

Znak sprawy: DZ.26.359.2025

Kraków dnia 04.12.2025 r.

Wykonawcy
strona internetowa – platforma zakupowa

<https://platformazakupowa.pl/pn/kolejemalopolskie/proceedings>

Dotyczy postępowania w celu udzielenia zamówienia pn.: **„Wykonanie przeglądu czwartego poziomu utrzymania P4 wraz z pracami dodatkowymi pojazdach serii EN78 (typ 31WE) oraz EN79 (typ 45WE)”**, prowadzonego w trybie przetargu nieograniczonego na podstawie przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. 2024 poz. 1320 z późn.zm.).

WYJAŚNIENIA I ZMIANY TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

W związku z zapytaniem dotyczącym zapisów Specyfikacji Warunków Zamówienia wniesionymi do Zamawiającego w dniu 28.11.2025 Zamawiający „Koleje Małopolskie Sp. z o.o.” w Krakowie działając na podstawie art. 135 oraz art. 137 ustawy Pzp wyjaśnia:

Pytanie 1

SWZ Rozdz. III pkt. 3.3. oraz Załącznik nr 4 do SWZ – projektowane postanowienia umowy § 24 ust. 3, pkt 3

Ponownie zwracamy się z wnioskiem o usunięcie wymogu dotyczącego złożenia oświadczenia zatrudnionego pracownika z pozostawieniem pozostałych wymogów tj. obowiązkiem przedstawienia oświadczenia wykonawcy oraz kopii umów o pracę. Oświadczenie wykonawcy oraz kopie umów są wystarczającym dowodem na spełnienie wymagań Zamawiającego. Pracodawca nie może zmusić pracowników do podpisywania dodatkowych oświadczeń.

Odpowiedź 1 WYJAŚNIENIE

Zgodnie z Odpowiedzią nr 3 z dnia 20.11.2025 Zamawiający dokonał zmiany 24 ust. 3, pkt 3, który otrzymał brzmienie:

W trakcie realizacji zamówienia na każde wezwanie Zamawiającego, w wyznaczonym w tym wezwaniu terminie jednak nie krótszym niż 10 Dni Roboczych, Wykonawca przedłoży Zamawiającemu wskazane poniżej dowody w celu potwierdzenia spełnienia wymogu zatrudnienia na podstawie umowy o pracę przez Wykonawcę lub podwykonawcę/ów osób wykonujących czynności wskazane w ust. 1 w trakcie realizacji Umowy, tj.: (...)

Powyższa treść dotyczy również Rozdz. III pkt. 3.SWZ

Pytanie 2

Załącznik nr 4 do SWZ – projektowane postanowienia umowy § 3, ust. 3e, pkt 5

Ponownie wnioskujemy o usunięcie zapisu. Pozostawienie zapisów rodzi ryzyko narzucania przez Zamawiającego sposobu/metod wykonywania przedmiotu umowy. Wnioski z audytu/kontroli mogą być wiążące dla wykonawcy tylko w przypadku ewentualnego stwierdzenia rażących naruszeń tj. wykonywania umowy niezgodnie ze sztuką.

Strona 1 z 5

ODPOWIEDŹ 2

Wskazany zapis nie odnosi się wyłącznie do obszaru cyberbezpieczeństwa

Zamawiający zmienia § 3, ust. 3e, pkt 5 PPU, który otrzymuje brzmienie

5. *Wnioski z audytu/kontroli przeprowadzonej przez Zamawiającego są wiążące dla Wykonawcy w przypadku stwierdzenia nieprawidłowości w realizacji przedmiotu umowy – w szczególności poprzez realizację prac niezgodnie z obowiązującymi przepisami, normami, standardami, dobrymi praktykami lub wymaganiami SWZ.*

Pytanie 3

Załącznik nr 8 OPZ – prace opcjonalne – praca 17

Wnoskujemy o wskazanie czy Zamawiający w ramach wymiany tapicerki zakłada wymianę samej tkaniny obiciowej, czy również gąbek/formatek siedziska i oparcia.

Odpowiedź 3 WYJAŚNIENIE

Zamawiający informuje, że ewentualna wymiana poszczególnych zużytych/wyeksplotowanych gąbek/formatek siedzisk i oparc – po weryfikacji przez Wykonawcę i potwierdzona przez przedstawiciela Zamawiającego - będzie zlecana jako zakres prac dodatkowych wykraczających poza stały zakres DSU.

Pytanie 4

W związku z udzielonymi odpowiedziami i zmianami, w szczególności w zakresie prac opcjonalnych wnoskujemy o udostępnienie zaktualizowanych załączników: Załącznik nr 7c i Załącznik nr 7d.

Odpowiedź 4 WYJAŚNIENIE

Zamawiający zmienił załączniki 7a-7d Odpowiedziami z dnia 28.11.2025

Pytanie 5

Biorąc pod uwagę szeroki zakres postępowania tj. wycena zakresu podstawowego oraz rozbudowanego zakresu opcjonalnego dla dwóch typów pojazdów wnoskujemy o zmianę terminu składania ofert na 16 stycznia 2026 r.

Odpowiedź 5 WYJAŚNIENIE:

Zamawiający zmienił termin składania ofert na dzień 16.12.2025 Odpowiedziami z dnia 28.11.2025

Pytanie 6

Załącznik nr 4 do SWZ – projektowane postanowienia umowy § 29

Ponownie zwracamy się z wnioskiem o usunięcie § 29 w całości.

Zamawiający wymaga, aby Wykonawca na etapie oferty uwzględnił i spełnił wymagania z niewdrożonych do prawa polskie dyrektyw 2022/2555 (NIS2) oraz 2022/2557 (CER), które zostaną wprowadzone do polskiego prawa w przyszłości, co prowadzi do niejednoznacznego opisu przedmiotu zamówienia i jest wymaganiem niemożliwym do spełnienia i skalkulowania.

W przypadku Rozporządzenia Parlamentu Europejskiego i Rady 2024/2847 z dnia 23 października 2024 r.

w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń nr 168/2013 i 2019/1020 i dyrektywy 2020/1828 (akt o cyberodporności) zwany dalej „CRA” podnosimy, że w okresie do grudnia 2027 roku dla produktów cyfrowych wprowadzanych na rynek obowiązuje okres przejściowy, w którym nie obowiązuje spełnienia wymagań zasadniczych wynikających z przedmiotowego aktu.

Zwracamy ponadto uwagę, że pojazdy stanowiące przedmiot umowy zostały na rynek wprowadzone przed datą publikacji stosownego rozporządzenia i jako produkty z elementem cyfrowym nie musiały w dniu wprowadzenia na rynek i nie muszą w całym cyklu życia wymagań zasadniczych spełniać.

Zważywszy na wskazany wyżej okres przejściowy informujemy, że wielu naszych dostawców produktów z elementem cyfrowym wykorzystywanych w systemach pokładowych pojazdów nie posiada opracowanych produktów w wersji spełniającej wymagania zasadnicze a według naszej najlepszej wiedzy nie istnieje techniczna możliwość migracji zabudowanych produktów z elementem cyfrowym w drodze ich aktualizacji do produktów spełniających wymagania CRA. Według najlepszej wiedzy Wykonawcy praktycznie żadne obecnie zabudowane w pojazdach produkty z elementem cyfrowym nie są kompatybilne w przód (forward compatibility) zatem nie można ich aktualizować do stanu spełniającego wymagania CRA.

Wskazujemy ponadto, że żadne z nowo opracowanych produktów z elementów cyfrowych nie jest w pełni kompatybilny wstecz (full backward compatibility) może skutkować w skrajnej sytuacji całkowitą zmiany architektury (z wyłączeniem architektury funkcjonalnej) systemów pokładowych, wymiany komponentów wszystkich systemów posiadających elementy cyfrowe czyli sterowniki systemu sterowania pojazdem TCMS, sterowniki systemu hamulcowego, sterowniki systemu napędowego, sterowniki systemu drzwiowego, sterowniki systemu HVAC, sterowniki systemu WC, sterowniki systemu ETCS, systemu rejestratora prawnego, sterowniki systemu szeroko pojętej informacji pasażerskiej, sterowniki systemu CCTV itp.

Wskazujemy ponadto, że obecnie **brak jest zasadniczych wymagań cyberbezpieczeństwa** w taborze kolejowym, co uniemożliwia określenie wymagań systemowych potencjalnym dostawcom w/w systemów.

Z braku pełnej kompatybilności wstecznej, tak postawione wymagania i wymiana większości obecnych produktów z elementem cyfrowym na produkty spełniające wymagania CRA spowoduje, iż naprawa P4 musi zostać potraktowana jako modernizacja (przez zmianę zasadniczych cech konstrukcyjnych pojazdu w myśl Rozporządzenia Wykonawczego Komisji (UE) 2023/1694 z dnia 10 sierpnia 2023 r. z późniejszymi zmianami), a tym samym spowoduje konieczność ponownej certyfikacji całego pojazdu, co w przypadku przeglądów i napraw już eksploatowanych pojazdów jest całkowicie nieuzasadnione i prowadzące do wprowadzenia do eksploatacji potencjalnie nowych typów pojazdów.

Zwracamy uwagę, że aktualne postanowienia § 29 są nieproporcjonalne do przedmiotu zamówienia oraz sprowadzają przeglądy do świadczenia niemożliwego.

Odpowiedź 6 WYJAŚNIENIE:

Zamawiający nie wyraża zgody na usunięcie § 29 i wyjaśnia poszczególne kwestie w kontekście zadanych pytań.

„Zamawiający wymaga, aby Wykonawca na etapie oferty uwzględnił i spełnił wymagania z niewdrożonych do prawa polskie dyrektyw 2022/2555 (NIS2) oraz 2022/2557 (CER), które zostaną wprowadzone do polskiego prawa w przyszłości, co prowadzi do niejednoznacznego opisu przedmiotu zamówienia i jest wymaganiem niemożliwym do spełnienia i skalkulowania”.

Zamawiający podkreśla, że wymagania wskazanych powyżej dyrektyw NIS2 i CER są znane od 3 lat i ich transpozycja do przepisów prawa krajowego winna odbyć się na zasadzie określonych wymagań minimalnych. Zamawiający nie może ignorować faktu, iż procesowanie nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa przez sejm Rzeczypospolitej, jako transpozycja w/w dyrektyw, jest zaplanowane na najbliższym posiedzeniu 3/4.12.2025. Tym samym z dużym prawdopodobieństwem odpowiednie wymagania staną się obowiązujące dla Zamawiającego na etapie realizacji umowy, jako podmiotu kluczowego.

„W przypadku Rozporządzenia Parlamentu Europejskiego i Rady 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń nr 168/2013 i 2019/1020 i dyrektywy 2020/1828 (akt o cyberodporności) zwany dalej „CRA” podnosimy, że w okresie do grudnia 2027 roku dla produktów cyfrowych wprowadzanych na rynek obowiązuje okres przejściowy, w którym nie obowiązuje spełnienia wymagań zasadniczych wynikających z przedmiotowego aktu”

Zamawiający podkreśla, że ze względu na aktualną sytuację geopolityczną, w tym nagłośnie w ostatnim czasie przez media przypadki sabotażu m.in. infrastruktury kolejowej, nie pozwalają ignorować wymagań z obszaru cyberbezpieczeństwa kolei. Wskazany przez organy UE okres przejściowy winien być wykorzystany przez podmioty kluczowe na dostosowanie ich infrastruktury do odpowiednich wymagań CRA. Bezpieczeństwo transportu pasażerskiego jest dla Zamawiającego absolutnym priorytetem. Nie ulega wątpliwości, że wskazany okres przejściowy należy inaczej traktować przez odległe z punktu widzenia konfliktu zbrojnego w Ukrainie kraje UE a zupełnie inaczej w przypadku Zamawiającego operującego bezpośrednio na obszarach kolejowych wysokiego ryzyka. Z uwagi na fakt znaczącego rozdrobnienia zarządzanej przez siebie infrastruktury kolejowej (7 różnych typów pojazdów) Zamawiający podjął decyzję o sukcesywnym dostosowaniu poszczególnych typów pojazdów do wymagań CRA niezależnie od wskazanych terminów maksymalnych.

„Zwracamy ponadto uwagę, że pojazdy stanowiące przedmiot umowy zostały na rynek wprowadzone przed datą publikacji stosownego rozporządzenia i jako produkty z elementem cyfrowym nie musiały w dniu wprowadzenia na rynek i nie muszą w całym cyklu życia wymagań zasadniczych spełniać”

Zamawiający podkreśla, że powyższa uwaga tyczy się bez wyjątku wszystkich typów pojazdów, których Zamawiający pozostaje dysponentem. Dlatego też została podjęta decyzja jak w akapicie powyżej tj. sukcesywnej poprawy cyberbezpieczeństwa pojazdów kolejowych będących w dyspozycji Zamawiającego.

„Zważywszy na wskazany wyżej okres przejściowy informujemy, że wielu naszych dostawców produktów z elementem cyfrowym wykorzystywanych w systemach pokładowych pojazdów nie posiada opracowanych produktów w wersji spełniającej wymagania zasadnicze a według naszej najlepszej wiedzy nie istnieje techniczna możliwość migracji zabudowanych produktów z elementem cyfrowym w drodze ich aktualizacji do produktów spełniających wymagania CRA. Według najlepszej wiedzy Wykonawcy praktycznie żadne obecnie zabudowane w pojazdach produkty z elementem cyfrowym nie są kompatybilne w przód (forward compatibility) zatem nie można ich aktualizować do stanu spełniającego wymagania CRA”

Zamawiający wskazuje, iż zgodnie ze standardem Cenelec CLC/TS 50701:2023 istnieją odpowiednie rekomendacje dotycząca właściwego zabezpieczenia systemów klasy legacy (tj. systemów odziedziczonych, nie spełniających odpowiednich wymagań cyberbezpieczeństwa) poprzez ich odpowiednią separację z wykorzystaniem koncepcji stref i kanałów, poddaną niezależnemu audytowi. Stosowanie w/w rekomendacji winno być jednak ograniczone wyłącznie do przypadków, gdy Wykonawca przedstawi dowodnie faktyczny i obiektywny brak możliwości uzyskania odpowiednich właściwości systemu w zakresie cyberbezpieczeństwa z wykorzystaniem odpowiedniej jego konfiguracji, aktualizacji oprogramowania bądź też wymiany na jego nowszą wersję spełniającą odpowiednie wymagania. Zamawiający podkreśla, że nie oczekuje w szczególności wymiany systemów kluczowych dla bezpieczeństwa pojazdu (np. TCMS), a których wymiana nie będzie racjonalna ze względów finansowych na obecnym etapie cyklu życia pojazdu kolejowego a przede wszystkim takiego ich zabezpieczenia w postaci poprawnej separacji, aby zapewnić odpowiedni poziom bezpieczeństwa pojazdu kolejowego jako całości – zgodnie z odpowiednimi rekomendacjami Urzędu Transportu Kolejowego.

„Wskazujemy ponadto, że żadne z nowo opracowanych produktów z elementów cyfrowych nie jest w pełni kompatybilny wstecz (full backward compatibility) może skutkować w skrajnej sytuacji całkowitą zmiany architektury (z wyłączeniem architektury funkcjonalnej) systemów pokładowych, wymiany komponentów wszystkich systemów posiadających elementy cyfrowe czyli sterowniki systemu sterowania pojazdem TCMS, sterowniki systemu hamulcowego, sterowniki systemu napędowego, sterowniki systemu drzwiowego, sterowniki systemu HVAC, sterowniki systemu WC, sterowniki systemu ETCS, systemu rejestratora prawnego, sterowniki systemu szeroko pojętej informacji pasażerskiej, sterowniki systemu CCTV itp.”

Zamawiający nie potwierdza opinii Wykonawcy. Według jego stanu wiedzy istotna część producentów komponentów cyfrowych dedykowanych w szczególności do kolei oferuje już produkty spełniające określone wymagania w zakresie cyberbezpieczeństwa, których integracja jest możliwa bez konieczności wymiany pozostałych elementów architektury teleinformatycznej pojazdu. Co więcej, do

takiej integracji nie jest wymagana pełna kompatybilność wstecz – wystarczająca jest kompatybilność na poziomie odpowiednio dostosowanych protokołów telekomunikacyjnych.

„Wskazujemy ponadto, że obecnie brak jest zasadniczych wymagań cyberbezpieczeństwa w taborze kolejowym, co uniemożliwia określenie wymagań systemowych potencjalnym dostawcom w/w systemów”

Zamawiający nie podziela opinii Wykonawcy. Zarówno norma cyberbezpieczeństwa w zakresie operational technology (OT) IEC 62443, jak i jej adaptacja na potrzeby rynku kolejowego w postaci standardu Cenelec TS/CLC 50701:2013 określa zasadnicze wymagania dotyczące cyberbezpieczeństwa m.in. taboru kolejowego. Co więcej, w najbliższym czasie przewidziana jest publikacja normy IEC 63452 będącej rozwinięciem w/w standardu Cenelec. Co więcej, według najlepszej wiedzy Zamawiającego, to właśnie te normy i standardy są uwzględniane przez producentów komponentów cyfrowych o których mowa w akapicie powyżej.

„Z braku pełnej kompatybilności wstecznej, tak postawione wymagania i wymiana większości obecnych produktów z elementem cyfrowym na produkty spełniające wymagania CRA spowoduje, iż naprawa P4 musi zostać potraktowana jako modernizacja (przez zmianę zasadniczych cech konstrukcyjnych pojazdu w myśl Rozporządzenia Wykonawczego Komisji (UE) 2023/1694 z dnia 10 sierpnia 2023 r. z późniejszymi zmianami), a tym samym spowoduje konieczność ponownej certyfikacji całego pojazdu, co w przypadku przeglądów i napraw już eksploatowanych pojazdów jest całkowicie nieuzasadnione i prowadzące do wprowadzenia do eksploatacji potencjalnie nowych typów pojazdów”

Zamawiający wskazał powyżej oczekiwaną ścieżkę spełnienia postawionych wymagań, bez konieczności zapewnienia pełnej kompatybilności wstecznej. Tym samym nie podziela opinii, że zmianie ulegną zasadnicze cechy konstrukcyjne pojazdu powodujące w konsekwencji konieczność ponownej certyfikacji pojazdów.

Treść niniejszego pisma stanowi integralną część Specyfikacji Warunków Zamówienia oraz Projektowanych postanowień umowy, znak sprawy: DZ.26.359.2025

.....
Kierownik Zamawiającego/ osoba upoważniona
do podejmowania czynności w jego imieniu |