

DIT-DITZBZ.260.47.2026.JS

Warszawa, 16 czerwca 2026 roku

Wykonawcy**Dot. zapytania ofertowego w zakresie zamówienia pn.: „Dostawa i wdrożenie narzędzia do transkrypcji mowy do tekstu”.**

Zamawiający przekazuje treść pytań oraz zmiany i wyjaśnienia do zapytania ofertowego.

Pytanie nr 1

Dotyczy: § 1, definicja „Kody źródłowe” (przypis 1), § 4 ust. 16–19 oraz § 7 ust. 40–46 projektu umowy — zakres przekazania kodu źródłowego

Wykonawca zamierza zaoferować autorskie oprogramowanie objęte licencją wieczystą, które do realizacji wybranych funkcji wykorzystuje komponenty open source (m.in. Whisper, pyannote.audio) udostępniane na licencjach permissywnych typu MIT. Licencje te nie nakładają na Wykonawcę obowiązku udostępniania kodu źródłowego produktu, w którym komponenty te zostały osadzone.

Zgodnie z przypisem 1 do definicji „Kody źródłowe” oraz przypisem 15 do § 4, postanowienia dotyczące przekazania Kodów źródłowych mają zastosowanie wyłącznie w przypadku zaoferowania Narzędzia opartego o Oprogramowanie Open Source, a w przypadku Narzędzia opartego w całości o licencje wieczyste są usuwane. Jednocześnie w odpowiedzi na Pytanie nr 6 z dnia 30 kwietnia 2026 r. Zamawiający potwierdził, że dla oprogramowania już istniejącego, licencjonowanego, oczekuje udzielenia licencji „bez przekazywania kodów źródłowych, czy też dokumentacji algorytmów”.

Prosimy o jednoznaczne potwierdzenie, że w przypadku zaoferowania autorskiego Narzędzia objętego licencją wieczystą, wykorzystującego komponenty open source na licencjach niewymagających ujawnienia kodu:

1. Wykonawca nie jest zobowiązany do przekazania ani udostępnienia w repozytorium Zamawiającego kodu źródłowego autorskiej aplikacji (produktu), a samo osadzenie w Narzędziu komponentów open source nie powoduje przekwalifikowania oferty na wariant „Oprogramowanie Open Source”;
2. postanowienia § 4 ust. 16–18 (składowanie i przekazywanie Kodów źródłowych, bieżące ich aktualizowanie, analiza SonarQube) nie mają zastosowania do autorskiej aplikacji objętej licencją wieczystą;
3. za wystarczające spełnienie obowiązków Wykonawcy w odniesieniu do wykorzystanych komponentów open source (zgodnie z § 7 ust. 45 oraz § 4 ust. 19) Zamawiający uzna dostarczenie wykazu tych komponentów zawierającego: nazwę komponentu, wersję, typ i treść licencji oraz link do publicznego repozytorium producenta.

Odpowiedź

Ad 1

Zamawiający potwierdza założenie przyjęte w pytaniu.

Ad 2

Zamawiający potwierdza założenie przyjęte w pytaniu.

Ad 3

Zamawiający potwierdza założenie przyjęte w pytaniu, pod warunkiem aktualizowania przez Wykonawcę informacji w sytuacji zaistnienia zmiany komponentu, jego wersji typu i treści licencji oraz linku do repozytorium.

Pytanie nr 2

Dotyczy: § 4 ust. 16 pkt 5 projektu umowy — termin „bieżącego aktualizowania” Kodów źródłowych

§ 4 ust. 16 pkt 5 zobowiązuje Wykonawcę do bieżącego aktualizowania Kodu źródłowego na repozytorium oraz jego przekazywania w terminie do 3 Dni roboczych od wprowadzenia zmian. W praktyce każda zmiana w komponencie open source wymaga uprzedniego przetestowania i walidacji przed wprowadzeniem do działającej aplikacji, a literalne brzmienie zapisu wymuszałoby przekazywanie każdej, nawet drobnej, zmiany w bardzo krótkim, sztywnym terminie.

W nawiązaniu do Pytania nr 1 prosimy o potwierdzenie, że:

1. obowiązek z § 4 ust. 16 pkt 5 — o ile w ogóle znajdzie zastosowanie do oferty Wykonawcy — dotyczy wyłącznie komponentów open source faktycznie składowanych w repozytorium Zamawiającego, a nie kodu autorskiej aplikacji objętej licencją wieczystą;
2. Zamawiający dopuszcza ograniczenie obowiązku przekazywania aktualizacji do zmian istotnych, tj. wpływających na bezpieczeństwo (usuwanie podatności) oraz wydań typu major release, z zachowaniem czasu niezbędnego na ich uprzednie przetestowanie, a termin 3 Dni roboczych liczony jest od wprowadzenia danej zmiany do środowiska produkcyjnego Zamawiającego.

Odpowiedź

Ad 1

Zamawiający potwierdza założenie przyjęte w pytaniu.

Ad 2

Zmawiający zmienia treść § 4 ust. 16 pkt 5 projektu umowy, który otrzymuje brzmienie:

„5) zapewni Zmawiającemu bieżące aktualizowanie Kodu źródłowego na repozytorium kodów źródłowych oraz ich przekazywanie Zamawiającemu w terminie do 3 Dni roboczych od poinformowania Wykonawcy – w formie mailowej na adres e-mail wskazany w § 16 ust. 1 pkt 2 – o wprowadzeniu danej zmiany do środowiska produkcyjnego Zamawiającego, przy czym przewidziane w ust. 17 wymagania dotyczące sposobu przekazania oraz elementów, które mają być przekazane wraz z Kodem źródłowym, stosuje się także do wszelkich aktualizacji Kodu źródłowego;”.

Pytanie nr 3

Dotyczy: § 6 ust. 2 pkt 4 i 6 projektu umowy — szyfrowanie komunikacji sieciowej (interfejs zewnętrzny a komunikacja wewnętrzna)

§ 6 ust. 2 pkt 4 i 6 wymagają zapewnienia bezpieczeństwa komunikacji sieciowej poprzez silne szyfrowanie oraz udostępniania bezpiecznych protokołów (np. HTTPS, SFTP). Jednocześnie zgodnie z § III ust. 2 Załącznika nr 1 Narzędzie działa wyłącznie lokalnie (on-premise), w izolacji od sieci internet.

W architekturze kontenerowej (mikrouслуги) komunikacja użytkownika z Narzędziem może być terminowana szyfrowaniem na zewnętrznym interfejsie (np. na reverse proxy / load balancerze Zamawiającego), natomiast komunikacja pomiędzy poszczególnymi komponentami odbywa się w wydzielonej, wewnętrznej sieci kontenerowej.

Prosimy o potwierdzenie, że:

1. wymóg szyfrowania komunikacji sieciowej z § 6 ust. 2 pkt 4 i 6 odnosi się do interfejsu Narzędzia udostępnianego użytkownikom (komunikacja zewnętrzna), a za jego spełnienie Zamawiający uzna zapewnienie połączenia HTTPS/TLS na tym interfejsie;
2. dla komunikacji wewnętrznej pomiędzy komponentami Narzędzia, realizowanej w odizolowanej sieci kontenerowej w środowisku on-premise pozbawionym dostępu do internetu, dopuszczalne jest stosowanie komunikacji nieszyfrowanej (np. HTTP) i nie zostanie to uznane za Podatność bezpieczeństwa w trakcie testów bezpieczeństwa, względnie — w razie braku takiego potwierdzenia — czy Zamawiający uzna brak szyfrowania komunikacji wewnętrznej za zgodny z wymaganiami w trybie § 6 ust. 3, jeżeli Wykonawca wykaże, że nie generuje on zagrożenia w rozumieniu definicji Podatności bezpieczeństwa.

Odpowiedź

Ad 1

Zamawiający potwierdza założenie przyjęte w pytaniu.

Ad 2

Zamawiający uzna brak szyfrowania komunikacji wewnętrznej za zgodny z wymaganiami § 6 ust. 3 projektu umowy, jeżeli Wykonawca wykaże, że nie generuje on zagrożenia w rozumieniu definicji Podatności bezpieczeństwa.

Pytanie nr 4

Dotyczy: § 6 ust. 2 pkt 5 projektu umowy w zw. z § III ust. 3 Załącznika nr 1 — poziom szyfrowania danych w spoczynku

§ 6 ust. 2 pkt 5 wymaga przechowywania danych wrażliwych w formie zaszyfrowanej, tam gdzie jest to technicznie i organizacyjnie możliwe. Jednocześnie w odpowiedzi na Pytanie nr 2 z dnia 30 kwietnia 2026 r. Zamawiający potwierdził, że funkcjonalności wskazane w § III ust. 3 Załącznika nr 1 (w tym mechanizm szyfrowania danych) mają być zapewnione na poziomie infrastruktury i systemu operacyjnego dostarczanego przez Zamawiającego (Red Hat Enterprise Linux), a nie stanowią wymagań funkcjonalnych wobec aplikacji do transkrypcji.

Prosimy o potwierdzenie, że:

1. wymóg szyfrowania danych w spoczynku (przechowywanych) jest spełniony poprzez szyfrowanie zapewniane na poziomie infrastruktury i systemu operacyjnego dostarczanego przez Zamawiającego (np. szyfrowanie wolumenów/dysków), a aplikacja nie musi implementować odrębnej, własnej warstwy szyfrowania danych w spoczynku;
2. przez „dane wrażliwe” w rozumieniu § 6 ust. 2 pkt 5 Zamawiający rozumie pliki nagrań audio i wideo wgrywane przez Użytkowników do aplikacji — co umożliwi Wykonawcy prawidłowe przygotowanie Narzędzia oraz jednoznaczny weryfikację w trakcie testów bezpieczeństwa.

Odpowiedź

Zamawiający potwierdza założenia przyjęte w pytaniach.

Pytanie nr 5

Dotyczy: § 6 ust. 2 pkt 10 projektu umowy — przechowywanie danych uwierzytelniających i sekretów w plikach konfiguracyjnych

§ 6 ust. 2 pkt 10 wymaga przechowywania danych uwierzytelniających w plikach konfiguracyjnych w formie zaszyfrowanej.

W architekturze kontenerowej (np. z wykorzystaniem Docker Compose) dosłowne spełnienie tego wymogu jest często technicznie niewykonalne — sekrety i dane uwierzytelniające zarządzane są przy użyciu innych, powszechnie uznanych za bezpieczne mechanizmów, takich jak zmienne środowiskowe, mechanizmy sekretów platformy konteneryzacji (np. Docker/Kubernetes secrets), dedykowane menedżery sekretów lub ograniczenie uprawnień dostępu do plików na poziomie systemu operacyjnego.

Prosimy o potwierdzenie, że za spełnienie wymogu z § 6 ust. 2 pkt 10 Zamawiający uzna zastosowanie ogólnie przyjętych, bezpiecznych metod zarządzania sekretami (m.in. wskazanych powyżej), a nie wyłącznie szyfrowanie zawartości plików konfiguracyjnych, względnie — w razie braku takiego potwierdzenia — czy zastosowane przez Wykonawcę rozwiązanie zostanie zaakceptowane w trybie § 6 ust. 3, jeżeli Wykonawca wykaże, że nie generuje ono zagrożenia w rozumieniu definicji Podatności bezpieczeństwa.

Odpowiedź

Zamawiający potwierdza, że zastosowane przez Wykonawcę rozwiązanie zostanie zaakceptowane w trybie § 6 ust. 3, jeżeli Wykonawca wykaże, że nie generuje ono zagrożenia w rozumieniu definicji Podatności bezpieczeństwa.

Pytanie nr 6

Dotyczy: § 1 pkt 2 i 3, § 4 ust. 9, ust. 11–12 projektu umowy — rozłożenie w czasie godzin serwisu (240 rg) i modyfikacji (160 rg)

Projekt umowy przewiduje świadczenie serwisu w wymiarze do 240 roboczogodzin oraz realizację modyfikacji w wymiarze do 160 roboczogodzin, w okresie 12 miesięcy od podpisania protokołu odbioru końcowego. Serwis jest rozłożony w czasie poprzez limit miesięczny (§ 4

ust. 9), natomiast pula modyfikacji nie zawiera analogicznego mechanizmu rozłożenia w czasie.

Tworzy to ryzyko skumulowania znacznej części zleceń (w szczególności modyfikacji) w końcowym okresie obowiązywania Umowy, co przy obowiązujących terminach realizacji i karach umownych (§ 12 ust. 7) jest trudne do rzetelnego oszacowania i obsłużenia.

Prosimy o potwierdzenie, że:

1. realizacja zleceń modyfikacji następuje na podstawie harmonogramu uzgodnionego z Wykonawcą (§ 4 ust. 12 pkt 1–2), a Wykonawca nie jest zobowiązany do zapewnienia jednoczesnej dostępności pełnej puli roboczogodzin w dowolnym, dowolnie krótkim terminie;
2. Zamawiający dopuszcza uzgadnianie realnych terminów realizacji zleceń, adekwatnych do ich pracochłonności, w przypadku kumulacji zleceń w danym okresie, w szczególności pod koniec obowiązywania Umowy.

Odpowiedź

Zgodnie z § 1 pkt 3 projektu umowy realizacja przez Wykonawcę modyfikacji Narzędzia w liczbie do 160 roboczogodzin będzie odbywała się na podstawie zleceń **otrzymanych od Zamawiającego, w okresie 12 miesięcy** od podpisania protokołu odbioru końcowego Narzędzia, co oznacza, że zlecenia będą realizowane sukcesywnie, zgodnie z potrzebami Zamawiającego tj. zlecenie może być realizowane i odebrane po zakończeniu okresu wsparcia.

Pytanie nr 7

Dotyczy: § 6 ust. 2 pkt 17 projektu umowy w zw. z § 1 pkt 1–2 i § 4 ust. 8–9 — czasowy zakres obowiązku utrzymywania komponentów wolnymi od podatności i ich aktualizacji

§ 6 ust. 2 pkt 17 zobowiązuje Wykonawcę do korzystania wyłącznie z aktualnych i wolnych od znanych podatności bezpieczeństwa komponentów oraz bibliotek programistycznych „przez cały okres wsparcia”.

Prosimy o potwierdzenie, że:

1. obowiązek utrzymywania komponentów wolnymi od znanych podatności oraz dostarczania związanych z tym aktualizacji trwa wyłącznie przez okres świadczenia wsparcia/serwisu, o którym mowa w § 1 pkt 1–2 (12 miesięcy), i nie ma charakteru bezterminowego; po zakończeniu tego okresu Zamawiający nie nabywa prawa do dalszych, nieodpłatnych aktualizacji;
2. nakład pracy związany z usuwaniem podatności i aktualizacją komponentów realizowany jest w ramach pul wsparcia/serwisu i modyfikacji przewidzianych w Umowie;
3. obowiązek z § 6 ust. 2 pkt 17 dotyczy wyłącznie komponentów i bibliotek bezpośrednio dostarczonych przez Wykonawcę w ramach Narzędzia, a nie warstwy systemu operacyjnego (Red Hat Enterprise Linux) ani infrastruktury pozostającej pod kontrolą i w gestii Zamawiającego.

Odpowiedź

Zamawiający potwierdza założenia przyjęte w pytaniach.

Pytanie nr 8

Dotyczy: § 4 ust. 8 pkt 1–3 oraz § 7 ust. 1 pkt 1–2 i ust. 3–4 projektu umowy w zw. z § III ust. 1 pkt 3 i ust. 2 Załącznika nr 1 — mechanizm dostarczania nowych wersji oprogramowania oraz stan po wygaśnięciu wsparcia

§ 4 ust. 8 przewiduje zapewnienie wsparcia producenta obejmującego m.in. możliwość pobierania i instalacji nowych wersji oprogramowania oraz dostęp 24/7 do aktualizacji i poprawek „poprzez portal producenta lub stronę www producenta”, a także możliwość dokonywania zgłoszeń przez portal producenta. Jednocześnie zgodnie z § III ust. 1 pkt 3 Załącznika nr 1 wgrywanie wszelkich poprawek, aktualizacji i konfiguracji realizowane jest w trybie offline, a zgodnie z § III ust. 2 Narzędzie działa w izolacji od sieci internet.

W przypadku oferowanego rozwiązania producentem Narzędzia jest Wykonawca, a samo Narzędzie jest specjalistycznym oprogramowaniem opartym o modele AI, którego obrazy kontenerów osiągają rozmiary rzędu wielu gigabajtów. Z tego względu nowe wersje i poprawki są dostarczane Zamawiającemu w sposób offline, w ramach świadczonej usługi serwisowej, a nie poprzez publiczny portal czy stronę www z dostępem 24/7. Udostępnianie aktualizacji „24/7 przez portal/stronę www producenta” jest w tym modelu fizycznie niewykonalne i sprzeczne z wymaganym w OPU trybem offline oraz izolacją od internetu.

Prosimy o potwierdzenie, że:

1. obowiązki dotyczące dostarczania nowych wersji, aktualizacji i poprawek (§ 4 ust. 8 pkt 1–2) oraz przyjmowania zgłoszeń (§ 4 ust. 8 pkt 3) Zamawiający uzna za spełnione, jeżeli będą realizowane kanałami Wykonawcy uzgodnionymi z Zamawiającym — tj. poprzez dostarczenie obrazów/poprawek w trybie offline w ramach usługi serwisowej oraz przyjmowanie zgłoszeń drogą elektroniczną (e-mail) — w sposób zgodny z trybem offline i izolacją wymaganymi w § III ust. 1 pkt 3 i ust. 2 Załącznika nr 1;
2. prawo Zamawiającego do nowych wersji, aktualizacji i poprawek przysługuje w okresie świadczenia wsparcia/serwisu (12 miesięcy), a po jego wygaśnięciu Zamawiający zachowuje prawo do korzystania z ostatnio dostarczonej wersji Narzędzia (zgodnie z § 7 ust. 4), nie nabywając jednak prawa do kolejnych wersji, aktualizacji ani poprawek dostarczanych po zakończeniu tego okresu.

Odpowiedź

Ad 1

Postanowienia zawarte w projekcie umowy są uniwersalne i pasują do Wykonawcy zarówno będącego jak i nie będącego producentem Narzędzia.

Jednocześnie Zamawiający zmienia § 4 ust. 8 projektu umowy, który otrzymuje brzmienie:

„8. Wykonawca zapewni wsparcie producenta dla licencji wieczystych, o którym mowa w § 1 pkt 1, w tym zapewni Zamawiającemu:

- 1) możliwość pobierania i prawo do instalacji nowych wersji oprogramowania bez dodatkowych opłat, w tym opłat licencyjnych;
- 2) dostęp 24/7 (dwadzieścia cztery godziny na dobę przez siedem dni w tygodniu) do aktualizacji i poprawek oprogramowania bez dodatkowych opłat, w tym opłat licencyjnych, poprzez portal producenta lub stronę www producenta lub inny, uzgodniony z Wykonawcą sposób;
- 3) możliwość dokonywania Nielimitowanej liczby zgłoszeń poprzez portal producenta lub stronę www producenta lub inny, uzgodniony z Wykonawcą sposób, w trybie 8/5 (osiem Godzin roboczych przez pięć Dni roboczych w tygodniu).”.

Ad 2

Zamawiający potwierdza, że, zgodnie z § 7 projektu umowy, Zamawiający nie nabywa prawa do kolejnych wersji, aktualizacji ani poprawek dostarczanych po zakończeniu okresu wsparcia, o którym mowa w projekcie umowy.

W związku z wątpliwościami zgłoszonymi przez Wykonawcę, Zamawiający zmienia treść § 7 ust. 1 projektu umowy, który otrzymuje brzmienie:

„1. Na podstawie Umowy, w ramach wynagrodzenia, o którym mowa w § 8 ust. 1, Wykonawca zapewni Zamawiającemu:

- 1) z chwilą podpisania protokołu odbioru, o którym mowa w § 5 ust. 1 – udzielenie niewyłącznych licencji, o których mowa w § 1 pkt 1 na dostarczone oprogramowanie wykorzystane do wdrożenia w środowisku Zamawiającego Narzędzia (dalej: „oprogramowanie”), na czas nieoznaczony dla nieograniczonej liczby użytkowników;
- 2) od momentu udostępnienia Zamawiającemu elementów oprogramowania zmienionych w ramach wsparcia producenta, w tym nowych wersji, uaktualnień, poprawek, modyfikacji, o których mowa w pkt 1 – udzielenie niewyłącznych licencji na czas nieoznaczony na wyżej wymienione elementy oprogramowania, w tym aktualizacje, nowe wersje, poprawki i modyfikacje, w okresie, o którym mowa w § 1 pkt 1,
- bez ograniczeń terytorialnych, na zasadach określonych w Umowie (dalej: „Licencje”).”.

Pytanie nr 9

Dotyczy: § 4 ust. 1–5 oraz § 6 ust. 14 projektu umowy — zakres projektu technicznego, projektu wdrożenia oraz scenariuszy testów akceptacyjnych dla gotowego produktu § 4 ust. 1–5 przewiduje opracowanie przez Wykonawcę, według szablonów przekazanych przez Zamawiającego, projektu technicznego i projektu wdrożenia Narzędzia, a § 6 ust. 14 — opracowanie planu testów akceptacyjnych i scenariuszy testowych.

Przedmiotem zamówienia jest dostawa i wdrożenie gotowego, istniejącego oprogramowania, którego uruchomienie w środowisku Zamawiającego sprowadza się do instalacji i konfiguracji komponentów (np. w oparciu o Docker Compose) oraz integracji z infrastrukturą sieciową Zamawiającego. Zakres dokumentacji projektowej oraz scenariuszy testowych adekwatny dla

wytwarzania oprogramowania na zamówienie jest niewspółmierny do dostawy gotowego produktu.

Mając na uwadze potrzebę rzetelnego oszacowania pracochłonności oferty, prosimy o doprecyzowanie:

1. jakiego poziomu szczegółowości oraz jakiego zakresu treści Zamawiający oczekuje w projekcie technicznym i projekcie wdrożenia w przypadku dostawy gotowego, istniejącego oprogramowania (czy dopuszczalne jest ograniczenie ich do dokumentacji instalacji, konfiguracji i integracji z infrastrukturą Zamawiającego);
2. czy Zamawiający potwierdza, że plan i scenariusze testów akceptacyjnych (§ 6 ust. 14) mogą obejmować wyłącznie weryfikację funkcjonalności wymaganych w OPU i zostać dostosowane do zakresu funkcjonalnego gotowego Narzędzia.

Odpowiedź

Ad 1

Zamawiający w szczególności oczekuje dokumentacji w postaci projektów, dokumentacji instalacji, konfiguracji i integracji Narzędzia z infrastrukturą Zamawiającego, instrukcji zatrzymania, uruchomienia Narzędzia, opisanie architektury Narzędzia, wymienienia zasobów infrastrukturalnych, na których Narzędzie zostanie wdrożone, wersji systemu operacyjnego. Jednocześnie Zamawiający podkreśla, że zgodnie z § 4 projektu umowy etap powstawania dokumentacji zakłada współpracę stron, wymianę uwag i prowadzenie uzgodnień w tym zakresie. Celem jest powstanie dokumentacji użytecznej dla Zamawiającego, uzupełnionej na szablonach udostępnionych przez Zamawiającego, wszędzie tam gdzie będzie to możliwe.

Ad 2

Zamawiający informuje, że plan i scenariusze testów akceptacyjnych (§ 6 ust. 14 projektu umowy) będą obejmować w szczególności weryfikację funkcjonalności wymaganych w OPU w celu ich porównania z zakresem funkcjonalnym Narzędzia. Zamawiający podkreśla, że plan i scenariusze zostaną uzgodnione przez Strony. Zamawiający lub podmiot wskazany przez Zamawiającego zgodnie z postanowieniami w Umowie przeprowadzi testy bezpieczeństwa.

Pytanie nr 10

Dotyczy: § II ust. 1 Załącznika nr 1 — parametry udostępnianego środowiska, w szczególności zasób dyskowy

Zgodnie z § II ust. 1 Załącznika nr 1 Zamawiający udostępni Wykonawcy infrastrukturę obejmującą m.in. 100 GB zasobu dyskowego.

W przypadku narzędzia opartego o modele AI należy uwzględnić rozmiary obrazów kontenerów (rzędu wielu gigabajtów), repozytorium dodawanych nagrań audio/video, bazę danych przechowującą — zgodnie z odpowiedzią na Pytanie nr 9 z dnia 29 maja 2026 r. — dane wejściowe, surową transkrypcję oraz pełną historię modyfikacji wprowadzanych przez użytkownika i metadane techniczne, a także pełne logi aktywności (§ III ust. 3 Załącznika nr 1). Łącznie może to wymagać zasobu dyskowego przekraczającego 100 GB.

Prosimy o potwierdzenie:

1. czy wskazany zasób dyskowy (100 GB) jest wartością sztywną, czy też Zamawiający dopuszcza jego zwiększenie na etapie wdrożenia, stosownie do rzeczywistego zapotrzebowania wynikającego z zaakceptowanego projektu technicznego;
2. czy zarządzanie retencją i rotacją danych (nagrań, transkrypcji, logów) w celu utrzymania zapotrzebowania na zasób dyskowy w udostępnionych granicach pozostaje po stronie Zamawiającego, czy stanowi wymaganie wobec Narzędzia.

Odpowiedź

Ad 1

Przebieg zasobu dyskowego 100 GB, wskazana w OPU dotyczy tylko i wyłącznie przestrzeni do zainstalowania Narzędzia. Przestrzeń na potrzeby transkrypcji zostanie zapewniona przez Zamawiającego w zgodzie z faktycznymi potrzebami w celu zapewnienia niezakłóconego korzystania przez Zamawiającego z Narzędzia.

Ad 2

Vide odpowiedź na pytanie nr 1.

Pytanie nr 11

§ 1. Przedmiot Umowy Przedmiotem Umowy jest: 3) realizacja przez Wykonawcę modyfikacji Narzędzia w liczbie do 160 roboczogodzin, na podstawie zleceń otrzymanych od Zamawiającego, w okresie 12 miesięcy od podpisania protokołu odbioru końcowego Narzędzia.

Pytanie: Prosimy o doprecyzowanie jakiego rodzaju modyfikacje narzędzia ma na myśli Zamawiający.

Odpowiedź

Zamawiający udzielił odpowiedzi na powyższe pytanie w piśmie z dnia 5 czerwca 2026r. (odpowiedź na pytanie nr 3).

Sławomir Flis

Dyrektor

Departamentu Informatyki

/podpisano kwalifikowanym podpisem elektronicznym/