — sposób pomiaru SLA, wyłączenia i limit 50 godzin

Treść pytania: „Prosimy o określenie punktu, narzędzia i częstotliwości pomiaru, monitorowanych usług, liczby nieudanych prób wymaganych do stwierdzenia awarii oraz momentu jej rozpoczęcia i zakończenia. Prosimy o potwierdzenie, że do SLA nie wlicza się uzgodnionych i awaryjnych prac bezpieczeństwa, błędów aplikacji i integracji poza zakresem Wykonawcy, działań Zamawiającego, awarii usług podmiotów niezależnych, ataków przekraczających uzgodniony poziom ochrony i siły wyższej.”

Wniosek o zmianę: „Prosimy o zmianę § 5 ust. 7 przez wskazanie, że limit 50 godzin obejmuje wyłącznie przerwy zawinione przez Wykonawcę i przekraczające dopuszczalne miesięczne limity SLA, z wyłączeniem przerw planowanych i pozostałych wyłączeń SLA.”

Odpowiedź: Zob. odpowiedzi na pytania 27 i 28 w Części I. W zakresie limitu 50 godzin: Zamawiający doprecyzowuje, że do limitu, o którym mowa w § 5 ust. 7 wzoru umowy, wliczane są wyłącznie przerwy przypisane Wykonawcy, stanowiące naruszenie gwarantowanego poziomu dostępności (tj. przekraczające dopuszczalny miesięczny limit niedostępności), z wyłączeniem przerw niewliczanych do czasu niedostępności zgodnie z odpowiedzią na pytanie 28 (Część I). Wniosek o zmianę zostaje uwzględniony w powyższym zakresie.

Pytanie 17 — raporty, konsultacje i prace dodatkowe

Treść pytania: „Prosimy o wskazanie zakresu i formatu raportu, maksymalnej częstotliwości żądania oraz potwierdzenie, czy wystarczający będzie standardowy raport miesięczny obejmujący SLA, zgłoszenia, backupy, wykorzystanie zasobów, aktualizacje i zdarzenia bezpieczeństwa. Prosimy również o określenie liczby godzin konsultacji i prac administracyjnych wliczonych w miesięczny ryczałt oraz zasad zlecania i rozliczania prac dodatkowych, zmian aplikacyjnych i zwiększenia zasobów.”

Odpowiedź: Zob. odpowiedź na pytanie 29 w Części I. Uzupełniająco: konsultacje i pomoc techniczna w ramach ryczałtu (§ 2 ust. 4 pkt 4) dotyczą funkcjonowania usługi hostingu i nie obejmują prac rozwojowych, zmian kodu aplikacji ani prac aplikacyjnych; Zamawiający nie wprowadza limitu godzin. Prace dodatkowe oraz zwiększenie zasobów wymagają odrębnego uzgodnienia Stron.

Pytanie 18 — odbiór miesięczny i podstawa wystawienia faktury

Treść pytania: „Czy brak przekazania przez Zamawiającego protokołu albo szczegółowych zastrzeżeń w terminie 3 dni roboczych będzie uprawniał Wykonawcę do wystawienia faktury? Czy wady nieistotne, które nie uniemożliwiają korzystania z usługi, mogą powodować negatywny odbiór całego miesiąca?”

Wniosek o zmianę: „Prosimy o przyjęcie, że brak zastrzeżeń w terminie 3 dni roboczych oznacza odbiór usługi bez zastrzeżeń i uprawnia do wystawienia faktury, a wady nieistotne podlegają usunięciu w uzgodnionym terminie bez wstrzymania całego wynagrodzenia.”

Odpowiedź: Zob. odpowiedź na pytanie 30 w Części I; wniosek o zmianę zostaje uwzględniony w zakresie tam wskazanym.

Pytanie 19 — podwykonawcy, dalsze powierzenie, audyty i usuwanie danych

Treść pytania: „Prosimy o wyjaśnienie relacji między obowiązkiem uprzedniego poinformowania o zmianie podwykonawcy a wymogiem pisemnej zgody na dalsze powierzenie, terminu udzielenia zgody lub sprzeciwu oraz statusu dostawców kolokacji i telekomunikacji bez dostępu do danych. Prosimy o określenie zasad audytów: powiadomienia, częstotliwości, godzin, kosztów, poufności i ochrony danych innych klientów oraz możliwości wykorzystania certyfikatów lub raportów niezależnych. Czy dane w niezmiennych kopiach mogą zostać usunięte przez automatyczne wygaśnięcie zgodnie z retencją, przy zablokowaniu ich wykorzystania poza wymaganiami prawa?”

Odpowiedź: Zob. odpowiedzi na pytania 31 i 32 w Części I. Uzupełniająco, w zakresie kopii niezmiennych: dane zawarte w kopiach zapasowych wykonanych w technologii uniemożliwiającej ich wcześniejsze usunięcie mogą zostać usunięte poprzez automatyczne wygaśnięcie zgodnie z uzgodnioną retencją, pod warunkiem logicznego odseparowania tych kopii po zakończeniu umowy, zakazu ich dalszego wykorzystania oraz przekazania Zamawiającemu potwierdzenia usunięcia po wygaśnięciu ostatniej kopii.

Pytanie 20 — kary umowne, odpowiedzialność i przesłanki wypowiedzenia

Treść pytania: „Czy Zamawiający potwierdzi, że kary będą naliczane wyłącznie za zawinione naruszenia Wykonawcy, po umożliwieniu mu przedstawienia wyjaśnień, a za jedno zdarzenie nie będzie naliczana więcej niż jedna kara? Prosimy o doprecyzowanie, że kara za „inne obowiązki” dotyczy wyłącznie istotnego naruszenia nieusuniętego mimo wezwania. Czy przy przesłance wypowiedzenia opartej na liczbie zgłoszeń uwzględniane będą wyłącznie zgłoszenia uzasadnione, dotyczące przyczyn leżących po stronie Wykonawcy, przy czym zgłoszenia powielone lub dotyczące tego samego zdarzenia będą traktowane łącznie?”

Wniosek o zmianę: „Prosimy o wprowadzenie zakazu kumulacji kar za to samo zdarzenie, procedury wezwania do usunięcia naruszenia oraz ograniczenia łącznej odpowiedzialności Wykonawcy z tytułu kar i odszkodowań do 100%

maksymalnego wynagrodzenia brutto, z wyjątkiem szkód wyrządzonych umyślnie i przypadków, w których ograniczenie jest prawnie niedopuszczalne.”

Odpowiedź: Zob. odpowiedzi na pytania 34 i 35 w Części I. Wniosek o zmianę: uwzględniony w zakresie zakazu naliczania więcej niż jednej kary za to samo zdarzenie oraz doprecyzowania przesłanki wypowiedzenia; w zakresie ograniczenia łącznej odpowiedzialności odszkodowawczej — nieuwzględniony.

Pytanie 21 — przedłużenie terminu składania ofert

***Treść pytania:** „Czy Zamawiający przedłuży termin składania ofert w taki sposób, aby wykonawcy dysponowali co najmniej 5 dniami roboczymi od dnia przekazania kompletnych odpowiedzi i opublikowania ewentualnych zmian dokumentacji?”*

***Wniosek o zmianę:** „Wnosimy o wyznaczenie nowego terminu przypadającego nie wcześniej niż w piątym dniu roboczym po przekazaniu pełnych odpowiedzi.”*

Odpowiedź: Termin składania ofert został przedłużony do dnia 30 lipca 2026 r., do godz. 12:00 (komunikaty z 23 i 27 lipca 2026 r.). Zamawiający uznaje ten termin za wystarczający z uwagi na zakres udzielonych wyjaśnień, które w przeważającej mierze potwierdzają lub doprecyzowują dotychczasową treść dokumentacji, oraz z uwagi na planowany termin rozpoczęcia świadczenia usługi (1 września 2026 r.) i konieczność wcześniejszego zawarcia umowy oraz przeprowadzenia migracji; dalsze przedłużenie zagrażałoby ciągłości działania serwisu. W pozostałym zakresie wniosek nie zostaje uwzględniony.

Część III. Odpowiedzi na pytania przekazane pocztą elektroniczną (wpływ: 20.07.2026)

Pytanie 1 — wersja środowiska PHP (8.1 — status wsparcia)

***Treść pytania:** „W specyfikacji systemu (Załącznik nr 1) wskazano wymóg zastosowania środowiska PHP w wersji 8.1. Zwracamy uwagę, że wersja ta posiada status End-of-Life (EOL), co oznacza oficjalny brak wsparcia i nieotrzymywanie kluczowych łatek bezpieczeństwa od jej twórców. Biorąc pod uwagę wymóg instalacji krytycznych aktualizacji bezpieczeństwa w czasie do 72 godzin od ich udostępnienia, prosimy o odpowiedź: Czy Zamawiający dopuszcza wdrożenie nowszej i wspieranej wersji PHP (np. 8.2 lub 8.3)? W przypadku twardego wymogu pozostania przy PHP 8.1 (np. z racji ograniczeń frameworka Yii), czy Zamawiający wyraża zgodę na zastosowanie wyspecjalizowanego systemu klasy CloudLinux OS, który oferuje komercyjne wsparcie (HardenedPHP) na starsze wersje środowiska?”*

Odpowiedź: Zob. Część II, odpowiedź na pytanie 12. Zamawiający dopuszcza wdrożenie PHP 8.3 lub nowszej wersji objętej wsparciem — także od rozpoczęcia świadczenia usługi — pod warunkiem pozytywnego wyniku testów aplikacji w środowisku testowym przed przełączeniem produkcyjnym i uzgodnienia z Zamawiającym; bazową wersją środowiska pozostaje PHP 8.1 z zapewnionymi aktualizacjami bezpieczeństwa (komercyjnie wspierany build zgodny z Debianem 12). Zastosowanie systemu CloudLinux OS oznaczałoby zmianę wymaganej rodziny systemu operacyjnego i nie jest dopuszczalne.

Pytanie 2 — system operacyjny (Debian 12 — cykl wsparcia)

***Treść pytania:** „W OPZ narzucono wykorzystanie systemu operacyjnego Debian 12. Biorąc pod uwagę bieżący cykl wsparcia dla tej dystrybucji, która obecnie znajduje się głównie w fazie rozszerzonego wsparcia bezpieczeństwa (LTS), czy Zamawiający dopuszcza zaproponowanie nowszego środowiska serwerowego o długotrwałym wsparciu (np. aktualna wersja systemu Debian lub dystrybucje AlmaLinux)?”*

Odpowiedź: Zob. Część II, odpowiedź na pytanie 12. Wymagany jest Debian 12 (objęty wsparciem bezpieczeństwa LTS) lub — po uzgodnieniu z Zamawiającym — nowsze stabilne wydanie systemu Debian. Dystrybucje innych rodzin (w tym AlmaLinux) nie są dopuszczalne.

Pytanie 3 — parametry środowiska testowego

***Treść pytania:** „Zamawiający w Załączniku nr 1 informuje o konieczności uruchomienia środowiska testowego (1 serwer app + 1 serwer bazy danych), lecz nie określa jego parametrów brzegowych (RAM, vCPU, NVME). Prosimy o wskazanie minimalnych oczekiwanych parametrów środowiska testowego, bez których niemożliwa jest rzetelna wycena wymaganej infrastruktury.”*

Odpowiedź: Zob. Część I, odpowiedź na pytanie 7.

Pytanie 4 — zakres uprawnień dostępowych Zamawiającego

Treść pytania: „W związku z wymogami opisanymi w OPZ, nakładającymi na Wykonawcę pełną odpowiedzialność za administrację środowiskiem, jego bezpieczeństwo, poprawne działanie oraz rygorystyczne warunki SLA, prosimy o doprecyzowanie kwestii uprawnień dostępowych dla Zamawiającego. Zgodnie z najlepszymi praktykami rynkowymi dla usług utrzymaniowych (model managed) oraz standardami bezpieczeństwa (m.in. ISO 27001), pełen dostęp administracyjny (root) musi znajdować się wyłącznie pod kontrolą podmiotu odpowiedzialnego za SLA. Czy Zamawiający potwierdza, że do standardowej obsługi własnej aplikacji i warstwy developerskiej oczekuje wyłącznie dostępu nieuprzywilejowanego (tj. na poziomie standardowego użytkownika, realizowanego np. poprzez SSH, SFTP, panel lub repozytorium kodu, bez uprawnień root)?”

Odpowiedź: Uprawnienia root do warstwy systemowej pozostają pod kontrolą Wykonawcy odpowiedzialnego za administrację środowiskiem i dotrzymanie SLA. Zamawiający oraz osoby przez niego wskazane (w tym podmiot utrzymujący aplikację SOP) otrzymają dostęp zgodny z zasadą najmniejszych uprawnień, w zakresie niezbędnym do utrzymania i rozwoju aplikacji, obejmujący co najmniej: dostęp SSH/SFTP do zasobów aplikacji, dostęp do bazy danych, logów aplikacyjnych, konfiguracji aplikacyjnych oraz repozytorium kodu. Jeżeli określone czynności wdrożeniowe wymagają podwyższonych uprawnień, będą one nadawane czasowo i imiennie, a działania wykonywane z ich użyciem — rejestrowane; szczegóły zostaną uzgodnione w ramach § 2 ust. 6 wzoru umowy, bez przekazywania stałych poświadczeń root. Wymagania § 2 ust. 12d (indywidualne konta, MFA, ograniczenie dostępu, rejestrowanie działań) stosuje się do wszystkich kont administracyjnych, niezależnie od Strony, której dostęp przyznano.

Niniejsze odpowiedzi wiążą wszystkich wykonawców i zostaną odzwierciedlone w treści umowy zawieranej z wybranym wykonawcą. Termin składania ofert: 30 lipca 2026 r., godz. 12:00. Warunki zaproszenia w zakresie niezmienionym niniejszymi odpowiedziami pozostają bez zmian.