

Wrocław, 12.05.2026

Dotyczy: postępowania o udzielenie zamówienia publicznego pn.
„Wdrożenie systemu rekrutacji i rozliczeń do żłobków oraz jego utrzymanie”, znak postępowania: CUI-ZZ.3201.7.2026

Zamawiający informuje, że do przedmiotowego postępowania wpłynęły wnioski o treści jak poniżej. Działając w trybie art. 137 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 ze zm.) Zamawiający odpowiednio wyjaśnia i zmienia treść SWZ:

1. Załącznik nr 1 do Umowy - Specyfikacja Wymagań.

Pkt. 4. Wymagania funkcjonalne systemu

Sygnatura	Treść pytania - Odpowiedź
WO.01	<p>Czy Zamawiający dopuszcza rozwiązanie, w którym system wyświetla wyłącznie ostrzeżenie o nieaktualnej przeglądarce bez twardego blokowania dostępu, z wyjątkiem przeglądarek starszych niż dwa ostatnie wydania stabilne?</p> <p>Odpowiedź:</p> <p>Zamawiający wymaga, aby zapewnić kompatybilność z przeglądarkami aktualizowanymi przez producenta do trzech lat wstecz. W przypadku wcześniejszych przeglądarek Zamawiający dopuszcza wyświetlanie się komunikatu.</p>
WO.04	<p>Czy umieszczenie logotypu Wykonawcy w stopce lub sekcji 'O systemie' jest traktowane jako informacja reklamowa w rozumieniu niniejszego wymagania, czy też Zamawiający dopuszcza jego obecność za uprzednią akceptacją?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza rozwiązanie.</p>

Sygnatura	Treść pytania - Odpowiedź
WO.15	<p>Czy Zamawiający dopuszcza, aby interfejs integracji z Open Data Wrocław obejmował wyłącznie z góry określony, uzgodniony w Analizie Przedwdrożeńowej zestaw danych anonimowych i statystycznych (np. liczba miejsc, liczba wniosków per placówka), z możliwością późniejszego rozszerzenia zakresu na podstawie osobnego zlecenia?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza takie rozwiązanie.</p>
WO.16	<p>Czy Zamawiający dopuszcza zastąpienie pseudonimizacji/anonimizacji funkcją trwałego usunięcia danych konkretnego dziecka lub rodzica na żądanie operatora?</p> <p>Odpowiedź:</p> <p>Zamawiający nie dopuści zastąpienia pseudonimizacji/anonimizacji funkcją trwałego usunięcia danych. Obie funkcje mają być dostępne niezależnie.</p>
WT.01	<p>Czy Zamawiający dopuszcza, aby logi operacji użytkownika były dostępne w formie dedykowanego raportu w panelu administratora z filtrowaniem po użytkowniku, dacie i typie akcji, bez konieczności przechowywania zapisu każdego kliknięcia w interfejsie użytkownika?</p> <p>Odpowiedź:</p> <p>Struktura logów zostanie doprecyzowana w trakcie Analizy Przedwdrożeńowej.</p>
WT.04	<p>Czy Zamawiający dopuszcza zastąpienie dat obowiązywania konta mechanizmem ręcznego blokowania/odblokowania kont przez Administratora Głównego?</p> <p>Odpowiedź:</p> <p>Zamawiający wymaga obu mechanizmów, zatem nie dopuszcza zastąpienia.</p>
WT.07	<p>Czy Zamawiający akceptuje politykę haseł opartą na aktualnych wytycznych CERT Polska (minimalna długość,</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>brak wymogu rotacji), bez możliwości konfiguracji tych parametrów przez Administratora, mając na uwadze że CERT wycofał zalecenia dotyczące przymusowej zmiany hasła i znaków specjalnych?</p> <p>Odpowiedź:</p> <p>Zamawiający podtrzymuje obecne zapisy.</p>
WT.14	<p>Czy Zamawiający dopuszcza, aby raporty z dużą liczbą kolumn były dostępne wyłącznie w formatach xls/xlsx, natomiast eksport do PDF, csv i xml dotyczył raportów o standardowej strukturze – z uwagi na techniczne ograniczenia formatowania wielokolumnowych zestawień?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza, aby raporty z dużą liczbą kolumn były dostępne wyłącznie w formatach xls/xlsx oraz csv. Określenie dużej ilości kolumn dokonane zostanie w trakcie Analizy Przedwdrożeniowej.</p>
WA.04	<p>Czy Zamawiający dopuszcza zastąpienie wymogu prowadzenia dziennika zmian wersji aplikacji przez Wykonawcę obowiązkiem każdorazowego informowania Administratora Głównego o planowanych zmianach z wyprzedzeniem bez konieczności utrzymywania w Systemie dedykowanego modułu historii wersji?</p> <p>Odpowiedź:</p> <p>Zamawiający nie dopuszcza zastąpienia.</p>
WA.06	<p>W jakim czasie od wdrożenia nowych funkcjonalności lub poprawek baza testowa musi zostać zaktualizowana do wymaganej minimalnej wersji? Czy Zamawiający dopuszcza, aby środowisko testowe zawierało dane anonimizowane w sposób nieodwracalny (bez możliwości odkodowania do danych produkcyjnych), przy czym dostęp do środowiska testowego byłby ograniczony wyłącznie do wskazanych przez Zamawiającego adresów IP — co w praktyce eliminuje potrzebę odtwarzania danych osobowych w środowisku testowym?</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>Odpowiedź:</p> <p>Zamawiający wymaga, aby aktualizacja bazy testowej była dokonana przed wdrożeniem produkcyjnym nowej funkcjonalności, w przypadku poprawek jedynie na żądanie Zamawiającego. Zamawiający dopuszcza by środowisko testowe zawierało dane anonimizowane w sposób nieodwracalny oraz zgadza się by dostęp do środowiska testowego był ograniczonych wyłącznie do wskazanych przez Zamawiającego adresów IP.</p>
SWS.05	<p>Czy Zamawiający dopuszcza, aby blokada kwalifikacji wniosku bez numeru PESEL następowała automatycznie po upływie ustawowego terminu nadania numeru, z możliwością ręcznego odblokowania przez Operatora po uzupełnieniu danych przez rodzica?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza rozwiązanie.</p>
SWS.07	<p>Czy Zamawiający dopuszcza zastąpienie statycznych makiet graficznych dostępem do działającego środowiska demonstracyjnego (demo) systemu, które prezentuje rzeczywisty wygląd i działanie formularzy oraz interfejsu — co pozwoli na bardziej miarodajną ocenę i szybszą akceptację niż wizualizacje w formie makiet?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza rozwiązanie.</p>
SWS.10	<p>Czy Zamawiający dopuszcza, aby układ pól formularza wniosku był ustalony wspólnie w Analizie Przedwdrożeniowej jako stały szablon, bez możliwości dynamicznego przestawiania pól przez Administratora po wdrożeniu?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza takie rozwiązanie.</p>
SWS.11	<p>Czy Zamawiający oczekuje dostarczenia pełnego kreatora, umożliwiającego administratorowi definiowanie zależności</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>warunkowych między polami formularza (np. pokaż/ukryj pole, zmień wymagalność, zmień zakres wartości) bez udziału Wykonawcy, czy dopuszcza częściową konfigurację oraz implementację części logiki po stronie Wykonawcy?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza częściową konfigurację oraz implementację części logiki po stronie Wykonawcy.</p>
SWS.14	<p>Czy Zamawiający dopuszcza, aby blokada edycji danych identyfikacyjnych dziecka (imię, nazwisko, data urodzenia, PESEL) obowiązywała wyłącznie po zatwierdzeniu wniosku przez Operatora, z możliwością korekty przez Administratora Głównego w uzasadnionych przypadkach?</p> <p>Odpowiedź:</p> <p>Zamawiający w procesie rekrutacji nie posiada pojęcia równoznacznego z zatwierdzeniem wniosku, jeżeli w pytaniu chodziło o wniosek oczekujący, to zamawiający dopuszcza blokadę modyfikacji danych w momencie zmiany statusu na zakwalifikowany/wstępnie przyjęty i po przejściu do pracy bieżącej. Operator może zmieniać dane jedynie w module pracy bieżącej na podstawie posiadanych uprawnień.</p>
SWS.19	<p>Czy Zamawiający oczekuje możliwości definiowania odrębnych zestawów kryteriów punktowych dla każdej placówki lub części placówek (np. różnych dla poszczególnych żłobków, w tym żłobków projektowych UE), a także ich samodzielnej konfiguracji?</p> <p>Odpowiedź:</p> <p>Zamawiający oczekuje takiego rozwiązania.</p>
SWS.20	<p>Czy Zamawiający dopuszcza, aby powiadomienia e-mail były wysyłane na adresy wszystkich rodziców/opiekunów wskazanych we wniosku, bez konieczności wskazywania preferowanego adresu korespondencyjnego, z opcją dodania takiego wyboru w kolejnej iteracji systemu?</p> <p>Odpowiedź:</p>

Sygnatura	Treść pytania - Odpowiedź
	Zamawiający nie dopuszcza takiego rozwiązania.
SWS.30	<p>Jakie są różnice pomiędzy formularzami wniosków dla poszczególnych typów żłobków (np. objętych projektami UE) – czy dotyczą one wyłącznie kryteriów rekrutacyjnych, czy również zakresu danych (pól) wymaganych od wnioskodawcy?</p> <p>Odpowiedź:</p> <p>Obecnie Zamawiający nie posiada różnych formularzy wniosków.</p>
SWS.31	<p>Prosimy o wskazanie pełnej listy statusów wniosków, jakie mają obowiązywać w Systemie zgodnie z aktualnym zarządzeniem w sprawie rekrutacji na dany rok żłobkowy.</p> <p>Odpowiedź:</p> <p>Zamawiający oczekuje wprowadzenia statusów wniosków zgodnych z zarządzeniem dostępnym na: https://rekrutacja-zlobki.um.wroc.pl/wroclaw/zlobek/dokumenty</p>
SWS.32	<p>Prosimy o wskazanie szczegółowego zakresu danych, jakie mają być prezentowane użytkownikowi o roli „Rodzic/Opiekun” po zalogowaniu, w tym listy informacji dotyczących wniosku oraz komunikatów systemowych.</p> <p>Odpowiedź:</p> <p>Zamawiający nie jest w stanie na tym etapie wskazać szczegółowego zakresu danych i dokona tego dopiero na etapie Analizy Przedwdrożeniowej. Zestaw danych nie jest stały.</p>
SWS.33	<p>Czy Zamawiający dopuszcza, aby automatyczne usuwanie dokumentów elektronicznych następowało po upływie 24 godzin od ich pierwszego otwarcia przez Operatora, przy czym czas ten liczony jest od zdarzenia otwarcia, a nie od momentu przesłania dokumentu?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza takie rozwiązanie.</p>

Sygnatura	Treść pytania - Odpowiedź
SWS.34	<p>Prosimy o wyjaśnienie rozbieżności w wymaganiu SWS.34: treść OPZ wskazuje 'system może', natomiast kolumna wymagalności określa 'Musi być' – czy ankieta satysfakcji jest wymaganiem obowiązkowym, czy opcjonalnym?</p> <p>Odpowiedź: Wymaganie jest wymaganiem obowiązkowym („musi być”).</p>
SWS.37	<p>Prosimy o doprecyzowanie zasad kontroli liczby zmian wyboru żłobków w ciągu 24h, w szczególności: co Zamawiający rozumie przez „jedną zmianę” (czy powrót do poprzedniego wyboru również ją konsumuje) oraz w jaki sposób liczony jest okres 24h (np. od momentu dokonania zmiany)?</p> <p>Odpowiedź: Zasady kontroli liczby zmian wyboru żłobków zostały określone w Zarządzeniu Nr 4101/25 Prezydenta Wrocławia z dnia 23.12.2025 r. w sprawie przyjęcia zasad postępowania i kryteriów rekrutacji do żłobków wchodzących w skład Wrocławskiego, dokładnie w par. 4.</p>
SWS.40	<p>Prosimy o wyjaśnienie, czy codzienna weryfikacja duplikatów wniosków jest wymagana pomimo istniejącego mechanizmu blokady uniemożliwiającego złożenie więcej niż jednego wniosku dla tego samego dziecka (PESEL), a jeśli tak – jakie dodatkowe przypadki ma ona obejmować.</p> <p>Odpowiedź: Zamawiający wymaga codziennej weryfikacji.</p>
SWS.48	<p>Czy Zamawiający potwierdza, że wymóg dostępności wszystkich modułów systemu poprzez aplikację mobilną (SWS.48) dotyczy wyłącznie modułu Dziennika Elektronicznego, natomiast moduł rekrutacji (składanie i zarządzanie wnioskami) pozostaje dostępny wyłącznie przez przeglądarkę internetową – w tym na urządzeniach mobilnych w trybie responsive web?</p> <p>Odpowiedź:</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>Zamawiający potwierdza, że wymóg dostępności wszystkich modułów systemu poprzez aplikację mobilną (SWS.48) dotyczy wyłącznie modułu Dziennika Elektronicznego.</p>
SWS.53	<p>Czy Zamawiający dopuszcza, aby mechanizm globalnego blokowania kont Rodziców/Opiekunów był dostępny wyłącznie dla Administratora Głównego po stronie Zamawiającego (CUI), bez dostępu dla operatorów placówek, z jednoczesnym wylogowaniem wszystkich aktywnych sesji?</p> <p>Odpowiedź: Zamawiający dopuszcza rozwiązanie.</p>
SWS.54	<p>Czy w przypadku wdrożenia Dziennika Elektronicznego jako odrębnego modułu blokada konta Rodzica/Opiekuna może działać niezależnie w każdym module?</p> <p>Odpowiedź: Konto rekrutacyjne (rodzica) na którym składowane są wnioski rekrutacyjne nie podlega blokadom. Ograniczeniom podlegają jedynie wnioski (zależne od statusu). Natomiast konto w Dzienniku Elektronicznym może zostać zablokowane i blokada ta ma być niezależna od konta rekrutacyjnego.</p>
SWS.60	<p>Czy Zamawiający może wskazać, które raporty historyczne (generowane 'na dany dzień') są krytyczne do uruchomienia systemu, a które mogą zostać dodane w kolejnych fazach wdrożenia, aby umożliwić priorytetyzację prac?</p> <p>Odpowiedź: Zamawiający nie może wskazać na tym etapie. Jest to możliwe dopiero na etapie Analizy Przedwdrożeniowej.</p>
SWS.63	<p>Czy Zamawiający dopuszcza, aby przypisanie placówek do użytkowników odbywało się na poziomie ról (np. Operator żłobka X automatycznie widzi tylko swoją placówkę), bez konieczności ręcznego przypisywania każdej placówki do każdego konta z osobna?</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>Odpowiedź: Zamawiający nie dopuszcza takiego rozwiązania.</p>
SWS.65	<p>Czy Zamawiający dopuszcza, aby podgląd listy użytkowników z możliwością grupowego blokowania był dostępny wyłącznie dla Administratora Głównego na poziomie wszystkich placówek, natomiast Operatorzy widzieliby wyłącznie użytkowników swojej jednostki?</p> <p>Odpowiedź: Zamawiający dopuszcza takie rozwiązanie.</p>
SWS.66	<p>Czy Zamawiający może wskazać minimalne wymagane operacje masowe na kontach użytkowników (np. grupowa blokada, grupowa zmiana roli), aby możliwe było zaprojektowanie rozwiązania dostosowanego do rzeczywistych potrzeb operacyjnych?</p> <p>Odpowiedź: Zamawiający nie jest wskazać na obecnym etapie minimalnych wymaganych operacji masowych. Przedstawi je na etapie Analizy Przedwdrożeniowej.</p>
SWS.67	<p>Czy Zamawiający dopuszcza, aby widoczność przeterminowanych i usuniętych wniosków była realizowana poprzez dedykowany raport z filtrowaniem, zamiast wyświetlania ich bezpośrednio na głównej liście wniosków?</p> <p>Odpowiedź: Zamawiający nie dopuszcza rozwiązania.</p>
SWS.68	<p>Czy Zamawiający dopuszcza, aby grupowe blokowanie kont odbywało się na poziomie placówki (blokada wszystkich operatorów wybranego żłobka) lub typu użytkownika, bez hierarchicznego wyboru na kilku poziomach jednocześnie?</p> <p>Odpowiedź: Zamawiający nie dopuszcza takiego rozwiązania.</p>

Sygnatura	Treść pytania - Odpowiedź
SWS.69	<p>Czy Zamawiający może wskazać szczegółowy zakres danych widocznych dla Operatora na poszczególnych etapach procesu (oczekujący/zakwalifikowany/wstępnie przyjęty), aby możliwe było zaprojektowanie matrycy uprawnień przed rozpoczęciem prac?</p> <p>Odpowiedź: Zakres jest ujęty w Załączniku nr 1 do Umowy.</p>
SWS.73	<p>Czy Zamawiający dopuszcza, aby historia zmian ról użytkowników była dostępna w formie raportu audytowego generowanego na żądanie Administratora Głównego, zamiast widoku inline przy profilu użytkownika?</p> <p>Odpowiedź: Zamawiający nie dopuszcza takiego rozwiązania.</p>
SWS.74	<p>Czy Zamawiający dopuszcza, aby szczegółowy podgląd operacji na wniosku (kwalifikacje, karencje, zmiany) był dostępny w rozbudowanej historii podania, a nie jako osobny widok – z uwagi na spójność interfejsu i centralizację informacji o wniosku?</p> <p>Odpowiedź: Zamawiający nie dopuszcza takiego rozwiązania.</p>
SWS.77	<p>Czy Zamawiający może doprecyzować, w jakim czasie po zakończeniu opieki w żłobku (usunięciu z Dziennika Elektronicznego) miejsce ma być automatycznie widoczne jako wolne w module rekrutacji, aby możliwe było zaprojektowanie mechanizmu synchronizacji?</p> <p>Odpowiedź: Usunięcie z modułu pracy bieżącej/Dziennika Elektronicznego powoduje automatyczne i natychmiastowe uwolnienie miejsca do rekrutacji.</p>
WTAB.1	<p>Czy Zamawiający dopuszcza separację danych na poziomie logicznym (dedykowany schemat bazy danych per jednostka z unikalnym identyfikatorem) zamiast fizycznej separacji</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>infrastruktury, przy zachowaniu pełnej izolacji danych i braku możliwości ich przenikania?</p> <p>Odpowiedź:</p> <p>Separacja danych na poziomie logicznym jest rozumiana jako separacja realizowana na poziomie zapisu danych (np.: dedykowany schemat bazy danych per jednostka z unikalnym identyfikatorem). Separacja fizyczna oznacza natomiast separację realizowaną na poziomie sprzętowym. Zamawiający nie uznaje separacji logicznej za spełnienie przedmiotowego wymagania, ponieważ zgodnie z jego treścią dodatkowej punktacji podlega wyłącznie zapewnienie separacji fizycznej.</p>
WTAB.1a	<p>Czy wymaganie WTAB.1a (separacja fizyczna per tenant) jest traktowane jako opcja dodatkowa premiowana w ocenie ofert, czy też jest ono obowiązkowe – mając na uwadze, że WTAB.1 dopuszcza separację logiczną jako równoważne rozwiązanie?</p> <p>Odpowiedź:</p> <p>Wymagalność WTAB.1a jest dodatkowo punktowana - zgodnie z kryterium oceny ofert.</p>
WTAB.4	<p>Czy Zamawiający dopuszcza zabezpieczenie API poprzez tokeny sesyjne (session tokens) lub klucze API z rotacją, jako rozwiązanie równoważne tokenom JWT, przy zachowaniu tych samych gwarancji bezpieczeństwa autoryzacji?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza rozwiązanie.</p>
WTAB.5	<p>Jak mierzony jest RTO (4h) — czy jest to czas od zgłoszenia utraty danych do Wykonawcy, czy od momentu faktycznego wykrycia awarii, i jaka jest procedura zgłaszania utraty danych przez Zamawiającego</p> <p>Odpowiedź:</p> <p>Od wykrycia awarii i/oraz zgłoszenia.</p>

Sygnatura	Treść pytania - Odpowiedź
WTAB.11	<p>Czy Zamawiający dopuszcza, aby polityka haseł była ustalona na stałe przez Wykonawcę zgodnie z aktualnymi rekomendacjami CERT Polska (bez wymogu periodycznej zmiany hasła), zamiast umożliwiania jej konfiguracji przez Administratora – mając na uwadze, że parametryzacja polityki haseł przez użytkownika może obniżać poziom bezpieczeństwa?</p> <p>Odpowiedź: Zamawiający nie dopuszcza rozwiązania.</p>
WTAB.11a	<p>Czy wymaganie odrębnej polityki haseł per tenant (WTAB.11a) jest obowiązkowe, czy też Zamawiający dopuszcza jednolitą politykę haseł dla wszystkich jednostek, zapewniającą spójny i wysoki poziom bezpieczeństwa?</p> <p>Odpowiedź: Tak, wymaganie odrębnej polityki haseł per tenant jest obowiązkowe. Zapis ten jest niezbędny jako elastyczny element systemu, który może zostać dostosowany do wymagań konkretnej polityki bezpieczeństwa informacji, mogącej ulegać zmianom w trakcie obowiązywania umowy. Wymagalność WTAB.11a jest dodatkowo punktowana - zgodnie z kryterium oceny ofert.</p>
WTAB.12	<p>Czy Zamawiający dopuszcza procedurę resetowania hasła, w której Administrator ustawia tymczasowe jednorazowe hasło (przekazywane użytkownikowi bezpośrednio, nie e-mailem) i system wymusza jego zmianę przy pierwszym logowaniu – jako rozwiązanie zapewniające równoważny poziom bezpieczeństwa?</p> <p>Odpowiedź: Zamawiający wymaga, aby system opierał się na generowaniu jednorazowego linku służącego do zmiany hasła, co zapewnia wyższy poziom bezpieczeństwa poprzez ograniczenie ryzyka pomyłki po stronie administratora.</p>
WTAB.13	<p>Czy Zamawiający dopuszcza, aby automatyczne odblokowanie konta po blokadzie spowodowanej błędnymi próbami logowania następowało po upływie stałego okresu</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>czasu (np. 15-30 minut), bez konieczności konfiguracji tego czasu przez Administratora?</p> <p>Odpowiedź: Zamawiający oczekuje by był domyślnie jeden czas dla wszystkich kont w Tenancie wcześniej prekonfigurowany przez administratora, nie konfigurowany przy każdej blokadzie.</p>
WTAB.16	<p>Czy Zamawiający dopuszcza, aby czas automatycznego wylogowania po bezczynności był ustawiony na stałe przez Wykonawcę na poziomie 30 minut, zgodnie z aktualnymi zaleceniami bezpieczeństwa, bez konieczności udostępniania Administratorowi możliwości zmiany tego parametru?</p> <p>Odpowiedź: Zamawiający nie dopuszcza rozwiązania.</p>
WTAB.19	<p>Mając na uwadze, że wymaganie WTAB.19 jest oznaczone jako 'Opcja', prosimy o potwierdzenie, że jego niespełnienie nie wpłynie na ocenę oferty ani na warunki realizacji umowy.</p> <p>Odpowiedź: Wymaganie WTAB.19 stanowi warunek konieczny realizacji zamówienia, tak samo pozostałe wymagania oznaczone jako „Opcja”.</p>
WTAB.20	<p>W jaki sposób Wykonawca ma potwierdzić zgodność zastosowanego mechanizmu szyfrowania z normą FIPS 140-2 Level 2 – czy wymagane jest przedstawienie aktualnego certyfikatu dla zastosowanego modułu kryptograficznego?</p> <p>Odpowiedź: Należy zweryfikować urządzenia z listą urządzeń spełniających zgodnych/kompatybilnych z FIPS 140-2 level 2. Link z listą dostępny jest w Załączniku nr 1.</p>
WTAB.24	<p>Czy wymóg szyfrowania dotyczy również komunikacji wewnętrznej pomiędzy komponentami systemu (np. aplikacja–baza danych, mikroserwisy), czy wyłącznie połączeń zewnętrznych?</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>Odpowiedź:</p> <p>Tak, dotyczy również komunikacji wewnętrznej pomiędzy komponentami systemu.</p>
WTAB.29	<p>Czy Zamawiający może wskazać katalog operacji użytkowników, które bezwzględnie muszą być rejestrowane i dostępne w raportach (np. logowanie, zmiana statusu wniosku, modyfikacja danych dziecka), aby możliwe było zaprojektowanie systemu logowania odpowiadającego rzeczywistym potrzebom audytowym?</p> <p>Odpowiedź:</p> <p>Zamawiający na tym etapie nie jest w stanie wskazać katalogu operacji użytkowników, które muszą być rejestrowane i dostępne w raportach. Katalog ten zostanie wypracowany w ramach Analizy Przedwdrożeniowej.</p>
WTAB.33	<p>Czy Zamawiający dopuszcza zastąpienie mechanizmu daty ważności konta funkcją ręcznego dezaktywowania konta przez Administratora (bez daty automatycznego wygaśnięcia), z możliwością masowej dezaktywacji kont przypisanych do placówki?</p> <p>Odpowiedź:</p> <p>Zamawiający nie dopuszcza rozwiązania.</p>
WTAB.37	<p>Czy Zamawiający dopuszcza, aby historia blokowania i odblokowywania kont użytkowników była dostępna w formie raportu audytowego generowanego przez Administratora, zamiast być przechowywana jako osobny log systemowy?</p> <p>Odpowiedź:</p> <p>Zamawiający nie dopuszcza rozwiązania.</p>
WB.4	<p>Czy Zamawiający dopuszcza, aby Wykonawca zapewnił monitoring zdarzeń bezpieczeństwa w godzinach roboczych (5x8), z automatycznymi alertami i zdefiniowaną procedurą reagowania na incydenty krytyczne poza godzinami pracy, zamiast pełnego dyżuru SOC 24/7?</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>Odpowiedź:</p> <p>Zamawiający nie dopuszcza rozwiązania.</p>
WB.5	<p>Czy Zamawiający może wskazać, który system SIEM będzie odbiorcą logów, oraz zdefiniować minimalny wymagany format i zakres przesyłanych zdarzeń (np. Syslog RFC 5424, CEF), aby możliwe było zaprojektowanie integracji w ramach Analizy Przedwdrożeniowej?</p> <p>Odpowiedź:</p> <p>Zamawiający wskazuje, że będzie to oprogramowanie Logstash w wersji 7. Wszystkie obsługiwane przez Logstash protokoły i formaty są dostępne.</p>
WB.6	<p>W jakim przedziale czasowym (np. co ile dni/tygodni/miesiący) Wykonawca jest zobowiązany przeprowadzać regularne aktualizacje systemu i infrastruktury, oraz w jakim terminie od wykrycia podatności muszą zostać wdrożone zabezpieczenia niwelujące znalezione luki bezpieczeństwa?</p> <p>Odpowiedź:</p> <p>Zgodne z zapisami załącznika nr 3 do Umowy – SLA.</p>
WB.7	<p>W jakim maksymalnym czasie (np. liczba godzin od wykrycia lub zgłoszenia) Wykonawca jest zobowiązany podjąć działania naprawcze oraz usunąć lukę lub podatność bezpieczeństwa w trybie awarii krytycznej – zarówno wykrytej samodzielnie, jak i zgłoszonej przez Zamawiającego?</p> <p>Odpowiedź:</p> <p>Zgodne z zapisami załącznika nr 3 do Umowy – SLA.</p>
WL.1	<p>Czy Zamawiający dopuszcza, aby wymóg pełnego wsparcia cyklu życia dotyczył wyłącznie kluczowych komponentów infrastrukturalnych (system operacyjny, serwer aplikacji, środowisko uruchomieniowe), natomiast dla bibliotek open source za wystarczające uznane zostało aktywne utrzymanie projektu przez społeczność (aktywne repozytorium, regularne</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>wydania, brak statusu EOL) — bez wymogu komercyjnego wsparcia technicznego od producenta?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza rozwiązanie. Pod warunkiem że wykorzystywane komponenty będą podlegały weryfikacji pod kątem zidentyfikowanych podatności, a w przypadku wykrycia luk bezpieczeństwa zostaną zastąpione rozwiązaniami równoważnymi, po uprzednim uzgodnieniu z Zamawiającym.</p>
WL.2	<p>Czy Zamawiający dopuszcza, aby 12-miesięczny termin przed końcem Umowy dotyczył wyłącznie głównych komponentów platformy (JVM, Node.js, serwer aplikacji, baza danych), natomiast dla bibliotek pomocniczych open source wystarczające było zapewnienie, że nie posiadają one statusu End-of-Life oraz że znane podatności bezpieczeństwa są na bieżąco eliminowane przez Wykonawcę?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza rozwiązanie.</p>
WL.3	<p>Czy Zamawiający dopuszcza, aby wymóg aktywnego wsparcia technicznego dla bibliotek i komponentów był weryfikowany na poziomie braku statusu EOL oraz dostępności aktualizacji bezpieczeństwa, bez wymogu posiadania komercyjnej umowy wsparcia — mając na uwadze, że ekosystem open source (Spring, Hibernate, React i in.) funkcjonuje w oparciu o wsparcie społeczności, nie zaś gwarancje producenta?</p> <p>Odpowiedź:</p> <p>Zamawiający dopuszcza rozwiązanie, ale w przypadku EOL komponentów Open source wykonawca powinien zastąpić je równoważnymi rozwiązaniami.</p>
W-AA 1.4.4	<p>Czy Zamawiający dopuszcza, aby wymóg powiększenia tekstu do 200% był realizowany poprzez natywną funkcję powiększenia przeglądarki (Ctrl+/zoom), bez dedykowanego mechanizmu zmiany rozmiaru tekstu wbudowanego w interfejs systemu — mając na uwadze, że wszystkie</p>

Sygnatura	Treść pytania - Odpowiedź
	<p>współczesne przeglądarki obsługują tę funkcję natywnie i jest ona powszechnie dostępna dla użytkowników bez konieczności instalacji technologii wspomagających?</p> <p>Odpowiedź: Dopuszczalne jest spełnienie wymagania powiększenia tekstu do 200% poprzez natywną funkcję zoom przeglądarki, bez konieczności implementowania dedykowanego mechanizmu w interfejsie systemu, o ile po powiększeniu do 200% nie dochodzi do utraty treści ani funkcjonalności</p>
W-AA 1.4.10	<p>Czy Zamawiający dopuszcza, aby wymóg WCAG 1.4.10 (320px) dotyczył wyłącznie modułu publicznego (strony rodzica/opiekuna), natomiast panel administracyjny przeznaczony dla pracowników żłobków był dostosowany do minimalnej szerokości odpowiadającej standardowym urządzeniom używanym w pracy biurowej?</p> <p>Odpowiedź: Nie ma podstaw do ograniczenia wymogu WCAG 1.4.10 wyłącznie do modułu publicznego. Jeżeli panel administracyjny działa w przeglądarce i stanowi część systemu tworzonego dla podmiotu publicznego, to co do zasady również podlega wymaganiom dostępności cyfrowej, w tym kryterium 1.4.10.</p>

2. Dotyczy: Załącznik nr 4 do umowy - Umowa PPDO

Czy Zamawiający wyraża zgodę na skrócenie czasu trwania audytu, o który mowa w § 12. ust. 3 umowy PPDO, do 7 dni od jego rozpoczęcia? Skrócenie okresu audytu do 7 dni nie narusza obowiązków wynikających z przepisów RODO, audyt wciąż pozwala na dokładną weryfikację procedur bezpieczeństwa i przetwarzania danych.

Odpowiedź:

Zamawiający nie wyraża zgody na zmianę zapisu. Zakres powierzonych danych oraz sposób świadczenia usługi (usługa w infrastrukturze Wykonawcy) może powodować, że Wykonawca nie będzie w stanie odpowiadać w czasie pozwalający na realizację audytu w terminie 7 dni. Mając na uwadze doświadczenie Zamawiającego w zakresie audytów określony czas na realizację audytów jest optymalny.

3. Dotyczy: Załącznik nr 4 do umowy - Umowa PPDO

Czy Zamawiający wyraża zgodę, aby w § 14 umowy PPDO usunąć zapisy wprowadzające inspektora ochrony danych osobowych z imienia i nazwiska dla Powierzającego oraz Przetwarzającego. Z punktu widzenia przepisów RODO najważniejsze jest, aby dane kontaktowe, takie jak adres e-mail i numer telefonu, były prawidłowe i aktualne, zwłaszcza w kontekście IOD.

Propozycja zmiany zapisów w § 14 na:

- 1) Powierzający wyznaczył inspektora ochrony danych: _____
służbowy adres poczty elektronicznej: _____ służbowy nr
telefonu: _____
- 2) Przetwarzający wyznaczył inspektora ochrony danych / osobę
kontaktową w sprawach dotyczących Danych Osobowych:
służbowy adres poczty elektronicznej: _____, służbowy nr
telefonu: _____

W przypadku zmiany adresów e-mail do inspektorów ochrony danych, o których mowa w ust. 1 lub 2, Strona u której doszło do zmiany adresu e-mail IOD, zobowiązana jest do niezwłocznego zawiadomienia o tym drugiej Strony.

Odpowiedź:

Zamawiający wyraża zgodę, pod warunkiem publikacji zapisu o osobie pełniącej funkcję IOD na stronie internetowej Wykonawcy.

Zamawiający **zmienia treść § 14 Załącznika nr 4 do umowy** poprzez wykreślenie dotychczasowej treści i zastąpienie nową w brzmieniu:

- 1) Powierzający wyznaczył inspektora ochrony danych: _____
służbowy adres poczty elektronicznej: _____ służbowy nr
telefonu: _____
- 2) Przetwarzający wyznaczył inspektora ochrony danych / osobę
kontaktową w sprawach dotyczących Danych Osobowych:
służbowy adres poczty elektronicznej: _____, służbowy nr
telefonu: _____
- 3) W przypadku zmiany adresów e-mail do inspektorów ochrony danych,
o których mowa w ust. 1 lub 2, Strona u której doszło do zmiany
adresu e-mail IOD, zobowiązana jest do niezwłocznego zawiadomienia
o tym drugiej Strony.

4. Dotyczy: Załącznik nr 4 do umowy - Umowa PPDO

Czy Zamawiający wyraża zgodę na dodanie do umowy PPDO w formie załącznika „wzoru klauzuli informacyjnej stosowanej przez Przetwarzającego, do wykonania obowiązku z art. 14 RODO względem osób realizujących umowę”?

W przypadku wyrażenia zgody na dodanie wzoru klauzuli wnosimy o zmianę:

- 1) w § 15 treści ust. 3 na „W celu realizacji obowiązku, o którym mowa w ustępie 2, Przetwarzający w załączniku nr 4 do Umowy przekazuje Powierzającemu treść obowiązku informacyjnego dla personelu Powierzającego .”
- 2) dodanie w § 17 ustępu o treści „wzór klauzuli informacyjnej stosowanej przez Przetwarzającego, do wykonania obowiązku z art. 14 RODO względem osób realizujących umowę.”

Odpowiedź:

Zamawiający wyraża zgodę pod warunkiem, że przedmiotowa klauzula nie nakłada innych, niewskazanych w umowie, obowiązków na Zamawiającego.

Zamawiający **zmienia treść § 15 ust. 3 Załącznika nr 4 do umowy** poprzez wykreślenie dotychczasowej treści i zastąpienie nową w brzmieniu:

„W celu realizacji obowiązku, o którym mowa w ustępie 2, Przetwarzający w załączniku nr 4 do Umowy przekazuje Powierzającemu treść obowiązku informacyjnego dla personelu Powierzającego.

Przetwarzający zobowiązany jest w terminie 7 dni od zawarcia Umowy do przekazania Powierzającemu treści obowiązku informacyjnego, o którym mowa w art. 14 RODO, dla personelu Powierzającego, a po tym terminie, zobowiązany będzie względem tego personelu do samodzielnej realizacji obowiązku informacyjnego, o którym mowa w art. 14 RODO.”

Zamawiający **zmienia treść § 17 Załącznika nr 4 do umowy** poprzez wykreślenie dotychczasowej treści i zastąpienie nową w brzmieniu:

„Integralną część Umowy stanowią następujące załączniki:

- 1) *szczegóły powierzenia przetwarzania danych,*
- 2) *lista kontrolna - kryteria wyboru podmiotu przetwarzającego, któremu administrator zamierza powierzyć dane osobowe,*
- 3) *wzór klauzuli informacyjnej stosowanej przez Powierzającego, do wykonania obowiązku z art. 14 RODO względem osób realizujących umowę;*
- 4) *Lista kontrolna*
- 5) *Wzór klauzuli informacyjnej stosowanej przez Przetwarzającego, do wykonania obowiązku z art. 14 RODO względem osób realizujących umowę.”*

5. Dotyczy: Załącznik nr 4 do umowy - Umowa PPDO

Z uwagi na fakt, że dotychczasowy adres siedziby Prezesa Urzędu Ochrony Danych Osobowych, wskazany w umowie PPDO (Warszawa, ul. Stawki 2) jest już nieaktualny, wnosimy o dokonanie stosownej zmiany w umowie i wskazanie nowego adresu: ul. Stanisława Moniuszki 1A, 00-014 Warszawa.

Odpowiedź:

Zamawiający **zmienia w treści Załącznika nr 4 do umowy** adres siedziby Prezesa Urzędu Ochrony Danych Osobowych z „ul. Stawki 2, 00-193 Warszawa” na „ ul. Stanisława Moniuszki 1A, 00-014 Warszawa.

6. Dotyczy: Załącznik nr 1 do Umowy - Specyfikacja Wymagań

W wymaganiu WT.06 jest mowa o załączniku dot. bezpieczeństwa. Prosimy o doprecyzowanie gdzie znajduje się załącznik dot. bezpieczeństwa.

Odpowiedź:

Zapis WT.06 stanowi omyłkę pisarską. Zapisy załącznika dot. bezpieczeństwa zostały ujęte w Załączniku nr 1 z sygnaturą wymagań WTAB, WB oraz WL.

Zamawiający **zmienia treść wymagania WT.06 w Załączniku nr 1 do Umowy** - Specyfikacja Wymagań poprzez wykreślenie dotychczasowej treści i zastąpienie nową w brzmieniu:

„System musi przechowywać hasła kont i zdefiniowanych połączeń w postaci zaszyfrowanej zgodnej z wymaganiami z Załącznika nr 1 o sygnaturze WTAB, WB oraz WL.”

7. Pytanie doprecyzowujące szczegóły techniczne: dot. SWS.60

Wymaganie SWS.60 wymaga raportów statystycznych z możliwością generowania na zadany dzień. Czy Zamawiający precyzuje, że raporty mają mieć możliwość:

- a) zapisu szablonów raportów (do późniejszego wywołania bez ponownej parametryzacji);
- b) harmonogramowania (cron) wysyłki raportów na e-mail Operatora?

Odpowiedź:

Zamawiający dopuszcza, ale nie wymaga zapisu szablonów raportów, natomiast oczekuje, by raporty miały możliwość wysyłki na e-mail Operatora z opcją harmonogramowania.

8. Pytanie doprecyzowujące szczegóły techniczne: dot. SWS.85 / SWS.70

Wymaganie SWS.85 wymaga publikacji jadłospisów na zadany okres (tydzień, 10 dni, itp.). SWS.70 wskazuje, że jadłospis tygodniowy ma być widoczny w aplikacji rodziców. Czy Zamawiający precyzuje:

- a) wymagany format publikacji (PDF, HTML, JSON dla aplikacji mobilnej, obraz);
- b) integrację z systemem cateringu (zewnętrznym)?

Odpowiedź:

Zamawiający wymaga publikacji jadłospisu w formacie HTML z opcjonalną możliwością pobrania w formacie PDF. Integracji z systemem cateringu nie przewiduje.

Wątpliwości dotyczące spójności wymagań

9. dot. WT.11 / WTAB.10

Wymaganie WT.11 wymaga wymuszania zmiany hasła co 30 dni. Tymczasem WTAB.10 odsyła do OWASP Password Storage Cheat Sheet, a OWASP (potwierdzone przez NIST SP 800-63B Rev. 3, sekcja 5.1.1.2) odradza okresową rotację haseł bez powodu, ponieważ prowadzi do osłabienia haseł (przewidywalne wzorce, hasła zapisywane na karteczkach). Czy Zamawiający dopuszcza politykę zgodną z aktualnymi rekomendacjami OWASP/NIST, tj. zmianę hasła wyłącznie w przypadku podejrzenia kompromitacji, a nie cyklicznie co 30 dni? Jeśli nie, prosimy o uzasadnienie wymagania sprzecznego z międzynarodowymi standardami, do których odsyła samo OPZ.

Odpowiedź:

Zamawiający dopuszcza takie rozwiązanie.

10. dot. WB.2

Wymaganie WB.2 wylicza nagłówki bezpieczeństwa: „Strict-Transport-Security, Referrer-Policy, XContent-Type-Options, Permissions-Policy, X-Frame-Options, Content-Security-Policy, HTTP Strict Transport Security”. Strict-Transport-Security i HTTP Strict Transport Security to ten sam nagłówek (HSTS). Czy Zamawiający wymaga jakiegoś innego, dodatkowego nagłówka ponad listę faktyczną, czy jest to omyłka redakcyjna?

Odpowiedź:

Zamawiający nie wymaga innego, dodatkowego nagłówka ponad listę faktyczną. Ujęcie Strict-Transport-Security i HTTP Strict Transport Security jako dwóch różnych nagłówków stanowi omyłkę.

11. dot. WTAB.20

Wymaganie WTAB.20 wskazuje na zgodność z FIPS 140-2 Level 2. National Institute of Standards and Technology (NIST) oficjalnie ogłosił, że certyfikaty FIPS 140-2 są wycofywane od września 2026 na rzecz FIPS 140-3 (CMVP transition policy). Czy Zamawiający potwierdza, że dopuszczalne są moduły kryptograficzne certyfikowane wg FIPS 140-3 Level 2 lub 3 oraz czy dopuszcza europejskie odpowiedniki — Common Criteria EAL 4+ lub ENISA EUCS — jako rozwiązania równoważne, zgodnie z art. 101 ust. 5 ustawy Pzp?

Odpowiedź:

Zamawiający podtrzymuje obecne zapisy. Na dzień przeprowadzenia przetargu obowiązujący standard FIPS 140-2 Level 2 pozostaje zgodny z wymaganiami NIST i takie wymagania muszą zostać spełnione w ramach niniejszego zamówienia.

12. dot. WTAB.9

Wymaganie WTAB.9 wymaga zgodności z certyfikatem Uptime Institute TIER III. Wskazujemy, że dostawcy infrastruktury europejskiej (Hetzner, OVHcloud, Beyond.pl, Atman) oraz hyperscalerzy (AWS, Microsoft Azure, Google Cloud) nie certyfikują pojedynczych regionów Uptime Institute, posługując się równoważnymi certyfikatami EN 50600 (klasa 4), ISO 22301, ISO 27001, ISO/IEC 22237, SOC 2 Type II, oraz publikując SLA dostępności równe lub wyższe od 99,982%. Czy Zamawiający, zgodnie z art. 101 ust. 5 ustawy Pzp, dopuszcza rozwiązania równoważne gwarantujące taki sam poziom dostępności i bezpieczeństwa, ale potwierdzone innymi powszechnie uznanymi standardami międzynarodowymi? Wymaganie jednego konkretnego certyfikatu Uptime Institute istotnie ogranicza krąg potencjalnych Wykonawców i może być niezgodne z art. 99 ust. 4 ustawy Pzp.

Odpowiedź:

Zamawiający nie wymagana certyfikacji, jedynie spełnienie wymagań dla Tier 3, opisanych na stronie. <https://www.gov.pl/web/popcwsparcie/klasyfikacja-tier-centrum-danych-datacenter>.

13. dot. warunek 6.2.4.2.c SWZ vs WTAB.9

Warunek udziału 6.2.4.2.c SWZ wymaga: "Architekt Rozwiązań Chmurowych – przynajmniej 5 letnie doświadczenie w projektowaniu lub wdrażaniu rozwiązań chmurowych, udział w dwóch przynajmniej projektach wykorzystujących jedną z platform chmurowych (np. AWS, Microsoft Azure, Google Cloud Platform)". Zwrot "np." wskazuje, że jest to lista przykładowa, nie zamknięta. Czy Zamawiający potwierdza, że dopuszczalne są platformy chmurowe spoza tej listy (Hetzner Cloud, OVHcloud, Beyond.pl Pulsar, Atman Cloud), pod warunkiem spełnienia pozostałych wymagań warunku (architektura mikroservisowa, integracje, migracja do chmury, bezpieczeństwo)?

Odpowiedź:

Tak. Zamawiający potwierdza, że zaproponowane platformy chmurowe są równoważne.

Pytania o dopuszczenie rozwiązań równoważnych

14. dot. WTAB.9

Wymaganie WTAB.9 podaje wartość dostępności dokładnie 99,982% (cytuując definicję TIER III). Standardy SLA sektora publicznego (m.in. KPRM, Ministerstwo Cyfryzacji) operują wartościami zaokrąglonymi: 99,9% / 99,95% / 99,99%. Wartość 99,982% jest wyłącznie matematycznym wynikiem definicji Uptime Institute dla TIER III. Czy Zamawiający dopuszcza

rozwiązania o gwarantowanej dostępności co najmniej 99,9% mierzonej w cyklu rocznym, z wyłączeniem zaplanowanych okien serwisowych, jako równoważne i zgodne z dobrymi praktykami sektora?

Odpowiedź:

Zamawiający wymaga dopuszcza wymagania zgodnie z wytycznymi tier 3 <https://www.gov.pl/web/popcwsparcie/klasyfikacja-tier-centrum-danych-datacenter>.

15. dot. WTAB.1

Wymaganie WTAB.1 wskazuje na konieczność stosowania unikalnego TenantID dla separacji danych. Pojęcie „TenantID” jest specyficzne dla wybranych frameworków SaaS (Microsoft Azure, Salesforce). Większość systemów SaaS w sektorze publicznym stosuje logiczną izolację per ClientID/OrganizationID w warstwie aplikacji wraz z segregacją schematów lub baz w warstwie DB. Czy Zamawiający potwierdza, że logiczna separacja per identyfikator placówki w połączeniu z filtrowaniem zapytań SQL (row-level security) i polityką RBAC jest rozwiązaniem równoważnym?

Odpowiedź:

Zamawiający potwierdza, że są to rozwiązania równoważne.

16. dot. WO.19

Wymaganie WO.19 w sekcji "model SaaS" wymienia wymagania fizyczne datacenter (system klimatyzacji precyzyjnej, system sygnalizacji pożaru, system kontroli dostępu, monitoring wizyjny, system awaryjnego podtrzymania zasilania). W modelu SaaS odpowiedzialność za infrastrukturę fizyczną spoczywa na dostawcy chmury (np. Hetzner, OVHcloud, Beyond.pl, Atman, AWS, Microsoft Azure), a Wykonawca dziedziczy te zabezpieczenia poprzez certyfikaty audytów (ISO 27001, EN 50600 klasa 4, ISO 22301, SOC 2, PCI DSS). Czy Zamawiający potwierdza, że przedstawienie certyfikatów audytowych dostawcy chmury jest wystarczającym dowodem spełnienia tego wymagania, bez konieczności dokumentowania fizycznej infrastruktury własnej Wykonawcy?

Odpowiedź:

Tak, Zamawiający potwierdza, że przedstawienie certyfikatów audytowych dostawcy chmury jest wystarczającym dowodem, jeżeli spełniają one wymogi ujęte w Załącznikach do Umowy i SWZ.

17. dot. WB.4

Wymaganie WB.4 wymaga "zespołu SOC analizującego zdarzenia bezpieczeństwa". Czy Zamawiający dopuszcza: a) usługę MSSP/SOC-as-a-

Service od podmiotu trzeciego z certyfikatem ISO 27001 i SOC 2 Type II; b) wykorzystanie wbudowanych mechanizmów monitoringu SIEM (np. Wazuh, ELK Stack, Graylog, AWS GuardDuty, Azure Sentinel) z 24/7 alertingiem dyżurnego DevOps Wykonawcy i procedurą eskalacji; c) CSIRT/CERT dostawcy chmury jako równoważne SOC; d) systemy detekcji włamań typu Fail2Ban + CrowdSec wraz z procedurą reagowania? Wymaganie własnego, dedykowanego SOC dla systemu o regionalnym charakterze i skali ok. 450 operatorów wydaje się niewspółmierne do skali zamówienia.

Odpowiedź:

Zamawiający dopuszcza rozwiązanie z zastrzeżeniem, że leży to po stronie wykonawcy.

18. dot. WTAB.15

Wymaganie WTAB.15 wymaga, by każdemu użytkownikowi przypisana była tylko jedna aktywna sesja. Wymaganie to wymaga doprecyzowania, ponieważ w praktyce eksploatacyjnej Systemu występuje szereg sytuacji, w których pojedyncza „sesja” w sensie technicznym jest nieadekwatna do realnej pracy użytkownika. Wnosimy o doprecyzowanie:

- a) Czy wymóg „pojedynczej aktywnej sesji” oznacza: pojedynczą sesję w obrębie konta użytkownika (per UserID, niezależnie od urządzenia / przeglądarki / zakładki); pojedynczą sesję w obrębie urządzenia (per UserID + DeviceID); pojedynczą sesję w obrębie procesu przeglądarki (per UserID + Browser + Storage); czy pojedynczy token autoryzacyjny (per JWT / access token)?
- b) Czy wymóg pojedynczej sesji obejmuje również scenariusz pracy w wielu zakładkach tej samej przeglądarki? W praktyce eksploatacyjnej intendent / księgowy / administrator Operatora pracuje równolegle w kilku zakładkach (np. faktury + raport miesięczny + lista dzieci + jadłospis), które dzielą wspólne cookies oraz Local / Session Storage, a więc technicznie stanowią jedną sesję serwerową. Wymuszenie zamknięcia pozostałych zakładek przy każdym otwarciu nowej eliminuje normalny tryb pracy biurowej i jest sprzeczne ze standardem ergonomii interakcji człowiek-system (ISO 9241110:2020 — Ergonomia interakcji człowiek-system, Zasady dialogu).
- c) Czy wymóg pojedynczej sesji obejmuje również konto Rodzica / Opiekuna używane wspólnie przez obojga rodziców z dwóch różnych urządzeń (telefon matki + telefon ojca, równoczesna obsługa zgłoszeń wejścia / wyjścia, nieobecności, podgląd płatności)? W roli Rodzic / Opiekun jest to standardowa sytuacja eksploatacyjna i wymóg pojedynczej sesji eliminuje praktyczną używalność systemu dla obojga rodziców.
- d) Jaką techniczną definicję „sesji” stosuje Zamawiający — sesja serwerowa (PHPSESSID / Express Session), token JWT z czasem wygaśnięcia, cookie HttpOnly z fingerprintingiem urządzenia, czy mechanizm WebSocket connection?

Wnosimy o jednoznaczne sformułowanie WTAB.15 w sposób uwzględniający powyższe scenariusze pracy — w szczególności o dopuszczenie wielu zakładek w obrębie jednej sesji przeglądarki oraz pracy równoczesnej w roli Rodzic / Opiekun z dwóch urządzeń przy współdzielonym koncie.

Odpowiedź:

- a) Sesja rozumiana jest jako pojedyncza sesja w obrębie konta użytkownika per UserID + Browser Instance (przeglądarka na konkretnym urządzeniu), oparta na unikalnym identyfikatorze sesji przechowywanym po stronie serwera (token/cookie). Wiele kart w tej samej przeglądarce współdzieli ten identyfikator, co stanowi technicznie jedną sesję,
- b) Praca w wielu zakładkach tej samej przeglądarki jest w pełni dopuszczalna i objęta wymaganiami jako jeden dozwolony scenariusz,
- c) Wymaganie WTAB.15 nie rozróżnia ról użytkownika dotyczy wszystkich kont w systemie,
- d) Sesja technicznie oznacza unikalny identyfikator sesji serwerowej powiązany z kontem użytkownika, przechowywany po stronie klienta w cookie. Identyfikator ten jest generowany przy każdym logowaniu, a jego wygaśnięcie lub unieważnienie po stronie serwera skutkuje koniecznością ponownego uwierzytelnienia. Wygasłe identyfikatory sesji nie mogą być ponownie wykorzystane do autoryzacji.

19. dot. WTAB.2 (VPN)

Wymaganie WTAB.2 wymaga „dostępu VPN (szyfrowany dostęp zdalny)” dla sieci publicznej i prywatnej. W praktyce zarządczej dla małych zespołów Wykonawców (5–10 administratorów) dostęp SSH z whitelisy adresów IP w połączeniu z kluczami publicznymi RSA 4096 lub Ed25519 zapewnia równoważny lub wyższy poziom bezpieczeństwa niż VPN, przy znacznie niższym koszcie operacyjnym. Czy Zamawiający, zgodnie z art. 101 ust. 5 ustawy Pzp, dopuszcza jako rozwiązanie równoważne dostęp SSH z whitelisy IP kluczami publicznymi zamiast VPN?

Odpowiedź:

Zamawiający nie dopuszcza rozwiązania.

20. dot. WTAB.2 (firewall)

Wymaganie WTAB.2 wymaga „firewalla sprzętowego”. Wymóg ten:

- a) jest typowy dla infrastruktury klasy enterprise (Cisco ASA, Palo Alto, Fortinet, Check Point) o koszcie 30 000–200 000 PLN za urządzenie wraz z utrzymaniem rocznym;
- b) nie jest standardową usługą w popularnych ofertach SaaS i chmurowych (Hetzner, OVHcloud, AWS, Azure, GCP, IONOS, Scaleway), w których funkcję firewalla pełnią natywne mechanizmy programowe (Hetzner Robot

- Firewall, Hetzner Cloud Firewall, AWS Security Groups, Azure NSG, GCP VPC Firewall) zapewniające ten sam poziom kontroli ruchu sieciowego co rozwiązania sprzętowe, przy zachowaniu pełnej rozliczalności i logowania;
- c) w modelu SaaS jest zastępowany dodatkowo przez WAF (Web Application Firewall) pracujący na poziomie aplikacyjnym (warstwa 7 OSI) i chroniący przed atakami specyficznymi dla aplikacji webowych (OWASP Top 10: SQL injection, XSS, CSRF, RCE).

Wnosimy, zgodnie z art. 101 ust. 5 ustawy Pzp, o uznanie za rozwiązanie równoważne dla „firewalla sprzętowego”:

- 1) natywnego firewalla chmurowego dostawcy infrastruktury (Hetzner Cloud Firewall, Hetzner Robot Firewall, AWS Security Groups, Azure NSG, GCP VPC Firewall) działającego na poziomie sieciowym (warstwy 3–4 OSI);
- 2) WAF na poziomie aplikacyjnym, w jednej z poniższych form: a) ModSecurity z OWASP Core Rule Set (open source, integracja z nginx / Apache, standard branżowy); b) NAXSI (open source, dedykowany WAF dla nginx); c) CrowdSec WAF Bouncer (open source, kolektywna detekcja zagrożeń); d) Cloudflare WAF lub AWS WAF (komercyjny WAF działający jako reverse proxy przed infrastrukturą Wykonawcy);
- 3) systemu detekcji włamań (IDS / IPS) typu Suricata lub Snort z aktualizowanymi sygnaturami zagrożeń jako uzupełnienie ochrony.

Powyższe rozwiązania w zestawie zapewniają poziom ochrony równoważny lub wyższy w stosunku do tradycyjnego firewalla sprzętowego, są zgodne z modelem SaaS opartym na infrastrukturze chmurowej oraz nie wymagają zakupu i utrzymania dedykowanego sprzętu sieciowego, którego koszt jest niewspółmierny do skali zamówienia (~ok. 450 operatorów).

Odpowiedź:

Zgodnie z WTAB.2 Dopuszczalne jest zastosowanie innych równoważnych zabezpieczeń infrastruktury, po wykonaniu Analizy przedwdrożeniowej i akceptacji przez Zamawiającego. Wykonawca przedstawi dokumentację potwierdzającą wdrożenie i stosowanie wymienionych wyżej oraz uzgodnionych zabezpieczeń. Przedstawione rozwiązania spełniają wymogi równoważnych zabezpieczeń.

21. dot. WO.11 / W-A / W-AA

Czy zgodność WCAG 2.1 AA (WO.11, sekcja W-A i W-AA) dotyczy całego Systemu, czy w szczególności interfejsów dostępnych dla Gościa, Rodzica/Opiekuna oraz panelu Informatora? Standardową praktyką w sektorze publicznym jest wyłączenie panelu administracyjnego dla wewnętrznych Operatorów z bezwzględnego wymagania WCAG, gdyż nie jest on częścią e-usługi publicznej (analogicznie ustawa o dostępności cyfrowej z 4 kwietnia 2019 r. dotyczy treści udostępnianych obywatelom).

Odpowiedź:

Nie ma podstaw do automatycznego wyłączenia panelu administracyjnego z wymagań WCAG 2.1 AA. Ustawa o dostępności cyfrowej zawiera zamknięty katalog wyłączeń i nie ma tam ogólnego wyjątku dla paneli operatorów/adminów.

Co więcej, ustawa wprost wskazuje, że dotyczy podmiotów publicznych posiadających strony internetowe lub aplikacje mobilne albo zarządzających ich elementami. Czyli jeśli system jest tworzony dla jednostki publicznej i stanowi element jej systemu/aplikacji, to co do zasady podlega wymaganiom dostępności.

Jedyny wyjątek dotyczy intranetów/ekstranetów opublikowanych przed 23.09.2019 i nieprzebudowywanych od tego czasu.

Art. 5 mówi natomiast wprost, że podmiot publiczny ma zapewnić dostępność cyfrową swoich stron/aplikacji i ich elementów zgodnie z wymaganiami WCAG.

Czyli sam fakt, że moduł jest „wewnętrzny” albo „administracyjny”, nie stanowi automatycznego wyłączenia z ustawy.

Można tu jeszcze rozróżnić formę techniczną rozwiązania:

- jeśli panel admina jest klasyczną aplikacją desktopową, to co do zasady nie podlega tej ustawie, bo ustawa dotyczy stron internetowych i aplikacji mobilnych,
- natomiast jeśli panel działa w przeglądarce (webowy backoffice/admin), to jest traktowany jako strona internetowa/system webowy i wtedy wymagania dostępności mają zastosowanie.

22. dot. WO.13 / WO.14

Czy Zamawiający potwierdza, że integracja z Węzłem Krajowym (WO.13/WO.14) dotyczy wyłącznie pierwszego logowania w procesie rekrutacji — kontekst opisany w SWS.25 OPZ ("Logowanie do konkretnego konta jest możliwe tylko... przez Krajowy Węzeł Identyfikacji Elektronicznej") — natomiast późniejsze logowania do dziennika elektronicznego (po przyjęciu dziecka, na etapie pracy bieżącej zgodnie z pkt 2b OPZ) mogą odbywać się przez login/hasło z 2FA, w celu zapewnienia ciągłości dostępu rodzica do bieżących informacji o dziecku w sytuacji, gdy Węzeł Krajowy jest niedostępny lub rodzic utracił dostęp do profilu zaufanego/eID?

Odpowiedź:

Operatorzy oraz Administratorzy Główni mają mieć możliwość logowania się za pomocą hasła oraz loginu z racji cyklicznych operacji w systemie.

Natomiast pozostali użytkownicy (rodzic) mają mieć możliwość logowania jedynie przez Węzeł Krajowy za każdym razem.

23. dot. WO.15 — zakres publikacji danych

Wymaganie WO.15 stanowi: „Wykonawca dokona wdrożenia integracji z Open Data Wrocław (...) Wykonawca po stronie systemu zapewni przesłanie na portal dowolnych danych opublikowanych i skatalogowanych w systemie”.

Wskazujemy, że treść WO.15 nie definiuje zakresu danych podlegających publikacji. „Dowolne dane opublikowane i skatalogowane w systemie” jest sformułowaniem otwartym, podczas gdy w Systemie przetwarzane są w przeważającej części dane osobowe i dane szczególnej kategorii (zgodnie z art. 9 RODO — dane medyczne dziecka: diety, alergie, szczepienia, zalecenia żywieniowe; dane o frekwencji konkretnego dziecka; dane o płatnościach konkretnej rodziny). Publikacja takich danych w portalu Otwarte Dane Wrocław (data.wroclaw.pl) byłaby naruszeniem RODO oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych.

Brak doprecyzowania zakresu danych w OPZ uniemożliwia odpowiedzialną wycenę tego wymagania (zob. także Pytanie 26) oraz tworzy ryzyko sporu na etapie odbioru — Zamawiający może żądać publikacji danych, których publikacja jest prawnie zabroniona, a Wykonawca nie będzie miał formalnej podstawy do odmowy w zakresie umowy.

Zgodnie z art. 99 ust. 1 ustawy Pzp opis przedmiotu zamówienia musi być sporządzony w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń. Wnosimy o:

- a) doprecyzowanie listy datasetów (zbiorów danych) podlegających publikacji w portalu Otwarte Dane Wrocław, ze wskazaniem dla każdego datasetu: nazwy, opisu, schematu (lista pól + typy), przykładowego rekordu, częstotliwości aktualizacji, formatu pliku eksportu (CSV / JSON / XML / RDF / API REST);
- b) potwierdzenie, że publikacji w Otwartych Danych nie podlegają dane osobowe użytkowników
- c) (rodziców, dzieci, pracowników żłobków) ani dane szczególnej kategorii (art. 9 RODO);
- d) potwierdzenie, że dopuszczalne typy publikowanych danych obejmują wyłącznie dane zagregowane lub zanonimizowane, w szczególności: zagregowane statystyki frekwencji w żłobkach (procentowe, bez identyfikacji konkretnych dzieci); zajętość miejsc w żłobkach (liczba wolnych miejsc per żłobek, bez danych dzieci na liście); jadłospisy publiczne (dla wszystkich dzieci, bez powiązania z danymi konkretnego dziecka); listy żłobków publicznych wraz z ich ofertą i lokalizacją; agregowane dane o procesie rekrutacji (liczba zgłoszeń, liczba przyjętych, bez danych osobowych);
- e) doprecyzowanie, że za zgodność publikowanych danych z RODO odpowiada Zamawiający (jako

Administrator Danych Osobowych), zaś Wykonawca jako Procesor wykonuje wyłącznie polecenia Zamawiającego dotyczące publikacji w Otwartych Danych — zgodnie z umową powierzenia przetwarzania danych osobowych.

Odpowiedź:

Zbiorami eksportowanymi na portal OpenData będą: ilość aktywnych żłobków w ujęciu rocznym oraz ilość przyjętych podopiecznych w danym roku. Dane mają mieć charakter wyłącznie liczbowy a częstotliwość raz na miesiąc kalendarzowy w metodzie wybranej podczas Analizy Przedwdrożeniowej.

24. dot. SWS.45 / WT.07

Wymaganie SWS.45 wymaga „dedykowanej aplikacji mobilnej dystrybuowanej w Google Play oraz Apple App Store”. Wymaganie aplikacji wyłącznie w modelu natywnej dystrybucji w sklepach mobilnych:

- a) wymaga utrzymywania dwóch oddzielnych stacków technologicznych (Swift / SwiftUI dla iOS oraz Kotlin / Jetpack Compose dla Android) lub frameworka cross-platform (React Native, Flutter), co zwiększa koszt utrzymania bez wymiernych korzyści funkcjonalnych dla Zamawiającego;
- b) podlega procesowi review w obu sklepach (Apple App Review zwykle 24–72 godziny, Google Play Review zwykle 1–7 dni), co wydłuża cykl wdrożeniowy każdej poprawki — w szczególności poprawek bezpieczeństwa (krytyczne CVE w bibliotekach), gdzie czas reakcji jest wymierny w godzinach, a nie dniach;
- c) wymaga utrzymywania osobnego stacku technologicznego niewymaganego przez naturę Systemu — funkcje rekrutacji i dziennika elektronicznego są typowo realizowane w architekturze webowej. Aplikacja PWA (Progressive Web App) zapewnia: brak vendor lock-in wobec Apple i Google; pełną zgodność z wymaganiami ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (WCAG 2.1 AA — implementacja Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2102 z 26 października 2016 r.); zgodność z Krajowymi Ramami Interoperacyjności w zakresie otwartych standardów W3C (Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, tekst jednolity Dz.U. 2017 poz. 2247); zgodność z European Interoperability Framework (Komunikat Komisji Europejskiej COM(2017) 134 — Nowe europejskie ramy interoperacyjności); możliwość natychmiastowego deploymentu (rollout w ciągu minut, a nie dni przez proces review w sklepach); niższy całkowity koszt utrzymania (TCO). Wnosimy, zgodnie z art. 101 ust. 5 ustawy Pzp, o uznanie za rozwiązanie równoważne dla „dedykowanej aplikacji mobilnej w Google Play / Apple App Store”:

1) aplikacji typu Progressive Web App (PWA) zgodnej z W3C Manifest, Service Worker API, Web Push API, dystrybuowanej poprzez stronę internetową Wykonawcy, z opcjonalną instalacją „Add to Home Screen” na ekranie głównym urządzenia użytkownika (Android, iOS, Windows, macOS, Linux); 2) PWA dystrybuowanej dodatkowo poprzez

Trusted Web Activity (Android) z opcjonalną publikacją w Google Play, jeżeli Zamawiający wymaga obecności w sklepie Google Play.

Aplikacja PWA zapewnia w pełni równoważną funkcjonalność do natywnej aplikacji mobilnej w zakresie: powiadomień push (Web Push API + Firebase Cloud Messaging), obsługi offline (Service Worker + IndexedDB / Cache API), geolokalizacji (Geolocation API), kamery (MediaDevices API — kod QR, dokumenty), trwałego przechowywania danych (IndexedDB), instalacji na ekranie głównym (Web App Manifest), pełnoekranowego trybu pracy (display: standalone), integracji z systemem operacyjnym (Web Share API, Background Sync).

Odpowiedź:

Zamawiający podtrzymuje dotychczasowe zapisy.

25. dot. WT.12

Wymaganie WT.12 OPZ wymaga: "Hasło w systemie musi składać się z minimum 10 znaków i musi zawierać małe i wielkie litery oraz cyfry i znaki specjalne". Następnie WT.12 dopowiada: "Dla użytkownika zwykłego należy przewidzieć inny zestaw znaków dla zapewnienia poprawnego dostępu do dokumentów zabezpieczonych hasłem (pdf — bez polskich znaków, spacji itp.)". Czy Zamawiający potwierdza, że dla roli Rodzic/Opiekun możliwe jest odrębne uproszczenie polityki haseł — minimum 8 znaków, bez wymogu czterech grup znaków — w drodze parametryzacji systemowej, biorąc pod uwagę że WT.12 wprost przewiduje "inny zestaw znaków" dla użytkownika zwykłego, oraz że polityka 10 znaków + cyfry + małe + duże + znaki specjalne dla rodzica zgłaszającego nieobecność dziecka jest nieproporcjonalnie restrykcyjna i prowadzi do nadużywania funkcji "zapomniałem hasła"?

Odpowiedź:

Zamawiający nie potwierdza i podtrzymuje obecne zapisy.

26. dot. WO.17

Wymaganie WO.17 opisuje „ticketing przez SMTP”. W praktyce e-mail nie jest systemem ticketingowym — jest kanałem transportowym. Profesjonalne systemy ticketingowe (Jira Service Management, Zendesk, OTRS, Freshdesk) wymagają interfejsu webowego, statusów ticketów, SLA, eskalacji. Czy Zamawiający precyzuje, czy oczekuje: a) prostego mechanizmu wysyłki maila o ID wniosku z konta Rodzica (zgodnie z literą SWS.17), b) pełnego systemu ticketingowego dla operatorów (z UI, dashboardami, raportami), c) integracji z istniejącym Redmine na redmine.cui.wroclaw.pl (wzmiankowanym w sekcji 2b OPZ)?

Odpowiedź:

Zamawiający oczekuje, że rodzic/opiekun prawny będzie mógł zgłaszać zapytania/problemy m.in. za pośrednictwem maila. Przesłanie maila na wskazany adres poczty elektronicznej spowoduje automatyczne utworzenie zgłoszenia, z tematem taki jak temat wiadomości. Wątki będą grupowane po adresie nadawcy (wszystkie ewentualne kolejnego zgłoszenia będą rozpoznawane jako zgłaszane od danego użytkownika). Nie określamy innych sposobów zakładanie zgłoszeń - tu zdajemy się na propozycję potencjalnego wykonawcy systemu.

Zamawiający wskazał w OPZ, że nie precyzuje konkretnych rozwiązań/mechanizmów w zakresie działania takiego systemu. Wskazane zostało jasno, że Zamawiający oczekuje propozycji takiego rozwiązania ze strony potencjalnego wykonawcy. W Analizie Przedwdrożeniowej będzie to uszczegóławiane po przedstawieniu rozwiązania Wykonawcy.

Oczekiwane przez Zamawiającego funkcjonalności systemu powinny odpowiadać podstawowym funkcjonalnością jak w popularnych systemach ticketowych (np.: Jira, OsTicket, etc.). Oczekujemy systemu ticketowego umożliwiającego sprawne zarządzanie zgłoszeniami, w tym ich kategoryzację, priorytetyzację, przypisywanie do użytkowników oraz monitorowanie statusów i historii komunikacji. System powinien również zapewniać automatyzację procesów (powiadomienia, SLA), raportowanie oraz integrację z pocztą elektroniczną.

Doprecyzowanie zakresu prac

27. dot. WTAB.5

Wymaganie WTAB.5 definiuje RPO 1 dzień, RTO 4h. Czy Zamawiający precyzuje:

- a) od którego momentu liczone jest 4h RTO — od wykrycia awarii, zgłoszenia przez Zamawiającego, czy rozpoczęcia procedury DR;
- b) czy zaplanowane okna serwisowe (uzgodnione z Zamawiającym) są wyłączone z liczenia downtime'u dla SLA (WTAB.9);
- c) wymaganą częstotliwość testów DR (drills) — kwartalnie, rocznie, raz na 2 lata?

Odpowiedź:

- a) Od wykrycia awarii i/oraz zgłoszenia
- b) Tak,
- c) Rocznie.

28. dot. WTAB.8

Wymaganie WTAB.8 OPZ stanowi: "Wykonawca zapewni Zamawiającemu dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług Chmury

oraz metod weryfikacji poprawności ich konfiguracji i działania (...) Zakres informacji zawartych w instrukcjach zapewni możliwość przeniesienia systemu do innego dostawcy chmurowego". Czy Zamawiający potwierdza, że: a) zakres dokumentacji konfiguracji ma obejmować runbooks/Terraform/Ansible playbooks (Infrastructure as Code) — w formie umożliwiającej automatyczne odtworzenie infrastruktury — czy wystarczy opis architektury w formie tekstowej z diagramami i parametrami konfiguracyjnymi; b) format eksportu danych jest zgodny z WO.12 OPZ (XML lub format uzgodniony w Analizie)?

Odpowiedź:

Zamawiający potwierdza, że zakres dokumentacji konfiguracji ma obejmować runbooks/Terraform/Ansible playbooks (Infrastructure as Code) w formie umożliwiającej automatyczne odtworzenie infrastruktury, format eksportu danych jest zgodny z WO.12.

29. dot. SWS.84 (formaty)

Wymaganie SWS.84 OPZ stanowi: "Format plików do uzgodnienia na etapie Analizy Przedwdrożeniowej (zwyczajowo *.csv)". Czy Zamawiający potwierdza, że formatem domyślnym integracji finansowo-księgowej jest CSV, a docelowy schemat plików zostanie ustalony w ramach Analizy Przedwdrożeniowej dla każdej grupy zainteresowanych jednostek?

Odpowiedź:

Tak, Zamawiający potwierdza, że formatem domyślnym integracji finansowo-księgowej jest CSV, ale nie wyklucza to używania innych formatów wskazanych w Załączniku nr 1.

30. dot. SWS.84 (kontrahenci)

Wymaganie SWS.84 wskazuje na eksport „kontrahentów” do systemu FK. W kontekście dziennika elektronicznego „kontrahentem” jest rodzic/opiekun (płatnik za pobyt dziecka). Pojęcie „kontrahent” sugeruje terminologię systemów ERP dla relacji B2B. Czy Zamawiający potwierdza, że eksport dotyczy rodziców jako płatników (z zachowaniem RODO)?

Odpowiedź:

Zamawiający potwierdza, że eksport dotyczy rodziców jako płatników. W systemie księgowym wykorzystywanym przez WZZ kontrahentem jest rodzic lub opiekun prawny, którego dane widnieją w polu „Nazwa kontrahenta”. Natomiast na potrzeby wewnętrznej identyfikacji najczęściej wykorzystywana jest nazwa skrócona kontrahenta, zawierająca imię i nazwisko dziecka.

31. dot. WO.15 (wycena)

Wymaganie WO.15 wymaga „wdrożenia integracji z Open Data Wrocław” oraz „przesłania na portal dowolnych danych opublikowanych i skatalogowanych w Systemie”, z odesłaniem do Analizy Przedwdrożeniowej. Brak zdefiniowanego zakresu danych, ich struktur, częstotliwości publikacji oraz mechanizmu transformacji uniemożliwia rzetelną wycenę pracy w tym zakresie. Czy Zamawiający może na etapie postępowania doprecyzować: a) listę zbiorów danych do publikacji, b) szacunkową liczbę endpointów API, c) format danych (CSV, JSON, RDF), d) częstotliwość publikacji (real-time, dzienna, miesięczna)? Bez tych danych każdy Wykonawca dokona innego oszacowania, co może prowadzić do nieuczciwego porównania ofert.

Odpowiedź:

Zbiorami eksportowanymi na portal OpenData będą: ilość aktywnych żłobków w ujęciu rocznym oraz ilość przyjętych podopiecznych w danym roku. Dane mają mieć charakter wyłącznie liczbowy a częstotliwość raz na miesiąc kalendarzowy w metodzie wybranej podczas Analizy Przedwdrożeniowej.

32. dot. WA.02

Wymaganie WA.02 wymaga „kopii zapasowej do odtworzenia oryginalnych danych”, bez wskazania:

a) formatu kopii — pełny snapshot serwera (Veeam, Acronis), zrzut bazy danych (mysqldump, pg_dump), backup logiczny per tabela, czy inkrementalne bloki dyskowe; b) kanału przekazania — dedykowany link FTPS, S3-compatible, fizyczny nośnik; c) częstotliwości wykonywania kopii (dzienna, godzinowa, real-time); d) retencji kopii (30 dni, 1 rok, cały okres umowy + 5 lat dla RODO). Brak precyzji uniemożliwia wycenę usługi backupu i wybór właściwego rozwiązania.

Odpowiedź:

System musi posiadać zabezpieczenie w postaci kopii zapasowych.

Kopie zapasowe muszą być składowane w co najmniej dwóch różnych lokalizacjach przy czym co najmniej jedna z nich nie może być w tym samym centrum przetwarzania danych i tej samej miejscowości, w której jest rozlokowany system.

Kopie zapasowe muszą być testowane co najmniej raz w roku poprzez odtworzenie w odrębnym środowisku disaster recovery, przy czym pierwsze testowe odtworzenie musi zostać wykonane przed produkcyjnym uruchomieniem systemu. Zamawiający może zażądać udziału w testach.

Kopie zapasowe muszą być szyfrowane w sposób uniemożliwiający odczytanie danych kopii zapasowych poza systemem backupu z nośników, na których są składowane.

Dostęp do kopii zapasowych musi podlegać nadzorowi. Zapisy o pobraniu lub odtwarzaniu danych z kopii zapasowych muszą być dostępne dla Zamawiającego w całym okresie świadczenia usługi (wzgl. muszą być na bieżąco przesyłane Zamawiającemu pod wskazany adres email).

33. dot. WA.04

Wymaganie WA.04 OPZ wymaga, aby "decyzja o rozbudowie/poprawie Systemu (upgrade) była zatwierdzona przez Administratora Głównego". W praktyce wersjonowanie SemVer rozróżnia trzy poziomy: Major (X.0.0) — breaking changes, Minor (X.Y.0) — nowe funkcjonalności kompatybilne, Patch (X.Y.Z) — poprawki bezpieczeństwa i błędów. Czy Zamawiający potwierdza, że: a) Major version wymaga akceptacji Administratora Głównego; b) Minor version wymaga jedynie powiadomienia ex post; c) Patch (security fix) Wykonawca może wdrożyć niezwłocznie i samodzielnie (zgodnie z WB.6 i WL.3 OPZ wymagającymi regularnych aktualizacji eliminujących luki bezpieczeństwa), informując Administratora ex post?

Odpowiedź:

Dla Zamawiającego każdorazowa poprawka wymaga uzgodnień, bez względu na poziom poprawki.

34. dot. Rozdz. 3.7 SWZ

SWZ traktuje rekrutację i dziennik elektroniczny jako jedno zamówienie nierozdzielne (Rozdz. 3.7), ale w OPZ wielokrotnie odnosi się do nich jako do dwóch obszarów funkcjonalnych. Czy Zamawiający dopuszcza, aby rekrutacja i dziennik elektroniczny były dwoma odrębnymi aplikacjami zintegrowanymi przez SSO i API, działającymi pod różnymi subdomenami (np. rekrutacja.zlobki.wroclaw.pl i dziennik.zlobki.wroclaw.pl)? Wymaganie monolitu utrudnia tworzenie konsorcjów i ogranicza konkurencję wbrew art. 99 ust. 4 ustawy Pzp.

Odpowiedź:

Zamawiający oczekuje, że system będzie jednorodny i dostępny pod jednym adresem. Obszar funkcjonalny oznacza pewien zespół funkcji biznesowych, a nie oznacza oddzielnych aplikacji.

35. dot. WO.01

Wymaganie WO.01 stanowi: „Domenę oraz podmiot dostarczający domenę wraz z certyfikatem SSL zostanie wskazany na etapie Analizy”. Czy Zamawiający potwierdza, że: a) Domena — Zamawiający wskaże własną subdomenę pod wroclaw.pl lub cui.wroclaw.pl, czy też Wykonawca ma zarejestrować nową domenę publiczną; b) Certyfikat SSL — czy dopuszczalne jest stosowanie Let's Encrypt (DV, klucz RSA 2048+ lub ECDSA P-256, automatyczna rotacja co 90 dni), czy Zamawiający wymaga certyfikatu OV/EV

od komercyjnego CA (DigiCert, Sectigo, GlobalSign); c) Koszt — który z podmiotów (Wykonawca/Zamawiający) ponosi koszt domeny i certyfikatu w cyklu życia umowy?

Odpowiedź:

Zamawiający wskaże własną domenę i dostarczy certyfikat SSL. Przy czym w przypadku modelu SaaS gdy usługa ma być dostępna pod jakimś innym adresem niż natywny Wykonawcy, wtedy Wykonawca wraz Zamawiającym muszą zapewnić przekierowania.

36. dot. SWS.05 i SWS.40

Wymaganie SWS.05 wymaga, by System dokonywał walidacji unikalności wniosku przy zapisie (po PESEL lub kombinacji imię/nazwisko/data urodzenia w przypadku braku PESEL). SWS.40 wymaga osobno codziennej weryfikacji duplikatów przez raport. Jeśli walidacja przy zapisie skutecznie zapobiega duplikatom (SWS.05), codzienny raport z SWS.40 wykrywa wyłącznie błędy mechanizmu walidacji lub przypadki, gdy to samo dziecko jest zgłaszane dwoma sposobami (raz z PESEL, raz bez). Czy Zamawiający potwierdza intencję SWS.40 jako: a) raport diagnostyczny weryfikujący poprawność działania SWS.05; b) mechanizm wykrywania duplikatów ponad PESEL (np. dwóch rodziców zgłosiło to samo dziecko z różnymi PESELami z literówką)?

Odpowiedź:

Zamawiający potwierdza.

37. dot. SWS.46 (architektura NFC)

Wymaganie SWS.46 OPZ wymaga, aby aplikacja mobilna "komunikowała się za pomocą NFC z czytnikiem lub kartą". To jest technicznie niejednoznaczne i prowadzi do dwóch różnych implementacji: a) NFC HCE (Host Card Emulation) — telefon udaje kartę zbliżeniową, fizyczny czytnik w placówce odczytuje telefon (Android pełne wsparcie, iOS bardzo ograniczone — wymaga specjalnego programu Apple Developer); b) NFC Reader Mode — telefon czyta kartę dziecka (Android pełne wsparcie, iOS od iOS 11 z ograniczeniami — tylko NDEF, brak MIFARE Classic na iPhone < XS). Czy Zamawiający precyzuje, którą z dwóch architektur ma realizować aplikacja mobilna? Czy dopuszcza rozwiązanie hybrydowe: stacjonarny czytnik NFC/RFID w placówce (zgodnie z SWS.80, alternatywnie kody QR drukowane przy stanowiskach) wraz z aplikacją mobilną realizującą skanowanie kodów QR oraz pozostałe funkcje pomocnicze (zgłoszenia nieobecności, podgląd godzin, opłaty)?

Odpowiedź:

Zamawiający dopuszcza każde rozwiązanie, które spełni wymaganie wskazane w Załączniku nr 1.

38. dot. SWS.49

Wymaganie SWS.49 wymaga, by System „posiadał wydzielony Panel administracyjny wywoływany pod osobnym linkiem”. Standardową praktyką w nowoczesnych systemach SaaS jest wspólny URL z routinguem opartym o rolę użytkownika (po zalogowaniu System rozpoznaje rolę i prezentuje odpowiedni panel). Wydzielanie URL panelu administracyjnego nie zwiększa bezpieczeństwa (security through obscurity) i komplikuje zarządzanie certyfikatem SSL, monitoringiem oraz polityką haseł. Czy Zamawiający dopuszcza rozwiązanie równoważne — wspólny URL z autentyczną segregacją uprawnień opartą o RBAC i WAF rules — przy zachowaniu tych samych mechanizmów bezpieczeństwa (SWS.53, SWS.54, MFA)?

Odpowiedź:

Zamawiający precyzuje, iż pod pojęciem wydzielonego panelu administracyjnego wywoływanego pod osobnym linkiem rozumie separację panelu administracyjnego od modułu rekrutacji i dziennika elektronicznego, lecz nie wymaga odmiennego adresu url.

39. dot. SWS.07 / SWS.08

OPZ w wielu miejscach (SWS.79–SWS.91, WT, WTAB) zakłada istniejący produkt SaaS gotowy do dostosowania. Jednocześnie wymagania SWS.07 („Wykonawca musi przygotować projekt formularzy i strony w formie makiet”) i SWS.08 („Elementy architektury danych... Wykonawca opracuje i przekaze do akceptacji”) sugerują opracowanie systemu od podstaw według specyfikacji opracowanej dopiero w Analizie Przedwdrożeniowej. Czy Zamawiający potwierdza, że OPZ dotyczy istniejącego produktu typu COTS/SaaS dostosowanego do potrzeb Zamawiającego (zgodnie z warunkiem 6.2.4.1 SWZ — wymagane referencje wdrożenia w SaaS), a nie systemu projektowanego ad hoc? W tym kontekście SWS.07/SWS.08 należy rozumieć jako dostosowanie wyglądu i parametryzacji istniejącego produktu, a nie pełnoprawny etap projektowy?

Odpowiedź:

Zamawiający nie potwierdza, że OPZ wskazuje na istniejący produkt. Zamawiający dopuszcza dostosowanie gotowego rozwiązania jak i zbudowanie go od podstaw.

40. dot. WTAB.1, WTAB.9, WTAB.20, WTAB.22

Wymagania techniczne z Załącznika nr 1 do OPZ wskazują:

WTAB.1 (TenantID — separacja tenantów); WTAB.9 (TIER III Uptime Institute); WTAB.20 (moduł kryptograficzny FIPS 140-2 Level 2); WTAB.22 (AES-256 oraz para kluczy asymetrycznych 2048 bit). W każdym z tych przypadków istnieją równoważne (lub nowsze i silniejsze) standardy

europejskie i międzynarodowe powszechnie stosowane przez sektor publiczny w UE. W szczególności:

- a) WTAB.9 — TIER III Uptime Institute jest standardem amerykańskim. Europejskim odpowiednikiem o tych samych wymaganiach dostępności jest norma EN 50600 (klasy 3 lub 4) oraz certyfikacja TÜV TSI Level 3/4. Wnosimy o uznanie EN 50600 klasa 3/4 oraz TÜV TSI Level 3 za równoważne wymaganiu TIER III, zgodnie z art. 101 ust. 5 ustawy Pzp;
- b) WTAB.20 — FIPS 140-2 Level 2 jest standardem amerykańskim (NIST), wycofywanym z dniem 22 września 2026 roku na rzecz FIPS 140-3. W obszarze UE i sektorze publicznym standardem równoważnym jest Common Criteria (ISO/IEC 15408) na poziomie EAL4+ dla modułów kryptograficznych. Wnosimy o uznanie Common Criteria EAL4+ (lub wyższego) za równoważne wymaganiu FIPS 140-2 Level 2, zgodnie z art. 101 ust. 5 ustawy Pzp; ewentualnie o zastąpienie wymagania FIPS 140-2 Level 2 wymaganiem zgodności z eIDAS Annex II (kwalifikowane urządzenie do składania podpisu) lub Common Criteria EAL4+;
- c) WTAB.22 — wymóg pary kluczy asymetrycznych 2048 bit (RSA-2048) jest poniżej obecnego standardu bezpieczeństwa rekomendowanego przez NIST SP 800-131A i ENISA. Aktualne dobre praktyki (NIST od 2024, ENISA Cryptographic Recommendations 2024) zalecają RSA-3072 lub RSA4096 dla nowych systemów uruchamianych po 2026 roku, lub klucze ECC o długości co najmniej 256 bit (krzywe P-256, P-384). Wnosimy o doprecyzowanie WTAB.22 jako: "klucze asymetryczne RSA o długości co najmniej 3072 bit lub klucze ECC krzywych P-256 / P-384";
- d) WTAB.1 — wymóg TenantID może być rozumiany jako: separacja sprzętowa (osobne maszyny fizyczne per Tenant), separacja wirtualizacyjna (osobne VM), separacja kontenerowa (osobne kontenery), lub separacja aplikacyjna (wspólna baza danych z kolumną TenantID i RLS — Row Level Security). Wnosimy o doprecyzowanie, czy WTAB.1 wymaga separacji sprzętowej, czy wystarczająca jest separacja aplikacyjna (multi-tenant SaaS) z mechanizmem Row Level Security w bazie danych, co jest standardem wdrożeń SaaS w sektorze publicznym UE (np. mObywatel, KSeF).

Niezależnie od powyższego prosimy o wskazanie, czy wymagania WTAB.1, WTAB.9, WTAB.20, WTAB.22 zostały sformułowane: (i) w oparciu o analizę przedwdrożeniową prowadzoną przez CUI; (ii) w oparciu o specyfikację konkretnego produktu wskazanego przez analityków biznesowych; (iii) z dokumentów referencyjnych (np. KSC, Krajowe Ramy Interoperacyjności, RODO art. 32). Wskazanie źródła pozwoli Wykonawcom ocenić zasadność wymagań pod kątem proporcjonalności (art. 99 ust. 4 ustawy Pzp).

Odpowiedź:

WTAB.1a wskazuje że dostawca **może** zastosować separacje sprzętową, natomiast wymagania powstawały w oparciu o dokumenty referencyjne i najlepsze praktyki dostępne w czasie powstawania wymagań min. NSC,

OWASP TOP 10. We wcześniejszych pytaniach gdzie pojawiły się niejasności dokonano zmiany.

41. Dotyczy: Załącznik nr 8 do SWZ - Projekt Umowy

Czy Zamawiający wyraża zgodę, aby w projekcie umowy Zamawiający zostały dodane zapisy realizujące wymogi Data Act (kompleksowe zasady zwrotu danych Zamawiającego) Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (Akt w sprawie danych). Data Act jest stosowane od 12 września 2025 r.

Odpowiedź:

Zamawiający nie wyraża zgody.

42. Dotyczy: Załącznik nr 8 do SWZ - Projekt Umowy

W §1 umowy określono: „System Informatyczny lub System - Kompleksowy System Rekrutacyjny tj. zbiór programów komputerowych wraz z innymi elementami stanowiącymi utwór w rozumieniu Prawa autorskiego, do którego majątkowe prawa autorskie przysługują Wykonawcy, za wyjątkiem wykorzystanych Systemie bibliotek i komponentów dostawców/licencjodawców zewnętrznych (m.in. osób trzecich lub społeczności); udostępniony Zamawiającemu do korzystania w modelu SaaS w celu przeprowadzania rekrutacji do wskazanych przez Zamawiającego źłobków, którego szczegółowe wymagania funkcjonalne i pozafunkcjonalne opisane są w Załączniku nr 1 do Umowy – Specyfikacja wymagań.” W umowie w § 2. Ust. 1 pkt 9) jest mowa o udzieleniu Zamawiającemu niewyłącznej i nieprzenoszalnej licencji na korzystanie z Systemu i jego Dokumentacji na zasadach określonych w Umowie.

W projekcie umowy §2 ust 1. Pkt 8) jest mowa o wykonaniu i wdrożeniu aplikacji mobilnej stanowiącą składową systemu na platformy Android oraz iOS wraz z wykonaniem testów bezpieczeństwa po stronie Wykonawcy. Obecna definicja Systemu w § 1 oraz zapisy licencyjne w § 2 ust. 1 pkt 9) mogą budzić wątpliwości interpretacyjne w zakresie tego, czy aplikacja mobilna (jako "składowa systemu" wymieniona w osobnym punkcie) jest objęta tą samą licencją co System.

Czy Zamawiający doprecyzuje zapisy dotyczące udzielenia licencji, aby jednoznacznie wskazać, że zakres licencji, o której mowa w § 2 ust. 1 pkt 9), obejmuje również aplikację mobilną opisaną w § 2 ust. 1 pkt 8) projektu umowy?

Odpowiedź:

Zamawiający **zmienia treść Załącznika nr 8 do SWZ - Projekt Umowy** poprzez wykreślenie w § 1 dotychczasowej definicji „System Informatyczny lub System” i zastępuje ją nową w brzmieniu:

"System informatyczny lub System - Kompleksowy System Rekrutacyjny tj. zbiór programów komputerowych wraz z aplikacją mobilną oraz z innymi elementami stanowiącymi utwór w rozumieniu Prawa autorskiego, do którego majątkowe prawa autorskie przysługują Wykonawcy, za wyjątkiem wykorzystanych Systemie bibliotek i komponentów dostawców/licencjodawców zewnętrznych (m.in. osób trzecich lub społeczności); udostępniony Zamawiającemu do korzystania w modelu SaaS w celu przeprowadzania rekrutacji do wskazanych przez Zamawiającego źłobków, którego szczegółowe wymagania funkcjonalne i pozafunkcjonalne opisane są w **Załączniku nr 1 do Umowy – Specyfikacja wymagań.**"

43. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 3 ust. 3 i § 9 ust. 2

Treść pierwotnego zapisu:

„W przypadku przekroczenia przez Wykonawcę terminów realizacji przedmiotu umowy z przyczyn leżących po jego stronie, niezależnie od odpowiedzialności wynikającej z Umowy i obowiązujących przepisów, Wykonawca będzie zobowiązany do wykonania, na własny koszt, ewentualnych dodatkowych prac, jakie okażą się niezbędne w związku z nieterminową realizacją przedmiotu Umowy.”

Pytanie:

Obecne brzmienie zapisu wprowadza po stronie Wykonawcy obowiązek o charakterze nieograniczonym, zarówno co do zakresu, jak i kosztu dodatkowych prac. Wnosimy o usunięcie zapisu w całości bądź doprecyzowanie, co oznaczają „ewentualnych dodatkowych prac, jakie okażą się niezbędne w związku z nieterminową realizacją przedmiotu Umowy”.

W obecnym brzmieniu zapis ten nie określa zakresu ani charakteru „dodatkowych prac”, co może prowadzić do rozbieżności interpretacyjnych na etapie realizacji umowy oraz ryzyka rozszerzenia zakresu świadczenia Wykonawcy poza pierwotny przedmiot umowy. Jednocześnie przewidziany obowiązek ma charakter nieograniczony kosztowo i funkcjonuje niezależnie od innych sankcji umownych, co z kolei może skutkować nieproporcjonalnym obciążeniem Wykonawcy oraz wpływać na zaburzenie konkurencyjności postępowania.

Mając na uwadze powyższe, czy Zamawiający rozważy doprecyzowanie wskazanego postanowienia poprzez:

- 1) wskazanie, że przyczyny przekroczenia terminów realizacji przez Wykonawcę, skutkujące koniecznością wykonania prac dodatkowych, dotyczyć będzie wyłącznie opóźnień zawinionych przez Wykonawcę?

- 2) Potwierdzenie, że opóźnienia wynikające z działań lub zaniechań Zamawiającego, opóźnień w przekazywaniu danych oraz problemów integracyjnych po stronie Zamawiającego nie będą traktowane jako leżące po stronie Wykonawcy lub przez niego zawinione?
- 3) ograniczenie „dodatkowych prac” wyłącznie do działań pozostających w bezpośrednim związku przyczynowym z opóźnieniem zawinionym przez Wykonawcę,
- 4) wskazanie, że dodatkowe prace nie mogą prowadzić do rozszerzenia zakresu przedmiotu Umowy,
- 5) wprowadzenie ograniczenia (limitu) kosztowego tych prac dodatkowych i wskazanie, że prace ponad ten limit będą realizowane w ramach np. prawa opcji,
- 6) doprecyzowanie, że obowiązek ich wykonania nie prowadzi do wielokrotnego obciążenia Wykonawcy za to samo zdarzenie (w szczególności w przypadku naliczania kar umownych).

Odpowiedź:

Zamawiający nie wyraża zgody na zmianę zapisu Umowy w tym zakresie.

44. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 5 ust. 3

Treść pierwotnego zapisu:

„Zamawiający ma prawo do odstąpienia od Umowy (umowne prawo odstąpienia) bez podania przyczyny, również wówczas, gdy Wykonawca wykonuje Umowę w sposób należyty, w terminie do 1 miesiąca od dnia przewidzianego w Harmonogramie ramowym na odbiór Analizy Przedwdrożeniowej, ale jednocześnie nie później niż 30 dni od dnia Odbioru Analizy Przedwdrożeniowej. W takim przypadku odstąpienie od Umowy ma skutek wyłącznie na przyszłość, a Zamawiający zobowiązany jest do zapłaty odstępnego równego wynagrodzeniu, które należy się Wykonawcy za rzeczywiście wykonane prace.”

Pytanie:

Czy Zamawiający wyjaśni jaki jest powód wprowadzenia prawa odstąpienia od umowy bez podania przyczyny oraz wskaże, czy dopuszcza ograniczenie tego prawa do określonych, konkretnych i mierzalnych przesłanek?

Ewentualnie czy Zamawiający rozważy usunięcie tego postanowienia w całości?

Jak Zamawiający definiuje rzeczywiście wykonane prace i czy Zamawiający potwierdza, że rzeczywiście wykonane prace obejmują również prace koncepcyjne, przygotowanie architektury oraz inne prace, które mogły zostać wykonane przez Wykonawcę? Ponadto czy Zamawiający przewiduje zwrot

kosztów przygotowawczych, kosztów zasobów zarezerwowanych na projekt, kosztów licencji / infrastruktury przygotowanej pod projekt?

Odpowiedź:

Zamawiający standardowo wprowadza zapis celem możliwości rezygnacji z realizacji umowy gdyby na etapie prac nad Analizą Przedwdrożeniową ocenił, iż zaangażowanie i efekty prac po stronie Wykonawcy nie będą w stanie doprowadzić do rzetelnego i treściwego przygotowania dokumentu, co w następnym kroku uniemożliwi wdrożenie systemu o oczekiwanych wartościach i doprowadzi do negatywnego efektu wdrożeniowego projektu w postaci jego braku.

45. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 5 ust. 4

Treść pierwotnego zapisu:

„O ile sporządzona przez Wykonawcę Analiza Systemowa stanowi utwór w rozumieniu przepisów ustawy o prawie autorskim i prawach pokrewnych toż chwilą zapłaty przez Zamawiającego wynagrodzenia za Analizę Systemową Zamawiający nabywa całość autorskich praw majątkowych do Analizy Systemowej oraz praw zależnych na następujących polach eksploatacji”

Pytanie:

Czy mając na uwadze, że Analiza Systemowa przygotowywana przez Wykonawcę może zawierać elementy stanowiące jego know-how, w szczególności dotyczące architektury systemów SaaS, stosowanych wzorców projektowych, standardowych komponentów technologicznych, metodyk analitycznych oraz rozwiązań wielokrotnego użytku, a także inne elementy o charakterze ogólnym i niezależnym od konkretnego wdrożenia, Wykonawca zwraca się z uprzejmą prośbą o rozważenie przez Zamawiającego modyfikacji przedmiotowego postanowienia w kierunku rezygnacji z przeniesienia autorskich praw majątkowych do Analizy Systemowej na rzecz udzielenia Zamawiającemu niewyłącznej licencji na jej wykorzystanie w zakresie niezbędnym do realizacji, wdrożenia, utrzymania i rozwoju Systemu?

Ewentualnie, w przypadku utrzymania modelu przeniesienia praw, czy Zamawiający doprecyzuje przedmiotowe postanowienie poprzez wyraźnego wyłączenia z zakresu Analizy Systemowej i przeniesienia praw autorskich elementów stanowiących know-how Wykonawcy, w szczególności: standardowych komponentów i bibliotek SaaS, ogólnych wzorców architektonicznych, metodyk analitycznych i projektowych, narzędzi oraz rozwiązań wielokrotnego użytku, a także wszelkich elementów niewytworzonych wyłącznie na potrzeby realizacji niniejszego zamówienia.

W ocenie Wykonawcy takie podejście pozwoliłoby na zachowanie równowagi pomiędzy interesem Zamawiającego w zakresie możliwości pełnego wykorzystania dokumentacji na potrzeby wdrożenia Systemu, a

koniecznością ochrony dorobku technologicznego i modelu działania Wykonawcy w środowisku SaaS

Odpowiedź:

Zamawiający nie wyraża zgody na zmianę zapisu Umowy w tym zakresie.

46. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 7 ust. 3

Treść pierwotnego zapisu:

„Strony potwierdzają, że przedmiotem Umowy jest wykonanie dzieła, a pełna weryfikacja dzieła – w tym jego ewentualna integracja z innym oprogramowaniem oraz wydajność – będzie możliwa wyłącznie po jego całkowitym wykonaniu i przedstawieniu do Odbioru Wdrożenia. Jakikolwiek Odbiory poszczególnych Produktów lub Etapów nie wyłączają prawa Zamawiającego do weryfikacji całości Wdrożenia.”

Pytanie:

Mając na uwadze, że przedmiotem Umowy – zgodnie z jej pozostałymi postanowieniami – jest świadczenie usług w modelu SaaS, Wykonawca zwraca się z prośbą o wyjaśnienie oraz ewentualne doprecyzowanie wskazanego zapisu, w szczególności poprzez:

- 1) wskazanie czy Zamawiający potwierdza, że umowa ma charakter umowy o świadczenie usług (model SaaS), a nie umowy o dzieło w rozumieniu przepisów Kodeksu cywilnego? W konsekwencji, czy Zamawiający rozważy usunięcie sformułowania: „przedmiotem Umowy jest wykonanie dzieła” w celu zapewnienia spójności z usługowym charakterem Umowy?
- 2) Potwierdzenie, że odpowiedzialność Wykonawcy ma charakter starannego działania właściwego dla usług SaaS, a nie odpowiedzialności za „dzieło” rozumiane jako rezultat końcowy całego systemu, który będzie później utrzymywany w ramach Etapu IV?

Odpowiedź:

Zamawiający **zmienia treść §7 ust. 3 Załącznika nr 8 do SWZ - Projekt Umowy** poprzez wykreślenie dotychczasowej treści i zastępuje ją nową w brzmieniu:

„Strony potwierdzają, że przedmiotem Umowy jest świadczenie usług, a pełna weryfikacja ich wykonania – w tym ich ewentualna integracja z innym oprogramowaniem oraz wydajność – będzie możliwa wyłącznie po ich całkowitym wykonaniu i przedstawieniu do Odbioru Wdrożenia. Jakikolwiek Odbiory poszczególnych Produktów lub Etapów nie wyłączają prawa Zamawiającego do weryfikacji całości Wdrożenia.”

47. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 7 ust. 10 pkt 5)

Treść pierwotnego zapisu:

„Zamawiający dokonuje odbioru poszczególnych prac Wykonawcy w następujący sposób:(...)

*5) W zakresie realizacji aplikacji mobilnej na systemy Android oraz iOS – **po wdrożeniu aplikacji do systemów dystrybucji** (App Store oraz Sklep Play oraz ich odpowiednikach/wersji w wprowadzone do terminu odbioru oraz otrzymaniu przez Zamawiającego dokumentów poświadczających wykonanie testów bezpieczeństwa.”*

Pytanie:

W związku z postanowieniem dotyczącym odbioru aplikacji mobilnej na systemy Android oraz iOS, prosimy o doprecyzowanie i potwierdzenie, czy przez „wdrożenie aplikacji do systemów dystrybucji (App Store oraz Sklep Play)” Zamawiający rozumie przygotowanie aplikacji zgodnie z wymaganiami technicznymi tych platform oraz jej przekazanie do procesu publikacji, a nie uzależnia odbioru od uzyskania finalnej akceptacji i publikacji przez operatorów tych sklepów, którzy pozostają podmiotami trzecimi niezależnymi od Wykonawcy.

Mając na uwadze powyższe, wnosimy o potwierdzenie, że odbiór aplikacji mobilnej nastąpi w momencie spełnienia przez Wykonawcę wymagań technicznych oraz przekazania aplikacji do publikacji w sklepach dystrybucyjnych, niezależnie od finalnej decyzji operatorów tych platform.

Odpowiedź:

Zamawiający nie wyraża zgody na zmianę zapisów Umowy w tym zakresie.

48. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 7 ust. 12-15

Treść pierwotnego zapisu:

„12. Po przedstawieniu przedmiotu odbioru do Odbioru, Zamawiający zweryfikuje przedmiot odbioru pod kątem jego zgodności z Umową, w tym zgodności ze Specyfikacją wymagań oraz ofertą Wykonawcy, w szczególności poprzez przeprowadzenie testów oraz analizę Dokumentacji dostarczonej przez Wykonawcę.

13. W razie stwierdzenia, w trakcie Odbioru przez Zamawiającego, wad lub usterek przedmiotu odbioru polegających na niezgodności z Umową, w tym Specyfikacją wymagań, Zamawiający powiadomi o nich Wykonawcę w formie pisemnej lub mailowej.

14. Wykonawca ma obowiązek bezzwłocznego, nie później jednak niż w terminie 5 dni roboczych, usunięcia zgłoszonych wad lub usterek i ponownego przedstawienia przedmiotu odbioru do Odbioru.

*15. Po pozytywnie zakończonych testach oraz stwierdzeniu zgodności z Umową danego przedmiotu odbioru, Zamawiający podpisze każdorazowo Protokół Odbioru. **W przypadku ponownego stwierdzenia wad lub innych niezgodności, procedurę opisaną w ust. 4-6 stosuje się odpowiednio.”***

Pytanie:

Wykonawca wnosi o zdefiniowanie pojęcia „wad lub usterek” oraz „niezgodności”, gdyż nie pojawiają się one w innym miejscu w umowie.

W odniesieniu do obowiązku usunięcia wad w terminie 5 dni roboczych, prosimy o potwierdzenie, czy Zamawiający dopuszcza zróżnicowanie terminów ich usuwania w zależności od charakteru i stopnia złożoności zgłoszonych niezgodności, w szczególności w przypadku wad wymagających bardziej złożonych prac analitycznych lub programistycznych.

Dodatkowo prosimy o potwierdzenie, czy Zamawiający przewiduje, aby w sytuacji braku zgłoszenia uwag przez Zamawiającego w określonym terminie od przedstawienia przedmiotu do odbioru (np. 10 dni kalendarzowych) możliwe było przyjęcie przez Strony mechanizmu tzw. milczącego odbioru, co pozwoli na zapewnienie ciągłości realizacji Umowy oraz rozliczeń pomiędzy Stronami w sytuacji braku podpisania protokołu odbioru przez Zamawiającego.

W związku z powyższym Wykonawca zwraca się z prośbą o potwierdzenie, że:

- 1) możliwe jest dokonanie odbioru z zastrzeżeniami w przypadku wad nieistotnych,
- 2) ponowna weryfikacja będzie ograniczona do uprzednio zgłoszonych niezgodności,
- 3) a odbiory częściowe mają charakter wiążący i nie podlegają ponownej ocenie, z wyjątkiem wad ukrytych.

Odpowiedź:

Zamawiający w definicjach wyczerpująco określił definicjami Awarii i Awarii Krytycznej w Umowie przedmiot zapytania. W kwestii usunięcia wad w terminie 5 dni roboczych Zamawiający nie dopuszcza różnicowania terminu w zależności od złożoności zgłoszonych niezgodności.

Zamawiający również nie dopuszcza stosowania mechanizmu milczącego odbioru, dlatego w zakresie punktów 1-3 Zamawiający nie potwierdza postawionych tez.

49. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 8 ust. 1 i 2

Pytanie:

Czy Zamawiający potwierdza, że ust. 1 i 2 miały być jedną jednostką redakcyjną?

Odpowiedź:

Zamawiający potwierdza, że §8 ust. 1 i 2 miały być jedną jednostką redakcyjną, dlatego nadaje nowe brzmienie §8 ust. 1 Załącznika nr 8 do SWZ:

*„1. Z dniem Odbioru Wdrożenia Systemu Informatycznego Wykonawca rozpocznie świadczenie Usług Utrzymania. Wykonawca odpowiada za działanie Systemu zgodnie z parametrami zdefiniowanymi w **Załączniku nr 3 do Umowy – SLA, Serwisowanie**”*

zaś §8 ust. 2 zostaje usunięty.

50. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 8 ust. 3

Treść pierwotnego zapisu:

*„Celem Usług Utrzymania jest zapewnienie poprawnego i nieprzerwanego działania Systemu Informatycznego oraz zapewnienie **świadczenia dodatkowych usług wspomagających korzystanie z Systemu przez Zamawiającego, a także dostosowanie systemu do aktualnych regulacji prawnych W ramach usługi Utrzymania Systemu świadczona jest również Asysta Techniczna.**”*

Pytanie:

Wnosimy o doprecyzowanie zakresu obowiązku „dostosowania systemu do aktualnych regulacji prawnych”, w szczególności poprzez wskazanie czy realizacja takich zmian będzie odbywała się w ramach wynagrodzenia za utrzymanie, czy też w trybie odrębnych zleceń.

Jednocześnie prosimy o doprecyzowanie, co Zamawiający rozumie przez „dodatkowe usługi wspomagające korzystanie z Systemu”, tak aby możliwe było jednoznaczne określenie obowiązków Wykonawcy i uniknięcie rozbieżności interpretacyjnych w trakcie realizacji Umowy.

Odpowiedź:

Pod zapisem „dostosowania systemu do aktualnych regulacji prawnych” Zamawiający rozumie, że Wykonawca dostosuje system za każdym razem, gdy zmiany w prawie lokalnym i krajowym będą wymuszać na Zamawiającym modyfikacje systemu w taki sposób, że nie będzie się dało zrealizować wymogów prawnym poprzez podstawową konfigurację. Każdorazowe dostosowywanie systemu w tym zakresie musi się odbywać w ramach usług utrzymania.

51. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 8 ust. 7

Treść pierwotnego zapisu:

„Wykonawca zobowiązuje się do świadczenia Usług Utrzymania w sposób zapobiegający utracie danych Zamawiającego, w tym także tych, do których będzie miał dostęp w trakcie wykonywania usług. W przypadku, gdy wykonanie danej czynności przez Wykonawcę wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed przystąpieniem do wykonania takiej czynności wymagane jest uzyskanie zgody Zamawiającego.”

Pytanie:

Prosimy o doprecyzowanie, jakie czynności Zamawiający uznaje za „wiązące się z ryzykiem utraty danych”, a także wskazanie czy Zamawiający rozumie przez to czynności niestandardowe lub czy dopuszcza ograniczenie tego obowiązku do operacji niestandardowych (np. migracja danych, operacje manualne) oraz czy odpowiedzialność Wykonawcy z tego tytułu obejmuje należyta staranność podmiotu profesjonalnego?

Dodatkowo czy Zamawiający w odniesieniu do procedury zgody na wykonanie przez Wykonawcę czynności wiążących się z ryzykiem utraty danych, wskaże:

- 1) w jakim terminie Zamawiający zobowiązuje się udzielić zgody na wykonanie czynności?
- 2) czy brak odpowiedzi Zamawiającego w określonym terminie może być traktowany jako zgoda Zamawiającego?
- 3) Czy w sytuacjach awaryjnych Wykonawca może podjąć działania bez uprzedniej zgody Zamawiającego?

Odpowiedź:

Zamawiający nie jest w stanie wskazać pełnego katalogu czynności, które Wykonawca może wykonać na danych w Systemie zainstalowanym w infrastrukturze Wykonawcy. Przykłady czynności to m.in. działania wykonywane bezpośrednio na bazie danych, w tym działania w poszczególnych widokach i tabelach, mogą być to m.in. czynności realizowane w celu usunięcia wad, awarii, usterek (również na podstawie zgłoszeń Zamawiającego), migracje, skrypty (przykład: scalanie danych, przenoszenie danych), czynności administracyjne, prace rozwojowe mające wpływ na zakres danych w Systemie itp.. Po stronie Wykonawcy jest określenie czy planowana do wykonania czynność może wiązać się z ryzykiem utraty danych w Systemie.

Zamawiający udzieli zgody (lub odrzuci wniosek) niezwłocznie po uzyskaniu wszelkich niezbędnych informacji od Wykonawcy do przeprowadzenia analizy ryzyka dla danego przypadku oraz po dokonaniu analizy ryzyka dla danego przypadku. W przypadku podjęcia działań przez Wykonawcę bez uprzedniej zgody Zamawiającego, po stronie Wykonawcy jest zabezpieczenie danych w taki sposób, aby w przypadku ich utraty było możliwe przywrócenie danych przy jednoczesnym braku utraty danych zgromadzonych w Systemie, w tym danych bieżących, wprowadzonych do Systemu w okresie od utraty danych do momentu wykrycia utraty danych.

Zamawiający zwraca uwagę, że Wykonawca powinien zapewnić poufność, integralność i dostępność danych w Systemie. Utrata danych może wiązać się np. z naruszeniem dostępności i skutkować naruszeniem ochrony danych osobowych.

Treść pierwotnego zapisu:

„W razie otrzymania przez Wykonawcę zgłoszenia lub w razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Awarii Niekrytycznej, Awarii Krytycznej, Podatności Niekrytycznej lub Podatności Krytycznej z innego źródła niż zgłoszenie Zamawiającego Wykonawca zobowiązany będzie do podjęcia działań zmierzających do jej usunięcia. Wykonawca jest zobowiązany do poinformowania Zamawiającego o podjęciu działań w Czasie Reakcji.“

Pytanie:

1. Prosimy o doprecyzowanie, od jakiego momentu liczony jest Czas Reakcji w przypadku uzyskania wiedzy o awarii z innego źródła niż zgłoszenie Zamawiającego.
2. Czy Zamawiający dopuszcza, aby Czas Reakcji liczony był wyłącznie od momentu rejestracji zgłoszenia w systemie HelpDesk?
3. Prosimy o doprecyzowanie, co w kontekście niniejszej umowy oznacza „uzyskanie wiedzy”, w szczególności prosimy o wskazanie czy obejmuje ono alerty systemowe oraz innego rodzaju monitoring automatyczny?
4. Czy obowiązek podjęcia działań dotyczy wyłącznie potwierdzonych awarii, a nie potencjalnych lub niezweryfikowanych zdarzeń?
5. Czy Zamawiający dopuszcza, aby działania Wykonawcy były podejmowane po wstępnej weryfikacji zdarzenia przez Wykonawcę?
6. Czy klasyfikacja awarii/podatności nadana przez Zamawiającego podlega weryfikacji przez Wykonawcę?
7. Czy możliwe jest wprowadzenie mechanizmu uzgadniania kategorii awarii/podatności?

Odpowiedź:

AD.1 Zamawiający będzie liczył Czas Reakcji od momentu przekazania Wykonawcy zgłoszenia w systemie Helpdesk lub powiadomienia Wykonawcy o Awarii lub Podatności poprzez pocztę elektroniczną. W przypadku poczty elektronicznej Zamawiający niezwłocznie zarejestruje i przekaże Wykonawcy zgłoszenie w systemie Helpdesk.

Zamawiający jako inne „źródła niż zgłoszenie Zamawiającego” rozumie źródła wskazane w projekcie umowy m.in. zgodnie z §8 ust. 11: *„Wykonawca zobowiązany jest do potwierdzenia przyjęcia zgłoszenia odpowiednim wpisem w HelpDesk (dotyczy to również **zgłoszeń składanych pocztą elektroniczną** lub telefonicznie - takie zgłoszenie wymaga odnotowania po stronie Zamawiającego w systemie HelpDesk). „*

AD.2 Zamawiający będzie liczył Czas Reakcji od momentu przekazania Wykonawcy zgłoszenia w systemie Helpdesk lub powiadomienia Wykonawcy przez Zamawiającego poprzez pocztę elektroniczną. W sytuacji powiadomienia Wykonawcy poprzez pocztę elektroniczną Zamawiający niezwłocznie dokona zgłoszenia poprzez Helpdesk.

AD.3 Zamawiający jako „uzyskanie wiedzy” rozumie przekazanie Wykonawcy zgłoszenia w systemie Helpdesk, powiadomienia Wykonawcy poprzez pocztę elektroniczną.

Zamawiający zwraca uwagę, że brak zgłoszenia w systemie Helpdesk lub pozyskania wiedzy od Zamawiającego poprzez pocztę elektroniczną nie zwalnia Wykonawcy z obowiązku zachowania parametrów dostępności Systemu.

Wykonawca może monitorować działanie systemu (dostępność Systemu) poprzez m.in. monitoring automatyczny.

AD.4 Tak, w przypadku Awarii i Podatności Wykonawca ma obowiązek podjąć działania w przypadku pozyskania wiedzy poprzez np. zgłoszenie otrzymane od Zamawiającego w systemie Helpdesk lub pocztę elektroniczną o wystąpieniu Awarii lub Podatności.

Zamawiający zwraca uwagę, że brak zgłoszenia w systemie Helpdesk lub pozyskania wiedzy od Zamawiającego poprzez pocztę elektroniczną nie zwalnia Wykonawcy z obowiązku zachowania parametrów dostępności Systemu.

Zamawiający zwraca uwagę na obowiązki zapewnienia przez Wykonawcę bezpieczeństwa pracy i udostępnienia Systemu Zamawiającemu spełniającego wymagania bezpieczeństwa informacji jak i ochrony danych osobowych.

Jednocześnie Zamawiający **zmienia treść §15 ust. 20 Załącznika nr 8 do SWZ - Projekt Umowy** poprzez wykreślenie dotychczasowej treści i zastępuje ją nową w brzmieniu:

„20. Zamawiający naliczy kary umowne za każdą rozpoczętą godzinę braku dostępności Systemu (dostępności usługi) w zakresie wskazanym w Umowie w wysokości 500 PLN za każdą rozpoczętą godzinę braku zapewnienia dostępności Systemu.”

AD.5 Wykonawca od momentu otrzymania zgłoszenia w systemie Helpdesk lub informacji od Zamawiającego do momentu rozwiązania zgłoszenia ma określony czas na rozwiązanie zgłoszenia (Awaria, Podatność, zlecenie). Czas usunięcia Awarii, Podatności, zlecenia został określony w Załączniku nr 3 do Umowy Warunki świadczenia usług Utrzymania w ust. 5. Wykonawca może w tym czasie dokonać m.in. „weryfikacji zdarzenia”.

AD.6 Wykonawca może wnosić do Zamawiającego prośbę o zmianę klasyfikacji Awarii lub Podatności, w szczególności gdy jest ona niezgodna z wymaganiami wskazanymi w umowie. Wykonawca musi uzasadnić konieczność zmiany klasyfikacji zgłoszenia. Ostateczna decyzja co do klasyfikacji zgłoszenia Awarii lub Podatności jest po stronie Zamawiającego.

AD.7 Wykonawca może wnosić do Zamawiającego prośbę o zmianę klasyfikacji Awarii lub Podatności, w szczególności gdy jest ona niezgodna z wymaganiami wskazanymi w umowie. Wykonawca musi uzasadnić

konieczność zmiany klasyfikacji zgłoszenia. Ostateczna decyzja co do klasyfikacji zgłoszenia Awarii lub Podatności jest po stronie Zamawiającego

53. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 8 ust. 12

Treść pierwotnego zapisu:

„Czas Naprawy uważa się za dochowany z chwilą zgłoszenia dokonania Naprawy, jeżeli Awaria Niekrytyczna, Awaria Krytyczna, Podatność Niekrytyczna lub Podatność Krytyczna lub została faktycznie usunięta. Jeżeli okaże się podczas weryfikacji usunięcia Awarii Niekrytycznej, Awarii Krytycznej, Podatności Niekrytycznej lub Podatności Krytycznej, Awaria Niekrytyczna, Awaria Krytyczna, Podatność Niekrytyczna lub Podatność Krytyczna nie została usunięta, Czas Naprawy jest dochowany dopiero z chwilą zgłoszenia poprawki faktycznie usuwającej tę Awarię Niekrytyczną, Awarię Krytyczną, Podatność Niekrytyczną lub Podatność Krytyczną.”

Pytanie:

1. Czy Zamawiający dopuszcza, aby Czas Naprawy był uznany za dochowany z chwilą zgłoszenia usunięcia awarii, chyba że Zamawiający zgłosi zastrzeżenia w określonym terminie?
2. Prosimy o wskazanie maksymalnego czasu na weryfikację naprawy przez Zamawiającego.
3. Czy ponowne zgłoszenie tej samej awarii po jej zamknięciu traktowane będzie jako nowe zgłoszenie?
4. Czy Zamawiający dopuszcza wprowadzenie mechanizmu ponownej klasyfikacji zgłoszenia po jego zamknięciu?
5. Czy czas weryfikacji naprawy przez Zamawiającego wstrzymuje bieg Czasu Naprawy?

Odpowiedź:

AD.1 Zamawiający uważa Czas Naprawy za dochowany z chwilą zgłoszenia dokonania Naprawy, jeżeli Awaria Niekrytyczna, Awaria Krytyczna, Podatność Niekrytyczna lub Podatność Krytyczna lub została faktycznie usunięta. Wykonawca ma prawo zamknąć (zakończyć) zgłoszenie Awarii lub Podatności lub wysłać powiadomienie do Zamawiającego o usunięciu Awarii lub Podatności. Obie sytuacje powodują zatrzymanie czasu na usunięcie Awarii lub Podatności. Jeśli okaże się po weryfikacji przez Zamawiającego, że awaria nie została usunięta, czas na usunięcie Awarii lub Podatności (Czas Naprawy) jest wznawiany i biegnie dalej od momentu otrzymania zgłoszenia do momentu faktycznego usunięcia Awarii lub Podatności z pominięciem czasu na weryfikację rozwiązania lub zainstalowanych poprawek przez Zamawiającego.

AD.2 W przypadku zmiany statusu zgłoszenia na Resolved Zamawiający ma 3 dni na weryfikację rozwiązania. Po tym czasie, jeśli żadna ze stron nie

podejście działań w danym zgłoszeniu w systemie Helpdesk, zgłoszenie przechodzi automatycznie w status Closed. W przypadku braku rozwiązania przedstawiciel Zamawiającego może zarejestrować nowe zgłoszenie Awarii lub Podatności lub zgłosić Reklamację. Czas usunięcia Reklamacji wskazano w załączniku nr 3 do Umowy.

AD.3 Tak, w przypadku gdy upłynął czas na weryfikację Awarii przez Zamawiającego (3 dni).

AD.4 Wykonawca może wnosić do Zamawiającego prośbę o zmianę klasyfikacji Awarii lub Podatności, w szczególności gdy jest ona niezgodna z wymaganiami wskazanymi w umowie. Wykonawca musi uzasadnić konieczność zmiany klasyfikacji zgłoszenia. Ostateczna decyzja co do klasyfikacji zgłoszenia Awarii lub Podatności jest po stronie Zamawiającego.

AD.5 Tak, czas weryfikacji naprawy przez Zamawiającego wstrzymuje bieg Czasu Naprawy.

54. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 14 ust. 15

Treść pierwotnego zapisu:

„Wykonawca będzie składał faktury VAT drogą elektroniczną na adres mailowy eof_cui@cui.wroclaw.pl, a w przypadku braku takiej możliwości osobiście w sekretariacie zamawiającego na IV piętrze. Szczegółowe zasady w tym wymagania techniczne określone zostały w Załączniku nr 5a do Umowy.”

Pytanie:

Czy Zamawiający potwierdza, że w przypadku wystawiania faktur ustrukturyzowanych niniejszego postanowienia się nie stosuje?

Odpowiedź:

Zamawiający potwierdza, że w przypadku wystawiania faktur ustrukturyzowanych niniejszego postanowienia się nie stosuje.

55. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 15 ust. 1

Treść pierwotnego zapisu:

*„Naliczenie zastrzeżonych Umową kar umownych **nie wyłącza możliwości dochodzenia odszkodowania na zasadach ogólnych do pełnej wysokości szkody poniesionej przez Zamawiającego w związku ze zdarzeniem, które było podstawą naliczenia danej kary.**”*

Pytanie:

Czy mając na uwadze treść dobrych praktyk stosowanych w zakresie realizacji umów IT, Zamawiający wprowadzi ograniczenie odpowiedzialności kontraktowej Wykonawcy, np. do kwoty 60% wartości przedmiotu Umowy netto oraz wyłączy odpowiedzialność Wykonawcy w zakresie utraconych korzyści?

Brak określenia limitu odpowiedzialności Wykonawcy odbiega od standardów stosowanych na rynku usług IT. Zgodnie z dokumentem „ANALIZA DOBRYCH PRAKTYK W ZAKRESIE REALIZACJI UMÓW IT, ZE SZCZEGÓLNYM UWZGLĘDNIENIEM SPECYFIKI PROJEKTÓW INFORMATYCZNYCH 7 OSI PRIORYTETOWEJ PO IG” (dalej Analiza), udostępnionej przez Urząd Zamówień Publicznych (link:

[https://www.uzp.gov.pl/__data/assets/pdf_file/0016/](https://www.uzp.gov.pl/__data/assets/pdf_file/0016/24244/Analiza_dobrych_praktyk_w_zakresie_realizacji_umow_IT.pdf)

[24244/Analiza_dobrych_praktyk_w_zakresie_realizacji_umow_IT.pdf](https://www.uzp.gov.pl/__data/assets/pdf_file/0016/24244/Analiza_dobrych_praktyk_w_zakresie_realizacji_umow_IT.pdf)):

„Standardem w umowach dotyczących systemów informatycznych jest ograniczenie odpowiedzialności kontraktowej stron do określonej wysokości określanej kwotowo lub do wartości umowy” (str. 54 ww. Analizy) oraz „(...) standardowo w umowach IT, odpowiedzialność stron jest ograniczana do szkody rzeczywistej. Jest to podyktowane potrzebą wyeliminowania sytuacji, w której strona będzie odpowiadała za trudne do skwantyfikowania utracone korzyści drugiej strony” (str. 55 Analizy).

Zapis uwzględniający powyższe standardy rynkowe mógłby mieć następujące brzmienie :„Z zastrzeżeniem postanowień umowy przewidujących dalej idące ograniczenia lub wyłączenia odpowiedzialności odszkodowawczej Wykonawcy i w zakresie, w jakim jest to dopuszczalne w świetle bezwzględnie obowiązujących przepisów prawnych wszelka i całkowita odpowiedzialność odszkodowawcza Wykonawcy względem Zamawiającego za niewykonanie lub nienależyte wykonanie Umowy obejmuje wyłącznie rzeczywistą stratę Zamawiającego, z wyłączeniem w całości utraconych korzyści Zamawiającego, a nadto ograniczona jest do kwoty wynoszącej 60% wartości przedmiotu Umowy netto, wskazanej w § 14 ust. 1.”

Odpowiedź:

Zamawiający nie wyraża zgody na zmianę w zapisach Umowy.

56. Pytanie do Zał. nr 8 do SWZ - Projekt Umowy - § 15

Treść pierwotnego zapisu:

Brak limitu dla poszczególnych kar umownych

Pytanie:

Wykonawca zwraca się z prośbą o wprowadzenie maksymalnego limitu kar umownych przewidzianych w umowie. W obecnym brzmieniu postanowienia nie przewidują ograniczenia wysokości kar, co w praktyce może prowadzić do nieograniczonej odpowiedzialności Wykonawcy.

Jednocześnie wskazujemy, że zgodnie z art. 436 pkt 3 ustawy Prawo zamówień publicznych, umowa w sprawie zamówienia publicznego powinna określać łączną maksymalną wysokość kar umownych, których mogą dochodzić strony. Brak ustanowienia limitu może budzić wątpliwości co do zgodności postanowień Umowy z obowiązującymi przepisami prawa.

W związku z powyższym Wykonawca wnosi o potwierdzenie, czy Zamawiający przewiduje uzupełnienie Umowy o zapis określający łączny limit kar umownych?

Odpowiedź:

Zamawiający **zmienia treść §15 ust. 1 Załącznika nr 8 do SWZ - Projekt Umowy** poprzez wykreślenie dotychczasowej treści i zastępuje ją nową w brzmieniu:

„Naliczenie zastrzeżonych Umową kar umownych nie wyłącza możliwości dochodzenia odszkodowania na zasadach ogólnych do pełnej wysokości szkody poniesionej przez Zamawiającego w związku ze zdarzeniem, które było podstawą naliczenia danej kary. Maksymalna wysokość kar umownych nie przekroczy kwoty całkowitego wynagrodzenia brutto.

A. Charakter zamówienia, obecny system Zamawiającego i wykonalność terminów

57. W związku z Rozdziałem 3 SWZ oraz § 2 i § 5 projektu umowy, czy Zamawiający potwierdza, że przedmiotem zamówienia ma być wdrożenie gotowego systemu już istniejącego po stronie Wykonawcy, a nie zaprojektowanie i wykonanie nowego systemu lub zasadnicza rozbudowa systemu obcego, skoro umowa posługuje się pojęciami „System udostępniony w modelu SaaS”, „wdrożenie”, „dostosowanie”, „Analiza Przedwdrożeniowa” i „Wersja Produkcyjna”, a nie przewiduje odrębnych etapów projektowania, developmentu i testów akceptacyjnych typowych dla budowy nowego oprogramowania?

Odpowiedź:

Nie, zamawiający nie oczekuje, że wykonawca dysponuje systemem zgodnym z wymaganiami Zamawiającego, ale dysponuje systemem który jest sprawdzony w innych wdrożeniach, jest elastyczny i konfigurowalny i przez to będzie możliwe jego wdrożenie u Zamawiającego w terminach wskazanych w zamówieniu tak by spełniał wymagania Zamawiającego.

58. Czy Zamawiający korzysta obecnie z działającego systemu rekrutacji i/lub dziennika elektronicznego, z którego mają zostać zmigrowane dane, a jeśli tak, to czy system ten stanowi bazę funkcjonalną, procesową i danych dla oczekiwanego wdrożenia, o którym mowa w § 2 ust. 1 pkt 7 projektu umowy?

Odpowiedź:

System obecnie używany przez Zamawiającego nie stanowi bazy funkcjonalnej, procesowej, natomiast baza danych będzie pochodzić z obecnie używanego systemu.

59. Jeżeli Zamawiający korzysta z obecnego systemu, czy Wykonawca wyłoniony w postępowaniu otrzyma po zawarciu umowy:
- dostęp analityczny i techniczny do obecnego systemu,
 - dostęp do dokumentacji technicznej, integracyjnej i bazodanowej,
 - dostęp do pełnego modelu danych,
 - listę aktywnych interfejsów i zależności,
 - dostęp do środowiska testowego obecnego systemu?

Prosimy o jednoznaczne potwierdzenie zakresu tych dostępów oraz terminu ich przekazania. Obecne zapisy preferują obecnego dostawcę rozwiązania, dla którego znana jest architektura systemu, co automatycznie preferuje jednego Wykonawcę zamówienia.

Odpowiedź:

Odpowiadając na punkty a) do e) nie, Zamawiający nie jest właścicielem używanego obecnie oprogramowania i nie może zagwarantować przekazania do wskazanych w pytaniu zagadnień.

60. Czy Zamawiający posiada majątkowe prawa autorskie lub odpowiednie uprawnienia umowne do obecnie wykorzystywanego systemu w zakresie pozwalającym na przekazanie nowemu Wykonawcy kodów źródłowych, dokumentacji technicznej, struktur baz danych, definicji interfejsów i komponentów integracyjnych?

Odpowiedź:

Nie.

61. Jeżeli odpowiedź na pytanie poprzednie jest twierdząca, czy Zamawiający prześle po zawarciu umowy:
- kody źródłowe obecnego systemu,
 - repozytoria,
 - skrypty wdrożeniowe,
 - pliki konfiguracyjne,
 - dokumentację CI/CD,
 - instrukcje budowania i publikacji aplikacji mobilnej?

Jeżeli nie, prosimy o wskazanie, w jaki sposób Wykonawca ma realnie wykonać przedmiot zamówienia w terminach określonych w § 3 ust. 2 projektu umowy.

Odpowiedź:

Zamawiający nie jest właścicielem oprogramowania, dlatego nie jest w stanie przekazać wskazanych wymienionych pozycji i w żadnym elemencie zamówienia nie wskazywał, iż system ma być wdrożony na podstawie posiadanego rozwiązania.

62. Jeżeli Zamawiający nie prześle kodów źródłowych i zaplecza technicznego obecnego rozwiązania, to czy Zamawiający potwierdza, że w praktyce oczekuje dostarczenia innego, już gotowego produktu Wykonawcy, który będzie jedynie konfigurowany i integrowany z procesami Zamawiającego, a nie budowany od podstaw?

Odpowiedź:

Nie, Zamawiający nie określa nigdzie, że oczekuje dostarczenia gotowego produktu lub zbudowanego od podstaw. Zamawiający oczekuje dostarczenia systemu zgodnego z wymaganiami opisanymi w załącznikach oraz funkcjonującego prawidłowo do terminów określonych w Umowie.

63. Czy Zamawiający dostrzega, że terminy: 19 dni roboczych na analizę, 30 dni roboczych na wdrożenie wersji testowej, 15 dni roboczych na wersję produkcyjną, 5 dni roboczych na migrację danych oraz 15 dni roboczych na przeszkolenie 450 operatorów nie pozwalają na:
- a) napisanie nowego systemu,
 - b) dopisanie tak szerokiego zakresu do obcego systemu bez dostępu do kodów,
 - c) przejście pełnego cyklu analityczno-projektowo-deweloperskiego,
 - d) wykonanie integracji zależnych od podmiotów trzecich?

Odpowiedź:

W nawiązaniu do odpowiedzi na pytania numer 57 Zamawiający nie zmienia powyższych terminów, które uznaje za możliwe do dotrzymania przez wykonawców.

64. Czy w związku z powyższym Zamawiający zgodzi się na zmianę harmonogramu w ten sposób, aby:
- a) etap wdrożeniowy i integracyjny zakończył się po zakończeniu okresu obecnej rekrutacji,
 - b) wersja produkcyjna przedmiotowego systemu rekrutacji była dostępna od 2027 r.,
 - c) rozwój nowych funkcjonalności dziennika elektronicznego i integracji następował etapowo?

Prosimy o odpowiedź wraz z uzasadnieniem, dlaczego obecny harmonogram miałby być realny. Dlaczego premiuje obecnego dostawcę rozwiązania?

Odpowiedź:

Zamawiający nie wyraża zgody biorąc pod uwagę treść odpowiedzi na pytania numer 57 i 63.

65. Czy Zamawiający potwierdza, że zgodnie z harmonogramem rekrutacji na rok 2026/2027 system jest wykorzystywany od maja 2026 r., w tym dla udostępnienia systemu rodzicom od 15 maja 2026 r., a zatem wdrażanie

nowego rozwiązania w tym samym czasie zwiększa ryzyko dla ciągłości naboru?

Odpowiedź:

Czas przewidziany na wdrożenie przedmiotu zamówienia nie stanowi ryzyka w obecnie prowadzonych harmonogramach rekrutacji i Zamawiający nie zgadza się, że wdrażanie nowego rozwiązania zwiększa ryzyko dla ciągłości naboru.

66. Czy w związku z przebiegiem rekrutacji w maju i czerwcu 2026 r. Zamawiający dopuści model przejściowy polegający na:
- a) utrzymaniu obecnego narzędzia dla naboru 2026/2027,
 - b) przygotowaniu i wdrożeniu docelowego systemu na spokojnie po zakończeniu krytycznych etapów naboru,
 - c) uruchomieniu produkcyjnym przedmiotowego rozwiązania w 2027 r.?

Odpowiedź:

Zamawiający nie wyraża zgody na zastosowanie modelu przejściowego i podtrzymuje obecne zapisy.

B. Dziennik elektroniczny jako system odrębny, zintegrowany

67. W związku z definicją „Praca bieżąca/dziennik elektroniczny” oraz licznymi wymaganiami SWS dotyczącymi pracy bieżącej, czy Zamawiający dopuści, aby **dziennik elektroniczny stanowił odrębny system**, zintegrowany z systemem rekrutacji za pomocą API, mechanizmów wymiany danych lub eksportu/importu, zamiast stanowić jedną aplikację monolityczną?

Odpowiedź:

Zamawiający nie dopuści rozwiązania, aby dziennik elektroniczny stanowił odrębny system. Całość ma stanowić jedną aplikację monolityczną.

68. Czy Zamawiający potwierdza, że główny nabór ma charakter okresowy i skoncentrowany w określonych ramach czasowych, natomiast dalsza obsługa dzieci w placówkach ma charakter eksploatacyjny i ciągły, przez co nie istnieje obiektywna konieczność techniczna ani organizacyjna, aby rekrutacja i dziennik elektroniczny były dostarczone jako jeden nierozdzielny system?

Odpowiedź:

Proces rekrutacyjny ma charakter ciągły (nie kończy się) z częścią rekrutacji terminowej. System musi być spójny (jednorodny) i umożliwiać pracę na każdym z etapów. Operatorzy pracują jednocześnie na różnych etapach rekrutacji ale też wykonują bieżącą opiekę. Dlatego Zamawiający zaznacza, że system musi charakteryzować się ciągłością dostępnych funkcjonalności, a nie tylko ich okresowością.

69. Czy Zamawiający dopuści rozwiązanie, w którym:
- a) system rekrutacji odpowiada za składanie wniosków, kwalifikację, listy i decyzje;
 - b) dziennik elektroniczny odpowiada za obsługę dzieci przyjętych, obecności, rozliczenia;
 - c) między systemami funkcjonuje automatyczna wymiana danych o przyjęciach, zmianach statusów, grupach i zakończeniu opieki?

Odpowiedź:

Zamawiający nie dopuszcza takiego rozwiązania.

70. Czy Zamawiający potwierdza, że skoro sam wymaga i dopuszcza wymianę danych przez API z innymi systemami, to brak dopuszczenia dwóch zintegrowanych systemów w miejsce jednego rozwiązania ogranicza konkurencję bez należytego uzasadnienia? WO.15 wprost przewiduje API do Open Data.

Odpowiedź:

Wymagalność integracji z portalem Open Data przez API dotyczy przekazywania wąskiego fragmentu danych w celu realizacji polityki Otwartych Danych przez gminę Wrocław, zatem Zamawiający nie widzi w tym korelacji, która miałaby dopuszczać rozwiązanie dwusystemowe.

71. Czy Zamawiający zgodzi się na zmianę SWZ i Załącznika nr 1 w taki sposób, aby za zgodne z wymaganiami uznać rozwiązanie dwusystemowe: „system rekrutacji + odrębny dziennik elektroniczny”, połączone stabilnym interfejsem wymiany danych?

Odpowiedź:

Zamawiający nie wyraża zgody i podtrzymuje obecne zapisy.

72. Czy Zamawiający potwierdza, że dla rekrutacji ciągłej wystarczające jest przekazanie danych dziecka, statusu przyjęcia, grupy, dat umowy i historii zmian z systemu rekrutacyjnego do dziennika elektronicznego, bez konieczności utrzymywania obu procesów w jednym silniku aplikacyjnym?

Odpowiedź:

Zamawiający nie potwierdza. Nie jest to wystarczające.

C. Integracje i zależności od zewnętrznych API

73. W odniesieniu do WO.13–WO.15 prosimy o szczegółowe wskazanie wszystkich interfejsów zewnętrznych, które muszą zostać uruchomione w ramach zamówienia, wraz z informacją:

- a) czy API już istnieje,
- b) kto jest właścicielem API,
- c) jaki jest zakres danych,
- d) czy istnieją środowiska testowe,
- e) czy istnieją limity wywołań,
- f) jakie są SLA po stronie systemów zewnętrznych.

Odpowiedź:

Zamawiający w WO.13-15 wymaga wykorzystania następujących interfejsów zewnętrznych API:

- <https://api.open-data.cui.wroclaw.pl/> (właścicielem jest CUI Wrocław)
- <https://www.gov.pl/web/cyfryzacja/wezel-krajowy---dokumentacja-dotyczaca-integracji-z-wezlem-krajowym>

74. Dla integracji z Węzłem Krajowym prosimy o wskazanie:

- a) czy Zamawiający posiada już aktywne przyłączenie,
- b) czy istnieje już środowisko testowe,
- c) czy Zamawiający posiada wymagane identyfikatory, certyfikaty i profile usług,
- d) kto po stronie Zamawiającego odpowiada za formalności,
- e) czy Zamawiający uwzględnił kolejki i terminy po stronie administracji publicznej.

WO.14 nakazuje ująć tę integrację w harmonogramie, ale sam opis nie daje wykonawcy żadnych gwarancji terminowych po stronie podmiotów trzecich.

Odpowiedź:

Zamawiający używa obecnie system, który posiada aktywne przyłączenie do Węzła Krajowego, lecz jest to system nie znajdujący się na zasobach Zamawiającego. Dlatego należy przyjąć założenie, że wdrażany System będzie musiał przejść nową procedurę integracyjną z Węzłem Krajowym. Za formalności po stronie Zamawiającego odpowiada wyznaczona osoba do realizacji umowy we wsparciu odpowiednich pracowników Zamawiającego. Osoba ta ma bardzo duże doświadczenie w wielu innych projektach. W przypadku kolejek i terminów po stronie administracji publicznej zastosowanie znajdzie par. 10 ust.2 pkt a tiret trzecie Umowy.

75. Czy w przypadku Węzła Krajowego Zamawiający zgodzi się na uruchomienie początkowe logowania alternatywnego, a pełnej integracji z Węzłem po uzyskaniu gotowości po stronie administracji i testów integracyjnych?

Odpowiedź:

Nie

76. W odniesieniu do WO.15 prosimy o wskazanie dokładnego zakresu danych przekazywanych do Open Data Wrocław:

- a) jakie zbiory,
- b) jakie pola,
- c) z jaką częstotliwością,
- d) czy mają to być dane zagregowane czy rekordowe,
- e) które dane mogą zawierać elementy pośrednio identyfikujące osoby?

Odpowiedź:

a) Zbiorami eksportowanymi na portal OpenData będą: ilość aktywnych żłobków w ujęciu rocznym oraz ilość przyjętych podopiecznych w danym roku,

b) Pola adekwatne do uzyskania rezultatu z pkt a),

c) Częstotliwość raz na miesiąc kalendarzowy,

d) Dane mają mieć charakter zagregowanego pliku wskazującego na wyniki z miesiąca na miesiąc w okresie rocznym,

e) Dane w żaden sposób nie mogą pozwolić na identyfikacje osób, mają być prezentowane w wartościach liczbowych.

77. Czy Zamawiający potwierdza, że przekazywanie „dowolnych danych opublikowanych i skatalogowanych w Systemie” przez API jest sformułowaniem zbyt szerokim i niepozwalającym na rzetelną wycenę, wobec czego powinien opublikować zamknięty katalog zasobów podlegających integracji?

Odpowiedź:

Zamawiający oczekuje, że system będzie posiadał techniczną możliwość rozszerzania zakresu danych udostępnianych przez API. Celem takiego rozwiązania jest zapewnienie w przyszłości odpowiedniej możliwości integracji systemu wobec potencjalnych zmian wynikających z regulacji prawnych. Zamawiający nie wyklucza, że rozszerzanie zakresu udostępnianych danych będzie realizował poprzez usługę rozwoju, ale na ten moment nie jest w stanie określić, które zasoby będą musiały być udostępnione przez API w zamówieniu podstawowym. Na etapie Analizy Przedwdrożeniowej zostaną ustalone ramy wymaganych zasobów do udostępnienia w zamówieniu podstawowym.

78. Prosimy o opublikowanie pełnej dokumentacji wszystkich API, do których ma integrować się system, a nie jedynie odesłania do analizy powdrożeniowej lub zewnętrznych serwisów.

Odpowiedź:

Zamawiający dysponuje następującą dokumentacją:

- <https://api.open-data.cui.wroclaw.pl/>
- <https://www.gov.pl/web/cyfryzacja/wezel-krajowy---dokumentacja-dotyczaca-integracji-z-wezlem-krajowym>

79. Jeżeli pojawia się odwołanie do systemu CST w dokumentacji administratora, prosimy o wyjaśnienie, czy system CST rzeczywiście jest objęty zakresem tego zamówienia, czy też zapis ten stanowi omyłkę edycyjną pochodzącą z innego projektu. Załącznik dot. dokumentacji zawiera taki zapis w pkt 2.2.7–2.2.8.

Odpowiedź:

System CST nie jest objęty zakresem zamówienia, a zapis stanowi omyłkę pisarską. W związku z tym **Zamawiający wprowadza zmianę treści SWZ** w Załączniku nr 2 do Umowy – Dokumentacja poprzez wykreślenie całej treści w rozdz. 2.2 pkt. 2.2.7 i 2.2.8.

Jednocześnie w treści Zamawiający poprawia omyłkę pisarską w nazwie ww. Załącznika na „*Załącznik nr 2 do Umowy nr CUI*”

D. Raporty, eksporty i zakres danych

80. W odniesieniu do WT.14, SWS.75 oraz Załącznika nr 2 do umowy prosimy o opublikowanie kompletnej listy raportów wymaganych przez Zamawiającego, gdyż obecnie:
- a) WT.14 wymaga eksportu wszystkich raportów do licznych formatów,
 - b) SWS.75 odsyła do „załącznika do dokumentacji”,
 - c) szczegółowy zakres raportów ma być dopiero przekazany w analizie.
- Taki opis nie pozwala na porównywalną wycenę ofert.

Odpowiedź:

Zamawiający nie jest w stanie na tym etapie opublikować kompletnej listy raportów, natomiast poniżej prezentuje listę stanowiącą podstawę do prac w trakcie Analizy Przedwdrożeniowej.

Liczba dzieci oczekujących
Liczba dzieci wstępnie przyjętych
Liczba dzieci oczekujących wg preferencji
Liczba dzieci oczekujących wg roku urodzenia
Liczba dzieci oczekujących wg grupy wiekowej
Liczba wniosków z I preferencji wg grupy wiekowej
Liczba dzieci oczekujących z podziałem wg danych o szczepieniach

Liczba dzieci oczekujących wg sytuacji rodziców
Liczba wniosków dzieci niepełnosprawnych oraz wymagających
szczególnej opieki
Aktualny stan przydziału
Lista placówek - dane teleadresowe
Liczba wolnych miejsc w placówkach
Podsumowanie wyników rekrutacji
Statystyka zgłoszeń
Podsumowanie czasu oczekiwania na przyjęcie

Globalna lista dzieci aktualnie uczęszczających do żłobków
Globalna lista dzieci aktualnie uczęszczających ze szczegółowymi
danymi
Lista dzieci uczęszczających do placówek
Informacje o dziecku w pracy bieżącej
Globalna lista dzieci niepełnosprawnych oraz wymagających
szczególnej opieki
Globalna lista dzieci usuniętych
Dane po rekrutacji

Analiza liczebności oddziałów i dzieci w placówkach
Liczba dzieci uczęszczających do żłobków
Liczba dzieci uczęszczających do żłobków wg danych o szczepieniach
Liczba dzieci niepełnosprawnych oraz wymagających szczególnej
opieki
Liczba dzieci aktualnie uczęszczających do placówek z informacją o
niepełnosprawności
Liczba dzieci uczęszczających do placówek z informacją o
niepełnosprawności

81. Prosimy o wskazanie dla każdego raportu:
- a) nazwy raportu,
 - b) celu,
 - c) odbiorcy,
 - d) wszystkich kolumn,
 - e) filtrów,
 - f) sortowań,
 - g) zakresu danych historycznych,
 - h) formatu wyjściowego obowiązkowego i opcjonalnego.

Odpowiedź:

Zamawiający nie jest w stanie na tym etapie określić żądanych parametrów jako zbiór zamknięty. W pytaniu nr 80 przedstawił otwartą listę oczekiwanych raportów. W odpowiedzi na niniejsze pytanie Zamawiający dołącza „Raporty - przykłady i charakterystyka” jako Załącznik nr 1 do Załącznika nr 1 do Umowy – specyfikacja wymagań

82. Czy Zamawiający potwierdza, że żądanie eksportu wszystkich raportów do PDF, XLS, XLSX, CSV, XML, DOC, DOCX i TXT jest nadmierowe, nieuzasadnione funkcjonalnie i niebezpieczne z punktu widzenia bezpieczeństwa danych, a nadto niepozwalające na racjonalną ocenę zakresu, skoro nie wskazano nawet listy raportów?

Odpowiedź:

Zamawiający zgadza się na wycofanie wymagania formatu TXT i dokonuje zmiany treści SWZ w Załączniku nr 1 do projektu umowy poprzez wykreślenie dotychczasowej treści wymagania WT.14 i nadaje mu nowe brzmienie :

„Wszystkie raporty (zestawienia) generowane w Systemie muszą mieć możliwość eksportu na ekran, do plików: PDF, xls, xlsx, csv, xml, doc, docx - z prawidłowym formatowaniem i układem strony aby raport mieścił się na stronie o ile jest to możliwe i raport nie zawiera dużej ilości kolumn, MS Excel oraz niezbędne dla użytkownika w MS Word (szablony), które zostaną doprecyzowane w Analizie i Analizie Przedwdrożeniowej”

83. Czy Zamawiający usunie z WT.14 wymóg eksportu do formatu TXT lub wskaże, dla których konkretnych raportów jest on wymagany i z jakiego uzasadnionego powodu biznesowego?

Odpowiedź:

Zamawiający zgadza się usunąć wymóg i dokonał przedmiotowej zmiany ujętej w odpowiedzi na pytanie numer 82.

84. W odniesieniu do § 2 ust. 2 pkt 4 projektu umowy oraz WO.12 prosimy o wskazanie szczegółowego zakresu danych podlegających przekazaniu po zakończeniu współpracy lub w ramach opcji:

- a) które tabele,
- b) które pliki,
- c) które dokumenty,
- d) które metadane,
- e) które logi,
- f) w jakim formacie,
- g) z jakim słownikiem pól,
- h) z jaką dokumentacją struktury danych.

Odpowiedź:

Zamawiający nie zna architektury wszystkich systemów dostępnych na rynku, więc nie jest w stanie opisać wymaganych elementów. Dane o których mowa w Umowie mają pozwolić na ewentualne kontynuowanie procesów nabór i rozliczania w nowym systemie, gdyby okazało się konieczne jego wdrożenie.

85. Czy Zamawiający potwierdza, że sformułowanie „całość danych zawartych w Systemie (dokumenty, transakcje, wyliczenia itp.)” wymaga doprecyzowania poprzez opublikowanie minimalnego zakresu danych eksportowych oraz specyfikacji technicznej eksportu? WO.12 pozostawia to do analizy, co uniemożliwia porównywalność ofert.

Odpowiedź:

Zamawiający określił swoje oczekiwania odpowiadając na pytanie numer 84.

86. Prosimy o wskazanie, czy Zamawiający wymaga eksportu jednorazowego, cyklicznego, czy on-demand oraz, czy ma on obejmować pełny eksport, eksport przyrostowy, czy oba mechanizmy.

Odpowiedź:

Eksport danych jest wymagany po zakończeniu współpracy w ramach Umowy, dlatego Zamawiający wymaga rozwiązania on-demand.

87. Prosimy o wskazanie, czy raporty i eksporty mają obejmować również logi bezpieczeństwa, historię zmian użytkowników, historię uprawnień i zdarzeń RODO, skoro dokumentacja administratora wymaga tak rozbudowanego opisu logów i audytu.

Odpowiedź:

Zamawiający potwierdza, że raporty i eksporty mają obejmować logi bezpieczeństwa, historię zmian użytkowników, historię uprawnień i zdarzeń RODO.

E. Bezpieczeństwo, szyfrowanie, klucze, logi

88. W odniesieniu do WO.19, WTAB.20–WTAB.28 i dokumentacji administratora prosimy o wskazanie, które wymagania bezpieczeństwa są obowiązkowe na dzień odbioru, a które mają charakter opcjonalny, ponieważ obecnie część kluczowych wymagań szyfrowania baz i zarządzania kluczami jest oznaczona jako „Opcja”, mimo że opis podstawowy wymaga rozbudowanych zabezpieczeń i zgodności z KRI oraz ustawą o dostępności.

Odpowiedź:

Wszystkie wymagania objęte opisem Wymagalność: „Musi być” są obowiązkowe na dzień odbioru. Wymaganie objęte opisem Wymagalność: „Powinno być” stanowią obowiązkowe na dzień odbioru, jeżeli Wykonawca zadeklarował ich wykonanie, za co przyznawane są dodatkowe punkty w kryterium oceny ofert. Wymaganie objęte opisem Wymagalność: „Opcja” stanowią dodatkowe aspekty, które Zamawiający może zlecić do wykonania

w ramach prawa opcji i wtedy należy je wdrożyć w przewidzianym w Umowie terminie.

89. Czy Zamawiający potwierdza, że WTAB.21, WTAB.22 i WTAB.22a są opcjami, a nie wymaganiami obligatoryjnymi, a jeśli tak, to jak należy rozumieć podstawowy minimalny poziom szyfrowania danych w spoczynku i w transferze?

Odpowiedź:

Zamawiający potwierdza, że wymagania WTAB.21, WTAB.22 i WTAB.22a są opcjami, a nie wymaganiami obligatoryjnymi. Rozwiązanie musi być zgodne z zapisami opisanymi jako „Musi być”. Zamawiający zastrzega sobie, że zamówienie określone jako „prawo opcji” jest uprawnieniem a nie zobowiązaniem zamawiającego. Wykonanie przedmiotu zamówienia w ramach prawa opcji uzależnione jest od faktycznych potrzeb zamawiającego i jego możliwości finansowych. Brak wykonania przedmiotu zamówienia w zakresie prawa opcji nie rodzi żadnych roszczeń ze strony Wykonawcy.

90. Czy Zamawiający wymaga, aby Wykonawca zapewnił szyfrowanie danych w spoczynku dla wszystkich danych osobowych, czy tylko dla wybranych kategorii? Prosimy o wskazanie kategorii danych.

Odpowiedź:

W zamówieniu podstawowym Zamawiający nie wymaga, aby Wykonawca zapewnił szyfrowanie danych w spoczynku dla wszystkich danych osobowych. Dopiero w przypadku uruchomienia Opcji i jej wdrożenia taki wymóg będzie miał miejsce.

91. W zakresie WTAB.22 prosimy o wyjaśnienie, jak należy rozumieć wymóg, aby „zarządzanie kluczami szyfrującymi było dostępne zarówno dla Wykonawcy systemu, jak i zamawiającego”, skoro jednocześnie Zamawiający obliguje Wykonawcę do pełnego zarządzania kluczami. Czy chodzi o:

- a) wgląd,
- b) raportowanie,
- c) współzarządzanie,
- d) depozyt,
- e) escrow,
- f) możliwość samodzielnego użycia przez Zamawiającego?

Odpowiedź:

Wymóg należy rozumieć jako współzarządzanie (c) oraz możliwość samodzielnego użycia (f). Wykonawca realizuje pełne zarządzanie operacyjne, jednak Zamawiający musi posiadać stały i nadrzędny dostęp do kluczy, aby na własne żądanie móc kontrolować dostęp do danych lub

samodzielnie je odczytać w dowolnym momencie trwania umowy oraz po jej zakończeniu.

92. W odniesieniu do WTAB.28 prosimy o potwierdzenie, czy tunel VPN IPsec jest obowiązkowy dla wszystkich połączeń między środowiskami i systemami, czy tylko dla wybranych integracji. Prosimy o wskazanie tych integracji.

Odpowiedź:

Tunel VPN IPsec jest obowiązkowy dla wszystkich połączeń realizowanych bezpośrednio do sieci Wykonawcy (styk sieciowy). Wymóg ten dotyczy dostępu do serwerów oraz urządzeń i ma na celu wyeliminowanie ich wystawiania na publiczne adresy IP. Standard ten nie dotyczy standardowej komunikacji aplikacyjnej (np. poprzez protokół TLS), a jedynie bezpośredniej łączności między środowiskami na poziomie sieciowym

93. W odniesieniu do WT.01, WTAB.29–WTAB.37 oraz dokumentacji administratora prosimy o wskazanie zamkniętego katalogu logowanych zdarzeń, gdyż obecnie istotna część zakresu logów ma być dopiero ustalona w analizie, co uniemożliwia wycenę i ocenę zgodności.

Odpowiedź:

Zamawiający nie wskazuje zamkniętego katalogu logów, ponieważ ich ostateczny zakres zostanie ustalony podczas analizy i wymaga zatwierdzenia przez Klienta. Z punktu widzenia Zespołu Bezpieczeństwa Informacji i Cyberbezpieczeństwa CUI kluczowe są logi bezpieczeństwa, które Wykonawca musi uwzględnić w wycenie jako wymóg obligatoryjny:

- **Zarządzanie dostępem i uprawnieniami:** logowania (udane/błędne), blokady kont, zmiany ról, nadawanie uprawnień oraz operacje na kontach uprzywilejowanych.

- **Operacje na danych:** odczyt, modyfikacja i usunięcie rekordów (szczególnie danych osobowych i wrażliwych).

- **Administracja i sieć:** zmiany konfiguracji, restarty usług, operacje na kluczach szyfrujących, zmiany parametrów bezpieczeństwa oraz rejestracja połączeń administracyjnych i wywołań API.

94. Prosimy o wskazanie dla logów:

- a) okresu retencji,
- b) sposobu anonimizacji,
- c) sposobu eksportu,
- d) minimalnych pól,
- e) wymaganych filtrów,
- f) wymaganych raportów,
- g) podziału na logi aplikacyjne, administracyjne, bezpieczeństwa i danych osobowych.

Odpowiedź:

Zamawiający nie wskazuje zamkniętego katalogu parametrów logów, ponieważ ich ostateczny zakres zostanie ustalony podczas analizy i wymaga zatwierdzenia przez Klienta.

95. Czy Zamawiający wymaga testów penetracyjnych:

- a) po stronie Wykonawcy,
- b) przez niezależny podmiot trzeci,
- c) dla web, mobile i API,
- d) w jakich terminach i z jakim zakresem?

Załącznik nr 2 do umowy wymaga opisu częstotliwości i zakresu testów penetracyjnych, ale nie określa minimum odbiorowego.

Odpowiedź:

Wykonawca ma obowiązek spełnić wymagania przedstawiającego przez Zamawiającego w dowolny sposób wybrany przez siebie tak, by dotrzymać terminów zawartych w Umowie. Dotrzymaniu terminów może pomóc oczekiwanie Zamawiającego wskazane w odpowiedzi na pytanie numer 57.

96. Czy Zamawiający opublikuje wymagania bezpieczeństwa w formie checklisty odbiorowej, aby uniknąć sytuacji, w której zakres zabezpieczeń będzie dopiero doprecyzowany po wyborze Wykonawcy?

Odpowiedź:

Zamawiający podtrzymuje przedstawione wymagania bezpieczeństwa, które Wykonawca jest zobowiązany bezwzględnie spełnić w ramach oferowanej ceny. Proces odbioru systemu będzie składał się z audytu bezpieczeństwa, weryfikacji konfiguracji podczas wideokonferencji potwierdzającej realizację poszczególnych wymogów oraz formalnego oświadczenia Wykonawcy o pełnej zgodności wdrożonych rozwiązań. Szczegółowy scenariusz odbiorowy oraz precyzyjne kryteria akceptacji zostaną określone po zakończeniu analizy przedwdrożeniowej, co jest standardowym etapem doprecyzowania technicznych dowodów spełnienia wymagań określonych w dokumentacji zamówienia Dokumentacja.

97. Czy Zamawiający potwierdza, że zakres dokumentacji z Załącznika nr 2 obejmuje nie tylko dokumentację użytkownika, ale de facto pełną dokumentację architektoniczną, bezpieczeństwa, bazodanową, integracyjną, licencyjną, procedury eksploatacyjne i RODO, co odpowiada realizacji rozbudowanego projektu wdrożeniowo-deweloperskiego?

Odpowiedź:

Zamawiający podtrzymuje aktualne zapisy

98. Czy Zamawiający udostępni wzór lub minimalny spis treści dokumentacji, aby ujednolicić oferty i uniknąć sytuacji, w której różni Wykonawcy przyjmą skrajnie odmienne pracochłonności?

Odpowiedź:

Zamawiający nie udostępni wzoru lub minimalnego spisu treści dokumentacji.

99. Czy Zamawiający potwierdza, że wymóg dokumentowania środowiska deweloperskiego z Załącznika nr 2 pkt 1 lit. e oznacza obowiązek utrzymywania dedykowanego środowiska deweloperskiego dla Zamawiającego, czy jedynie obowiązek opisowy?

Odpowiedź:

Zamawiający nie potwierdza.

100. Czy w zakresie dokumentacji administratora Zamawiający wymaga rzeczywistego diagramu wdrożenia z portami, protokołami i wszystkimi punktami styku, także z systemami zewnętrznymi, na dzień odbioru? Jeżeli tak, to prosimy o potwierdzenie, że bez przekazania przez Zamawiającego pełnej informacji o obecnym systemie i wymaganych integracjach wykonanie tego obowiązku nie jest możliwe.

Odpowiedź:

Zamawiający wymaga rzeczywistego diagramu wdrożenia z portami, protokołami i wszystkimi punktami styku, także z systemami zewnętrznymi na dzień odbioru. Zamawiający nie przekaże pełnej informacji o obecnym systemie, gdyż nie jest właścicielem systemu, a jedynie użytkownikiem na bazie licencji.

101. Czy Zamawiający zgodzi się ograniczyć zakres dokumentacji powykonawczej do dokumentacji niezbędnej dla eksploatacji rozwiązania SaaS, bez nakładania obowiązków typowych dla zamawiającego będącego właścicielem pełnej platformy i kodów źródłowych?

Odpowiedź:

Zamawiający zgodzi się ograniczyć zakres dokumentacji powykonawczej, jeżeli zostanie to doszczegółowione i zaakceptowane w trakcie Analizy Przedwdrożeniowej.

F. Szkolenia

102. W odniesieniu do Załącznika nr 6 prosimy o wskazanie minimalnej liczby godzin szkoleniowych dla:

a) Administratorów Głównych,

- a) Operatorów,
- b) administratorów bezpieczeństwa,
- c) użytkowników dziennika elektronicznego,

skoro obecnie wymóg odwołuje się do rezultatu („mają potrafić obsługiwać system”), a nie do mierzalnego wolumenu szkolenia.

Odpowiedź:

Zamawiający wskazuje następującą liczbę godzin szkoleniowych, którą trzeba przeznaczyć na poszczególne rodzaje grup szkoleniowych:

- a) dla grupy Administratorów Głównych 15h na grupę.
- b) Operatorów: od 2h do 4h na grupę.

dla pozycji administrator bezpieczeństwa oraz użytkownik dziennika elektronicznego nie przewiduje się szkoleń.

103. Czy Zamawiający potwierdza, że zakres szkolenia obejmuje także omówienie plików konfiguracyjnych, rodzajów błędów, sposobów raportowania, reakcji na niestabilności i każdej składowej systemu, co w praktyce oznacza szkolenia nie tylko użytkowe, ale i administracyjno-techniczne?

Odpowiedź:

Zakres szkolenia ma odpowiadać i realizować przekazanie odpowiedniego poziomu wiedzy oraz zdolności, aby użytkownicy systemu uwzględniając ich rolę mogli korzystać w pełni świadomy i rzeczowy z wdrożonego systemu.

104. Czy Zamawiający zgodzi się na rozdzielenie szkoleń na:

- a) etap podstawowy przed produkcją,
- b) etap uzupełniający po stabilizacji systemu,
- c) szkolenia nagraniowe i e-learningowe,

skoro obecny termin 15 dni roboczych po Etapie III jest nieadekwatny do skali 450 operatorów?

Odpowiedź:

Zamawiający zgodzi się na rozdzielenie szkoleń według schematu z pytania. I w oparciu o zapis pkt 1 załącznika nr 6 do Umowy o tytule "Szkolenia" ustali ich ilość oraz typ w trakcie Analizy Przedwdrożeniowej z zachowaniem celowości.

105. Czy Zamawiający potwierdza, że materiały szkoleniowe w formie wideo, PDF lub plików edytowalnych stanowią dodatkowy obowiązek produkcyjny i dokumentacyjny, który powinien zostać uwzględniony w harmonogramie i odbiorach?

Odpowiedź:

Instrukcja jest integralną częścią systemu, zmienia się po każdej aktualizacji, tak samo jak dokumentacja systemu. Zamawiający potwierdza ich wymóg. Materiały szkoleniowe w formacie PDF mają być dostępne na zakończenie realizacji całego cyklu szkoleń.

G. Odbiory i kary

106. Czy Zamawiający zgodzi się doprecyzować kryteria odbioru dla każdego etapu, produktu, dokumentacji, migracji, aplikacji mobilnej i szkoleń, skoro wzór protokołu odbioru ma charakter bardzo ogólny i nie zawiera mierzalnych kryteriów jakościowych?

Odpowiedź:

Kryteria odbioru zostaną ustalone na etapie Analizy Przedwdrożeniowej.

107. Czy Zamawiający potwierdza, że brak szczegółowych kryteriów odbioru w połączeniu z szerokim zakresem analizy i dokumentacji przerzuca na Wykonawcę nieakceptowalne ryzyko interpretacyjne?

Odpowiedź:

Zamawiający nie potwierdza i utrzymuje dotychczasowe zapisy.

108. Czy Zamawiający zgodzi się powiązać kary umowne z jednoznacznie opisanymi kryteriami odbioru i zakresem odpowiedzialności po stronie podmiotów trzecich, zwłaszcza dla integracji i aplikacji mobilnej? § 15 przewiduje wysokie kary za opóźnienia, mimo że część zależności nie leży wyłącznie po stronie Wykonawcy.

Odpowiedź:

Zamawiający uważa, że zapis §10 ust. 2 lit a Umowy wystarczająco reguluje i określa tematykę w tym zakresie, dlatego podtrzymuje dotychczasowe zapisy.

109. Czy Zamawiający zgodzi się wyłączyć lub ograniczyć odpowiedzialność Wykonawcy za niedotrzymanie terminów wynikające z:

- a) nieprzekazania danych i dokumentacji obecnego systemu,
- b) opóźnień po stronie podmiotów zarządzających Węzłem Krajowym,
- c) opóźnień publikacyjnych w App Store / Google Play,
- d) opóźnień wynikających z uzgodnień z Zamawiającym?

Odpowiedź:

Zamawiający uważa, że zapis §10 ust. 2 lit a Umowy wystarczająco reguluje i określa tematykę w tym zakresie, dlatego podtrzymuje dotychczasowe zapisy.

H. Licencje i własność rozwiązania

110. W odniesieniu do § 11 i Załącznika nr 9 prosimy o potwierdzenie, że przedmiotem zamówienia jest udzielenie licencji do korzystania z systemu w modelu SaaS, a nie przeniesienie praw do kodu źródłowego systemu.

Odpowiedź:

Tak, zamawiający potwierdza, że przedmiotem zamówienia jest udzielenie licencji do korzystania z systemu w modelu SaaS.

111. Jeżeli Zamawiający nie oczekuje przeniesienia praw do kodu systemu, to prosimy o wyjaśnienie, z jakiego powodu opisuje dokumentację i obowiązki analityczne tak, jakby oczekiwał pełnej dokumentacji powykonawczej i architektonicznej zbliżonej do przejęcia platformy.

Odpowiedź:

Zamawiający stosuje standardowe, proceduralne wymagania co do dokumentacji systemowej w prowadzonych przez Zamawiającego projektach, zatem stwierdzenie, że Zamawiający oczekuje pełnej dokumentacji powykonawczej i architektonicznej zbliżonej do przejęcia platformy jest bezpodstawne.

112. Czy Zamawiający dopuszcza, aby wykaz licencji obejmował wyłącznie te licencje, które są faktycznie relewantne dla świadczenia usługi SaaS na rzecz Zamawiającego, bez ujawniania wewnętrznych polityk licencyjnych niezwiązanych z korzystaniem przez Zamawiającego?

Odpowiedź:

Tak, zamawiający dopuszcza, aby wykaz licencji obejmował wyłącznie te licencje, które są faktycznie relewantne dla świadczenia usługi SaaS na rzecz Zamawiającego.

Pytania szczegółowe do Załącznika nr 1 – Specyfikacja wymagań

WO – Wymagania ogólne

113. WO.01–WO.02: prosimy o wskazanie minimalnych wspieranych wersji przeglądarek oraz sposobu weryfikacji „zbyt starej wersji przeglądarki”, aby nie pozostawiać Wykonawcom swobody skutkującej nieporównywalnością ofert.

Odpowiedź:

Zamawiający określa, że minimalne wspierane wersje przeglądarek muszą uwzględniać aktualizowane i utrzymywane wersje przez producenta do trzech lat wstecz od daty wdrożenia.

114. WO.03: prosimy o wskazanie katalogu aktów prawnych i lokalnych, do których system ma być zgodny na dzień odbioru, oraz sposobu rozliczania zmian prawa w okresie utrzymania.

Odpowiedź:

Zamawiający nie jest w stanie na tym etapie wskazać zamkniętego katalogu aktów prawnych i lokalnych z racji, iż akty prawne i lokalne są aktualizowane niezależnie od Zamawiającego. Dopiero na etapie Analizy Przedwdrożeniowej będzie możliwe wskazanie obowiązujących aktów prawnych i lokalnych. W zakresie zmian prawnych w okresie utrzymania Wykonawca jest zobowiązany do dostosowania systemu na swój koszt do obowiązujących przepisów regulujących materię prawną, która wpływa na proces obsługiwany przez system.

115. WO.07–WO.08: prosimy o potwierdzenie, że szkolenia opcjonalne nie muszą być uwzględnione w terminach podstawowych oraz o wskazanie sposobu aktywacji opcji szkoleniowej.

Odpowiedź:

Szkolenia opcjonalne nie muszą być uwzględnione w terminach podstawowych wykonania umowy, ale Zamawiający zastrzega sobie prawo do wykorzystania ich w czasie trwania Umowy od momentu odbioru wdrożenia systemu i aktywuje je poprzez Zlecenie.

Zamawiający zastrzega sobie, że zamówienie określane jako „prawo opcji” jest uprawnieniem a nie zobowiązaniem zamawiającego. Wykonanie przedmiotu zamówienia w ramach prawa opcji uzależnione jest od faktycznych potrzeb zamawiającego i jego możliwości finansowych.

116. WO.09: prosimy o wskazanie, czy instrukcja ma być aktualizowana przy każdej zmianie wersji, nawet technicznej, czy tylko przy zmianie wpływającej na sposób obsługi systemu.

Odpowiedź:

Tak, instrukcja ma być aktualizowana przy każdej zmianie wersji, nawet technicznej.

117. WO.11: prosimy o potwierdzenie, czy zgodność z WCAG 2.1 AA dotyczy zarówno strony WWW, jak i aplikacji mobilnej oraz dokumentacji osadzonej w systemie. Załącznik nr 2 wskazuje bardzo szerokie obowiązki dowodowe w tym zakresie.

Odpowiedź:

Tak. Dotyczy zarówno strony WWW jak i aplikacji mobilnej.

118. WO.12: prosimy o wskazanie struktury eksportu, formatów obowiązkowych oraz sposobu bezpiecznego przekazania danych, w tym, czy dopuszczalne jest przekazanie przez API lub dump bazy, a nie wyłącznie przez pliki XML.

Odpowiedź:

Zamawiający nie dopuszcza do tego rozwiązania API lub procedury dump'u bazy danych i oczekuje oparcia się o pliki XML.

119. WO.13–WO.14: prosimy o wskazanie, czy Zamawiający dopuszcza etapowanie integracji z Węzłem Krajowym, skoro sam opis nie daje gwarancji czasu po stronie administracji publicznej.

Odpowiedź:

Procedura integracji zakłada dwa etapy integracji – na środowisku testowym, którą można wykonać na tyle wcześniej, by wyeliminować potencjalne problemy w uruchomieniu wersji produkcyjnej. To zdaniem Zamawiającego minimalizuje ryzyka związane z integracją z Węzłem Krajowym.

120. WO.15: prosimy o opublikowanie pełnej specyfikacji danych do Open Data i sposobu ich anonimizacji.

Odpowiedź:

Zbiorami eksportowanymi na portal OpenData będą: ilość aktywnych żłobków w ujęciu rocznym oraz ilość przyjętych podopiecznych w danym roku. Dane mają mieć charakter wyłącznie liczbowy, zatem nie ma wymogu opracowania sposobu ich anonimizacji.

121. WO.16: prosimy o wskazanie, które procesy anonimizacji mają być automatyczne, które ręczne i jakie mają być reguły retencji.

Odpowiedź:

Procesy anonimizacji i reguły retencji zostaną doprecyzowane na etapie Analizy Przedwdrozeniowej. W obecnym stadium Zamawiający nie jest w stanie wskazać przedmiotu pytania.

122. WO.17: skoro opcja „ticket przez SMTP” nie jest obowiązkowa, prosimy o potwierdzenie, że Wykonawca może zaoferować własne rozwiązanie ticketowe bez SMTP, jeśli zapewnia historię zgłoszeń i identyfikację wniosku.

Odpowiedź:

Tak, Wykonawca może zaoferować własne rozwiązanie.

123. WO.19: prosimy o doprecyzowanie wymogów dla SaaS, w szczególności:
a) czy dane muszą być przetwarzane wyłącznie w Polsce czy w UE,
b) jak rozumieć „dostęp VPN” dla użytkowników i administratorów,

- c) czy wszystkie wskazane zabezpieczenia sieciowe i fizyczne mają być potwierdzone certyfikatami lub oświadczeniami,
- d) które elementy są obligatoryjne, a które referencyjne.

Odpowiedź:

- a) Dane przetwarzane muszą być na terenie Europejskiego Obszaru Gospodarczego,
- b) Zamawiający rozumie przez to szyfrowany dostęp zdalny przewidziany dla Administratorów Głównych oraz Operatorów,
- c) Tak,
- d) Elementy obligatoryjne stanowią wszystkie wymagania określone Musi być oraz Powinno być (jeżeli Wykonawca zobowiązał się do ich wykonania w formularzu ofertowym), natomiast wymagania określone jako Opcja stanowią rozwiązania do wykonania w przypadku uruchomienia Zlecenia.

WT – Wymagania techniczne

124. WT.01: prosimy o wskazanie pełnego zakresu logów, pól raportowych i czasu retencji oraz o potwierdzenie, czy logi mają obejmować również usunięte wnioski i operacje na żłobkach.

Odpowiedź:

Zamawiający pełen zakres logów, pól raportowych i czas retencji wskaże w trakcie Analizy Przedwdrożeniowej, na ten moment może jedynie potwierdzić, że logi będą musiały obejmować usunięte wnioski i operacje na żłobkach.

125. WT.04–WT.05: prosimy o doprecyzowanie, czy system ma wspierać masowe zarządzanie użytkownikami i rolami według grup, czy wystarczające jest zarządzanie indywidualne.

Odpowiedź:

Tak - system ma wspierać masowe zarządzanie użytkownikami i rolami według grup oraz indywidualnych.

126. WT.11–WT.13: prosimy o wskazanie, czy polityka haseł dotyczy wszystkich ról jednakowo, czy Zamawiający dopuszcza inne polityki dla użytkowników zwykłych, opiekunów prawnych i administratorów.

Odpowiedź:

Tak dopuszcza – zostaną one doszczegółowione na etapie Analizy Przedwdrożeniowej.

127. WT.14: prosimy o opublikowanie listy wszystkich raportów i wszystkich wymaganych formatów eksportu per raport.

Odpowiedź:

Zamawiający nie jest w stanie podać na tym etapie zamkniętej listy wszystkich raportów. Poniżej znajduje się lista wstępnie wymaganych, lecz może ona zostać rozszerzona i zmienia w trakcie prac nad Analizą Przedwdrożeniową. Zakres formatów eksportu został ujęty w wymaganiu WT.14.

- Liczba dzieci oczekujących
- Liczba dzieci wstępnie przyjętych
- Liczba dzieci oczekujących wg preferencji
- Liczba dzieci oczekujących wg roku urodzenia
- Liczba dzieci oczekujących wg grupy wiekowej
- Liczba wniosków z I preferencji wg grupy wiekowej
- Liczba dzieci oczekujących z podziałem wg danych o szczepieniach
- Liczba dzieci oczekujących wg sytuacji rodziców
- Liczba wniosków dzieci niepełnosprawnych oraz wymagających szczególnej opieki
- Aktualny stan przydziału
- Lista placówek - dane teleadresowe
- Liczba wolnych miejsc w placówkach
- Podsumowanie wyników rekrutacji
- Statystyka zgłoszeń
- Podsumowanie czasu oczekiwania na przyjęcie

- Globalna lista dzieci aktualnie uczęszczających do żłobków
- Globalna lista dzieci aktualnie uczęszczających ze szczegółowymi danymi
- Lista dzieci uczęszczających do placówek
- Informacje o dziecku w pracy bieżącej
- Globalna lista dzieci niepełnosprawnych oraz wymagających szczególnej opieki
- Globalna lista dzieci usuniętych
- Dane po rekrutacji

- Analiza liczebności oddziałów i dzieci w placówkach
- Liczba dzieci uczęszczających do żłobków
- Liczba dzieci uczęszczających do żłobków wg danych o szczepieniach
- Liczba dzieci niepełnosprawnych oraz wymagających szczególnej opieki
- Liczba dzieci aktualnie uczęszczających do placówek z informacją o niepełnosprawności
- Liczba dzieci uczęszczających do placówek z informacją o niepełnosprawności

128. WT.15: prosimy o potwierdzenie, czy 30 minut bezczynności dotyczy wszystkich modułów, w tym dziennika elektronicznego i paneli

administracyjnych, oraz czy dopuszczalny jest mechanizm ostrzeżenia przed wylogowaniem.

Odpowiedź:

Tak – bez względu na pracę w konkretnym module. Polityka dotyczy całego systemu. Dopuszczamy także komunikat ostrzegający przed wylogowaniem pod rygorem powiązania z mechanizmem kontroli czasu sesji pracy z systemie i automatycznego wylogowania sesji użytkownika po określonym czasie bezczynności.

129. WT.17: prosimy o potwierdzenie, czy „odseparowanie od innych instancji systemów Wykonawcy” oznacza logiczną izolację tenantową czy osobne środowiska fizyczne/wirtualne.

Odpowiedź:

Odseparowanie od innych instancji systemów wykonawcy powinno być zapewnione co najmniej na poziomie logicznym, poprzez zastosowanie dedykowanych maszyn wirtualnych (VM), co gwarantuje separację zasobów i procesów

130. WT.18: prosimy o doprecyzowanie wszystkich przypadków automatycznej anonimizacji/usuwania i publikację reguł dla:

- a) zakończenia opieki,
- b) nieprzyjęcia dziecka,
- c) wniosku przeterminowanego,
- d) realizacji praw podmiotu danych.

Odpowiedź:

- a) Dla zakończenia opieki decyzję o usunięciu podejmuje Operator,
- b) W przypadku nieprzyjęcia dziecka (wniosek staje się przeterminowany w okresie pół roku od daty złożenia i nie oznaczenia go jako przyjęty)
- c) Po przejściu w stan wniosku przeterminowanego, pozostaje w systemie przez 1 rok czasu i zostaje usunięty.
- d) Informacje zostaną przedstawione podczas prac nad Analizą Przedwdrożeniową

WA – Wymagania administracyjne

131. WA.01: prosimy o potwierdzenie, czy Zamawiający dopuszcza ograniczenie dostępu do instancji testowej nie tylko po adresach IP, ale także przez VPN, MFA lub whitelistę użytkowników.

Odpowiedź:

Izolacja na pulę/adres IP jest wystarczająca, natomiast dopuszczamy VPN.

132. WA.02: prosimy o określenie:

- a) częstotliwości backupów,
- b) okresu przechowywania,
- c) RPO,
- d) RTO,
- e) zasad przekazania kopii po zakończeniu umowy.
- f)

Obecnie opis odsyła to do analizy, co uniemożliwia wycenę.

Odpowiedź:

Zamawiający wymaga, aby parametr RPO wynosił maksymalnie 1 dzień, zaś RTO maksymalnie 4 godziny. Częstotliwość backupów ma zostać dobrana przez Wykonawcę, aby spełnić wskazane parametry. Pozostałe aspekty ustalone zostaną w trakcie Analizy Przedwdrożeniowej.

133. WA.03: prosimy o określenie, jakie parametry wydajnościowe mają być osiągnięte przez load balancing i dla jakiej liczby jednoczesnych użytkowników.

Odpowiedź:

Parametry wydajnościowe mają pozwolić na swobodny dostęp dla minimum 5000 użytkowników dziennie, lecz Zamawiający zastrzega, że parametry okresowo mogą być zwiększone (rekrutacja terminowa).

134. WA.04–WA.05: prosimy o wskazanie procedury akceptacji upgrade'ów i wersjonowania, tak aby było jasne, które zmiany wymagają zatwierdzenia Zamawiającego, a które stanowią standardowe aktualizacje producenta.

Odpowiedź:

Procedura:

- przedstawiciele zamawiającego zgłaszają zapotrzebowanie na określoną zmianę/modyfikację lub nową funkcjonalność poprzez udostępniony system Redmine (obsługa projektu).
- Wykonawca przedstawia propozycję rozwiązania oraz ilość roboczogodzin (wycena)
- przedstawiciel zamawiającego akceptuje/odrzuca rozwiązanie
- a) odrzucone rozwiązanie może być dalej uzgadniane w celu dopasowania do potrzeb zamawiającego lub zostać zaniechane jako np. niesatysfakcjonujące/niewystarczające

- b) zaakceptowana zmiana jest procedowana do CUI w celu uzyskania zgody na finansowanie wdrożenia takiej zmiany

- Wykonawca przedstawia rozwiązanie w systemie testowym, a przedstawiciele zamawiającego wykonują testy wdrożonej zmiany. Jeżeli wszystko jest zgodne z założeniami, to zmiana może zostać wdrożona w systemie produkcyjnym.

- następnie ustalany jest moment wdrożenia zmiany w systemie (dzień, Godzina, zależność – np. wyłączenie dostępu do systemu na czas potrzebny do wdrożenia)

- po wyrażeniu zgody przez zamawiającego, zmiana jest wdrażana na produkcji

- zamawiający wprowadza zmiany w systemie produkcyjnym oraz dokonuje zmian w instrukcji operatora/administratora i wprowadza zmiany w dzienniku systemu.

135. WA.06: prosimy o doprecyzowanie, jak należy rozumieć wymóg anonimowej bazy testowej „z kluczem pozwalającym odtworzyć widzialność danych uprawnionym użytkownikom”. Czy Zamawiający ma na myśli pseudonimizację odwracalną, maskowanie, czy dwa zbiory danych?

Odpowiedź:

Zamawiający rozumie ten wymóg jako bazę ze zanonimizowanymi danymi, którą uprawniony użytkownik może zweryfikować poprzez odwrócenie anonimizacji. Zamawiający nie wskazuje konkretnego rozwiązania i dopuszcza rozwiązania techniczne pozwalające uzyskać efekt zgodny z wymaganiem.

SWS – użytkownik Rodzic/Opiekun, formularze i proces rekrutacji

136. SWS.01–SWS.02: skoro struktura konta i uprawnienia mają zostać dopiero opisane w analizie - prosimy o publikację minimalnego modelu ról i funkcji wymaganego na dzień składania ofert, w przeciwnym razie oferty będą nieporównywalne.

Odpowiedź:

Opisy ról i uprawnień znajdują się w Załączniku nr 1, dokładniej w rozdziale nr 2 „Słownik używanych pojęć”. Dokładniejsze doprecyzowanie zostanie określone w Analizie Przedwdrożeniowej.

137. SWS.03: prosimy o opublikowanie wzoru formularza/wniosku rekrutacyjnego wraz z pełną listą pól, walidacji, zależności, słowników i reguł biznesowych.

Odpowiedź:

Zamawiający publikuje „wzór formularza/wniosku rekrutacyjnego” jako Załącznik nr 2 do Załącznika nr 1 do Umowy – specyfikacja wymagań.

138. SWS.04: prosimy o wskazanie finalnego katalogu filtrów informatora, a nie odsyłanie ich do analizy.

Odpowiedź:

Filtry informatora są ogólnodostępne pod adresem : <https://rekrutacja-zlobki.um.wroc.pl/wroclaw/zlobek/oferta>

139. SWS.05–SWS.06: prosimy o jednoznaczne wskazanie reguł dla dziecka bez numeru PESEL, terminów tolerancji, blokady kwalifikacji i późniejszego uzupełnienia danych.

Odpowiedź:

W przypadku braku PESEL rodzic podaje datę urodzenia. Bez podania PESEL należy podać dokument wydany dla dziecka (wymogi z zarządzenia), wiek dziecka minimalny i maksymalny określa zarządzenie dot. rekrutacji na dany rok żłobkowym, przy czym bez spełnienia minimalnego wieku wnioski można złożyć, a nie zostanie wyznaczone miejsce w kolejce, a w przypadku przekroczenia wieku, złożenie wniosku nie będzie możliwe.

140. SWS.07–SWS.10: prosimy o wskazanie, czy Zamawiający oczekuje pełnego przeprojektowania UX formularzy i makiet, czy dopuszcza zastosowanie gotowego układu standardowego, jeśli spełnia wymagania funkcjonalne i WCAG.

Odpowiedź:

Wymagania ujęte w SWS.07-10 mają być zgodne z treścią wymagań. Zamawiający nie wskazuje konieczności przeprojektowania UX formularzy i makiet.

141. SWS.11: prosimy o wyjaśnienie, co Zamawiający rozumie przez „kreator budowania Informatora”, jakie scenariusze ma on obsługiwać i czy ma być narzędziem dla administratora, czy użytkownika.

Odpowiedź:

Zamawiający postrzega kreator jako narzędzie dla Administratorów Głównych, czymś co jest sposobem przyjmowania danych od rodzica. Chodzi o sekwencję pobierania informacji.

142. SWS.73–SWS.77: prosimy o publikację szczegółowej specyfikacji pracy bieżącej/dziennika elektronicznego, w tym:

a) listy operacji na wnioskach,

- b) pełnej listy raportów,
- c) zasad uwalniania miejsc,
- d) obsługi okresów wypowiedzenia,
- e) obsługi deklaracji kontynuacji,
- f) wymagań dot. obecności i rozliczeń.

Obecny opis pozostawia kluczowe elementy do analizy, mimo że są oznaczone jako „Musi być”.

Odpowiedź:

Operacje w pracy bieżącej

- przenoszenie dzieci między oddziałami (grupami wiekowymi)
- ustawianie flagi deklaracji kontynuacji opieki (tak/nie). Deklaracja blokuje możliwość złożenia nowego wniosku i pozwala na kontynuowanie opieki dziecka w żłobku. Brak deklaracji zwalanie miejsce do rekrutacji
- Ustawianie daty końca umowy (DD.MM.RRRR)
- Ustawienia daty początku umowy (DD.MM.RRRR)
- Ustawianie flagi końca opieki (ustawienie tego parametru powoduje uwolnienie PESEL - umożliwia złożenie nowego wniosku na np. X dni przed datą końca umowy)
- usunięcie dziecka z pracy bieżącej

W przypadku punktu f) Zamawiający nie jest w stanie na obecnym etapie udzielić odpowiedzi.

143. Czy Zamawiający zgodzi się wyłączyć z podstawowego terminu wdrożenia funkcjonalności dziennika elektronicznego i dopuścić ich etapową implementację po uruchomieniu rekrutacji, ewentualnie jako osobny system zintegrowany?

Odpowiedź:

Zamawiający nie wyraża zgody.

WTAB – bezpieczeństwo administracyjne i licencjonowanie

144. WTAB.29–WTAB.37: prosimy o publikację minimalnego modelu administracyjnego, skoro obecny opis wymaga pełnego panelu administratora, raportów ról, dezaktywacji, historii blokowania/odblokowywania i szkoleń bezpieczeństwa.

Odpowiedź:

Zamawiający podtrzymuje obecne zapisy

145. WTAB.31: prosimy o wskazanie zakresu raportu listy użytkowników i ról, pół raportu oraz częstotliwości jego generowania.

Odpowiedź:

Zamawiający w wymaganiu WTAB.31 nie wskazuje zakresu raportu, a jedynie wskazuje, że raporty mają mieć możliwość zawężania ich zakresu do konkretnej listy użytkowników w drodze wyboru oraz po określonych rolach. Częstotliwość generowania Zamawiający określa jako rozwiązanie on-demand, czyli na żądanie uprawnionego Użytkownika.

146. WTAB.35: prosimy o potwierdzenie, czy szkolenia z bezpiecznej eksploatacji są odrębnym obowiązkiem od szkoleń z Załącznika nr 6, czy stanowią ich część.

Odpowiedź:

Szkolenia z bezpiecznej eksploatacji stanowią część szkoleń z Załącznika nr 6.

147. WTAB.38–WTAB.41: prosimy o wskazanie, czy Zamawiający oczekuje ujawnienia pełnego modelu licencyjnego środowiska serwerowego i bazodanowego, czy wystarczające będzie oświadczenie zgodności i wykaz licencji wymaganych przez Załącznik nr 9.

Odpowiedź:

Zamawiający oznajmia, iż wystarczy oświadczenie zgodności i wykaz licencji.

148. dot. WO.19 (proporcjonalność)

Wymaganie WO.19 OPZ szczegółowo opisuje wymagania fizyczne datacenter (system klimatyzacji precyzyjnej, system sygnalizacji włamania i napadu, stałe urządzenia gaśnicze, system kontroli dostępu, monitoring wizyjny, awaryjne podtrzymanie zasilania, redundantne punkty dystrybucyjne sieci itd.). Wymagania te są standardem dla DC obsługujących systemy klasy bankowej, e-administracji rządowej lub krytycznej infrastruktury, a nie systemu o skali ok. 450 operatorów i charakterze usługi gminnej. Czy Zamawiający, zgodnie z zasadą proporcjonalności (art. 99 ust. 4 ustawy Pzp), potwierdza, że spełnieniem WO.19 jest przedstawienie certyfikatów dostawcy infrastruktury (np. Hetzner, OVHcloud, Beyond.pl, Atman — ISO 27001, EN 50600 klasa 4, ISO 22301, SOC 2 Type II) wraz z oświadczeniem Wykonawcy o gwarantowanym SLA dostępności co najmniej 99,9%, bez konieczności dokumentowania pojedynczych systemów fizycznych?

Odpowiedź:

Zamawiający potwierdza, że spełnieniem WO.19 jest przedstawienie certyfikatów dostawcy infrastruktury (np. Hetzner, OVHcloud, Beyond.pl, Atman — ISO 27001, EN 50600 klasa 4, ISO 22301, SOC 2 Type II) wraz z

oświadczeniem Wykonawcy o gwarantowanym SLA dostępności co najmniej 99,9%, bez konieczności dokumentowania pojedynczych systemów fizycznych.

149. § 3 ust. 2 Projektu Umowy

(Załącznik nr 8 do OPZ) określa terminy realizacji:

Etap I (Analiza Przedwdrożeniowa) — 19 dni roboczych od zawarcia umowy;

Etap II (Wdrożenie + Wersja Testowa) — 30 dni roboczych od zakończenia Etapu I;

Etap III (Wersja Produkcyjna) — 15 dni roboczych od zakończenia Etapu II;

migracja danych — 5 dni roboczych po zakończeniu Etapu II albo III;

aplikacja mobilna Android i iOS wraz z testami bezpieczeństwa — 4 miesiące kalendarzowe od zawarcia umowy.

Łączny czas Etapów I–III to ok. 64 dni roboczych (≈ 3 miesiące kalendarzowe).
W tym oknie Wykonawca, który nie zna struktury obecnie używanego przez Zamawiającego systemu, ma przeprowadzić Analizę Przedwdrożeniową dla 174 żłobków, wdrożyć i dostosować System SaaS wraz z integracjami (Węzeł Krajowy, ePUAP, PIK, BiP), uruchomić Wersję Produkcyjną, zmigrować dane z systemu Zamawiającego w 5 dni roboczych — bez wcześniejszej dokumentacji struktury źródłowej — oraz wykonać i przetestować pod kątem bezpieczeństwa aplikacje mobilne na Android i iOS w 4 miesiące kalendarzowe.

Migracja danych w 5 dni roboczych jest realnie wykonalna wyłącznie przez obecnego dostawcę systemu Zamawiającego, który zna strukturę źródłową bazy. Dla każdego innego oferenta wymaga to dodatkowo: reverse-engineeringu schematu bazy danych obecnego systemu, mappingu pól na model docelowy, testów migracji na próbie danych oraz okna walidacji rekordów osobowych pod kątem RODO. Zgodnie z art. 99 ust. 4 ustawy Pzp opis przedmiotu zamówienia nie może utrudniać uczciwej konkurencji przez wymagania faworyzujące konkretnego wykonawcę.

W związku z powyższym wnosimy o:

- a) wydłużenie Etapu II do minimum 60 dni roboczych oraz Etapu III do minimum 30 dni roboczych;
- b) wydłużenie okna migracji danych do minimum 30 dni roboczych z wyodrębnioną fazą migracji testowej (próba na podzbiórce danych) oraz fazą migracji produkcyjnej (cut-over);
- c) zapisanie w § 3 oraz w postanowieniach o karach umownych Projektu Umowy, że termin migracji liczony jest POD WARUNKIEM uprzedniego dostarczenia przez Zamawiającego pełnej dokumentacji struktury danych obecnie używanego systemu, obejmującej: schemat tabel źródłowej bazy danych (DDL); słowniki i kody wartości referencyjnych; formaty plików eksportu (CSV / XML / JSON) wraz z opisem semantyki kolumn; reprezentatywną próbkę danych testowych zanonimizowaną zgodnie z RODO o objętości umożliwiającej walidację mappingu; dokumentację

reguł walidacji i zależności referencyjnych (klucze obce, ograniczenia integralności); dokumentację formatu danych osobowych podlegających pseudonimizacji lub anonimizacji. W przypadku niedostarczenia powyższej dokumentacji wraz z dostępem do danych w terminie 30 dni roboczych przed planowanym rozpoczęciem migracji, termin migracji ulega proporcjonalnemu wydłużeniu o liczbę dni opóźnienia w dostarczeniu dokumentacji, bez naliczania kar umownych za opóźnienie po stronie Wykonawcy;

- d) dołączenie do OPZ wzoru SLA migracji obejmującego definicję cut-over, kryteria odbioru migracji (procent poprawnie zmigrowanych rekordów, akceptowalne odchylenia) oraz tryb rollbacku w razie niepowodzenia;
- e) jasne rozdzielenie w Załączniku nr 1 zakresu migracji obowiązkowej (dane bieżące — aktywne dzieci, oczekujące, listy rekrutacyjne) od migracji archiwalnej (dane historyczne $\geq N$ lat) — kryterium to istotnie wpływa na ryzyko i wycenę oferty;
- f) opublikowanie pełnego Harmonogramu Ramowego (kamienie milowe + zależności + bufor) w treści OPZ, a nie wyłącznie w Załączniku nr 8 — termin realizacji jest istotnym czynnikiem wyceny ryzyka oferty.

Odpowiedź:

W nawiązaniu do odpowiedzi na pytania numer 57 Zamawiający nie zmienia powyższych terminów, które uznaje za możliwe do dotrzymania przez wykonawców. Natomiast w odpowiedzi do punktów c-f Zamawiający informuje, że zapis Umowy tj. par.10 ust.2 pkt a wystarczająco reguluje elastyczność w tym zakresie na wypadek nieprzewidzianych problemów w kontekście podnoszonym przez pytającego.

150. dot. § 6 ust. 3 Projektu Umowy / Załącznik nr 8
§ 6 ust. 3 Projektu Umowy stanowi: „Serwer lub serwery, na którym (-ych) zainstalowany zostanie System zawsze znajdować się będzie (będą) na terenie Rzeczypospolitej Polskiej (...)”.
- Wskazujemy, że:
- a) Obowiązujące przepisy o ochronie danych osobowych (RODO, art. 44–49) wymagają lokalizacji przetwarzania danych w obszarze Europejskiego Obszaru Gospodarczego (EOG), a nie wyłącznie na terenie Rzeczypospolitej Polskiej. Transfery danych osobowych w ramach EOG nie podlegają ograniczeniom z art. 44 RODO i są w pełni dopuszczalne dla podmiotów publicznych;
 - b) W obszarze samoregulacji branżowej dostawców chmurowych funkcjonuje EU Cloud Code of Conduct (eucoc.cloud) — kodeks postępowania zatwierdzony przez Europejską Radę Ochrony Danych (EROD) zgodnie z art. 40 RODO, do którego mogą przystępować dostawcy infrastruktury chmurowej działający w obszarze EOG;
 - c) Restrykcje lokalizacyjne typu „data residency Poland only” są stosowane w polskim sektorze publicznym wyłącznie dla informacji

niejawnych (klauzule Zastrzeżone / Poufne / Tajne) lub danych szczególnej kategorii o znaczeniu krytycznym dla bezpieczeństwa narodowego. Dane przetwarzane w systemie rekrutacji i dziennika elektronicznego dla żłobków nie są informacjami niejawnymi i nie kwalifikują się do tej kategorii;

d) Wymóg lokalizacji wyłącznie w Polsce drastycznie ogranicza katalog dostępnych dostawców infrastruktury, eliminując konkurencyjnych dostawców europejskich oferujących korzystniejszy stosunek ceny do parametrów wydajnościowych przy tych samych standardach bezpieczeństwa potwierdzonych certyfikatami ISO 27001, ISO 27017, ISO 27018, EN 50600. Stanowi to ograniczenie konkurencji w rozumieniu art. 99 ust. 4 ustawy Pzp w związku z art. 16 (zasada równego traktowania wykonawców) oraz art. 17 ust. 1 (zasada uczciwej konkurencji) ustawy Pzp.

Wnosimy o:

- 1) zmianę zapisu § 6 ust. 3 Projektu Umowy na: „Serwer lub serwery, na którym (-ych) zainstalowany zostanie System, znajdować się będą na terenie Europejskiego Obszaru Gospodarczego (EOG). Wszystkie kopie zapasowe danych przechowywane będą w obszarze EOG. Wykonawca zobowiązuje się do zapewnienia zgodności lokalizacji przetwarzania z wymaganiami RODO art. 44–49.”; 2) doprecyzowanie, że wymóg lokalizacji nie ma zastosowania do węzłów CDN, usług anti-DDoS oraz infrastruktury monitorującej, o ile nie przetwarzają one danych osobowych użytkowników w sposób trwały;
- 2) potwierdzenie, że certyfikaty ISO 27001, ISO 27017, ISO 27018 oraz EN 50600 wystawione dla data center dostawcy infrastruktury w EOG są równoważne wymaganiom bezpieczeństwa wskazanym w Załączniku nr 1 do OPZ, zgodnie z art. 101 ust. 5 ustawy Pzp;
- 3) potwierdzenie, że Wykonawca może wykorzystać do realizacji Umowy infrastrukturę dostawcy chmurowego / hostingowego z DC w innych państwach EOG, pod warunkiem zachowania wszystkich pozostałych wymagań bezpieczeństwa OPZ (ISO 27001, szyfrowanie at-rest i in-transit, kopie zapasowe, RPO / RTO, ciągłość działania).

Odpowiedź:

AD.1 Zamawiający potwierdza, że serwer lub serwery, na których zostanie zainstalowany system mogą być umiejscowione na terenie Europejskiego Obszaru Gospodarczego.

Zamawiający **zmienia treść § 6 ust. 3 Załącznika nr 8 do umowy** poprzez wykreślenie dotychczasowej treści i zastąpienie nową w brzmieniu:

„Wykonawca zobowiązany jest do doboru parametrów wydajnościowych serwera lub serwerów (w tym wirtualnych) w taki sposób, aby Zamawiający mógł korzystać z Systemu i udostępniać go zgodnie z jego przeznaczeniem i funkcjonalnością opisaną w Dokumentacji. Wykonawca pozostaje wyłącznie uprawniony do decydowania o konkretnej specyfikacji serwera lub serwerów,

na którym (-ych) zainstalowany zostanie System, w szczególności o zastosowanym sprzęcie i oprogramowaniu serwera. Serwer lub serwery, na którym (-ych) zainstalowany zostanie System, znajdować się będą na terenie Europejskiego Obszaru Gospodarczego (EOG). Wszystkie kopie zapasowe danych przechowywane będą w obszarze EOG. Wykonawca zobowiązuje się do zapewnienia zgodności lokalizacji przetwarzania z wymaganiami RODO art. 44–49., przy czym Wykonawca podejmuje decyzję o konkretnej lokalizacji serwera (-ów). Wykonawca jest uprawniony do zmiany serwera lub serwerów, na którym (-ych) zainstalowany jest System, w tym zmiany lokalizacji takiego serwera (-ów), o czym każdorazowo będzie powiadamiać Zamawiającego”

AD.2 Zamawiający potwierdza, że wymóg lokalizacji nie ma zastosowania do węzłów CDN, usług anti-DDoS oraz infrastruktury monitorującej, o ile nie przetwarzają one danych osobowych użytkowników w sposób trwały,

AD.3 Zamawiający potwierdza.

ZMIANA TREŚCI SWZ

Zamawiający działając zgodnie z art. 137 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 ze zm.) zmienia treść SWZ w następujący sposób:

- 1) w rozdziale 3 ppkt. 3.3 SWZ wykreśla dotychczasową treść i zastępuje ją nowym brzmieniem:

„Zamawiający zastrzega sobie możliwość skorzystania z prawa opcji, o którym mowa w art. 441 ustawy Pzp na zasadach i w okolicznościach określonych w projekcie umowy – załącznik nr 8 do SWZ. Zamawiający zastrzega sobie, że zamówienie określane jako „prawo opcji” jest uprawnieniem a nie zobowiązaniem zamawiającego. Wykonanie przedmiotu zamówienia w ramach prawa opcji uzależnione jest od faktycznych potrzeb zamawiającego i jego możliwości finansowych. Brak wykonania przedmiotu zamówienia w zakresie prawa opcji nie rodzi żadnych roszczeń ze strony Wykonawcy.”

- 2) W Załączniku nr 8 do SWZ – projekt umowy w §1 dodaje się definicje:

*„**Zlecenie** – zakres usług, które Wykonawca ma wykonać w ramach prawa opcji wskazanych w niniejszej Umowie”*

- 3) w Załączniku nr 8 do SWZ – projekt umowy wykreśla dotychczasową treść w §2 ust. 3 i zastępuje ją nowym brzmieniem:

„3. Opcja, o której mowa w ust 2, zostanie uruchomiona na skutek zlecenia Zamawiającego, przesłanego na adres poczty elektronicznej

Wykonawcy, wskazany w §12 ust 1 , w formie elektronicznej, w terminach:

- 1) *przeprowadzenie wdrożenia i przeszkolenia, o których mowa w ust. 2 pkt 1 – nie później niż 15 dni roboczych od momentu przekazania Zlecenia przez Zamawiającego,*
 - 2) *wdrożenie dodatkowych elementów systemu opisanych jako „Opcja”, o których mowa w ust. 2 pkt 2 – nie później niż 15 dni roboczych od momentu przekazania Zlecenia przez Zamawiającego,*
 - 3) *zapewnienie Usług Rozwojowych, o których mowa w ust. 2 pkt 3 – nie później niż do dnia ustalonego w Zleceniu w oparciu o procedurę ujętą w § 19.,*
 - 4) *przygotowanie i przekazanie danych, o których mowa w ust. 2 pkt 4 – nie później niż 30 dni roboczych od terminu przekazania Zlecenia przez Zamawiającego do Wykonawcy,*
 - 5) *świadczenie Usług Utrzymania, o których mowa w ust. 2 pkt 5 – nie później niż następnego dnia kalendarzowego następującego po zakończeniu uprzedniego okresu świadczenia Usług Utrzymania, Zamawiający przekaże zlecenie najpóźniej do 10 dni kalendarzowych przed upływem terminu aktualnie świadczonych Usług Utrzymania,”*
- 4) w Załączniku nr 8 do SWZ – projekt umowy dodaje w §15 ustęp 15a o następującej treści:
- „15a. Zamawiający naliczy każdorazowo kary umowne w przypadku zwłoki we wdrożeniu przedmiotu zleconego przez Zamawiającego w ramach Usług Rozwojowych, wysokości 500 zł za każdy dzień zwłoki w stosunku do terminów określonych w Zleceniu”*
- 5) w Załączniku nr 8 do SWZ – projekt umowy dotychczasowy §19 zmienia numer na §20 i Zamawiający dodaje §19 o nowej treści w brzmieniu:

„§19. Zlecenie Usług Rozwojowych

1. *Zamawiający w ramach prawa opcji może zlecić Wykonawcy świadczenie Usług Rozwojowych wskazując w zleceniu rodzaj usługi, zakres i oczekiwany termin wykonania.*
2. *Przed zleceniem Usługi Rozwojowej Zamawiający wyśle zapytanie do Wykonawcy o przewidywaną liczbę Roboczogodzin potrzebnych do jej wykonania oraz o proponowany termin jej wykonania.*
3. *Wykonawca w terminie 14 dni od otrzymania zapytania Zamawiającego prześle do Zamawiającego odpowiedź*

obejmującą: wycenę zawierającą wskazanie liczby Roboczogodzin koniecznych do wykonania Usługi Rozwojowej oraz potwierdzenie lub propozycję terminu jej wykonania.

4. *Wskazanie, o którym mowa w ust.3 powyżej musi zawierać poniższe informacje:*
 - a. *Czy w wycenę wchodzi inne prace poza implementacją kodu (jeżeli tak to wymienić jakie oraz w jakiej liczbie Roboczogodzin);*
 - b. *Opis zmian w architekturze wynikającej ze zlecenia (jeżeli dotyczy) lub informację, że zmiana w architekturze nie wystąpi;*
 - c. *Czy zmieniają się struktury danych w Systemie w związku ze zleceniem. Jeżeli tak to należy krótko uzasadnić i opisać te zmiany;*
 - d. *W jakich technologiach będzie dokonywana zmiana (kod źródłowy, zastosowane narzędzia, konfiguracja, itp);*
 - e. *Ocena ryzyka zleconej zmiany - czy zmiana ma duży wpływ na inne role, proces biznesowy. Jeżeli tak należy je opisać;*
 - f. *Wskazanie wariantów realizacji zlecenia o ile istnieją; w szczególności czy możliwe jest uzyskanie efektów zlecenia z wykorzystaniem istniejących już funkcji Systemu;*
 - g. *Wskazanie czy zlecona zmiana została już zrealizowana dla innego klienta;*
 - h. *Czy zlecona zmiana została zaplanowana przez Wykonawcę w ramach własnych planów rozwojowych. Jeżeli tak to kiedy zostanie udostępniona klientom do korzystania;*
 - i. *Kontakt do osoby, która może odpowiedzieć na bardziej szczegółowe pytania techniczne wyceny.*
5. *Zamawiający po otrzymaniu odpowiedzi Wykonawcy może: potwierdzić zlecenie Usługi Rozwojowej zgodnie z treścią zlecenia i odpowiedzi Wykonawcy albo zaprosić Wykonawcę do negocjacji celem ustalenia ostatecznego zakresu, pracochłonności i terminu jej realizacji.*
6. *Działania opisane w ust.3 i 4 powyżej mogą być powtarzane nie więcej niż 3 razy.*
7. *W razie nieuzyskania przez Wykonawcę potwierdzenia zlecenia, uznaje się, że nie zostało ono zlecone i Wykonawca nie uzyskuje prawa do wynagrodzenia.*
8. *Wykonawca może odmówić realizacji zlecenia tylko i wyłącznie w przypadku gdyby wymagałyby one zmian w architekturze*

Systemu; w szczególności: naruszałyby integralność danych w Systemie, zmieniałyby przeznaczenie atrybutów w bazie danych lub zmieniałyby algorytmy stosowane w Systemie w sposób taki, że odbiegałyby od ogólnie przyjętych zasad oraz w innych sytuacjach gdy z przyczyn natury obiektywnej czy ze względu na specyfikę Systemu nie jest możliwa realizacja zleconych prac. W przypadku opisanym w poprzednim zdaniu, Wykonawca zobowiązany jest do przesłania szczegółowego uzasadnienia (w szczególności wariantu częściowej lub alternatywnej realizacji zlecenia, jeżeli taka częściowa lub alternatywna realizacja zlecenia jest możliwa), pod rygorem uznania, że Wykonawca pozostaje w zwłoce z przesłaniem informacji zwrotnej.

9. *Wykonawca jest zobowiązany zrealizować zlecenie najpierw na wersji testowej Systemu i dopiero po potwierdzeniu przez Zamawiającego prawidłowości uzgodnić z nim termin udostępnienia na wersji produkcyjnej Systemu.*
10. *Wycena musi uwzględniać przeprowadzenie testów przez Wykonawcę na wersji testowej Systemu, przygotowanie i udostępnienie Zamawiającemu stosownego raportu z nich oraz udostępnienia na wersji produkcyjnej Systemu.*
11. *Wszelkie oświadczenia składane w toku powyższej procedury przez Zamawiającego i Wykonawcę powinny być dokonane w HelpDesk.*

6) wykreśla się dotychczasową treść pkt. 9.1, 11.1, 11.2 SWZ i nadaje im nowe brzmienie:

9.1. Wykonawca pozostaje związany ofertą do dnia **14.08.2026r.**

11.1. **Ofertę należy złożyć** w formie elektronicznej za pośrednictwem platformy zakupowej zamieszczonej pod adresem:

<https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-033cba98-e0cf-409a-b636-860256cc4d91>

w terminie do dnia 22.05.2026 r. do godz. 11:00

11.2. **Otwarcie ofert nastąpi w dniu 22.05.2026 o godz. 11:30** poprzez odszyfrowanie wczytanych na Platformie ofert.

Pozostałe zapisy SWZ pozostają bez zmian.

W załączeniu:

- Załącznik nr 1 do Załącznika nr 1 do Umowy - „Raporty - przykłady i charakterystyka” jako Załącznik nr 1 do- specyfikacja wymagań

- Załącznik nr 2 do Załącznika nr 1 do Umowy – „wzór formularza/wniosku rekrutacyjnego”

**Dyrektor
Centrum Usług Informatycznych we
Wrocławiu
Tymoteusz Przybylski**

Dokument podpisano podpisem elektronicznym.

Sprawę prowadzi: Magdalena Anuszkiewicz

Informacje na temat przetwarzania danych osobowych przez CUI znajdują się na stronie BIP CUI