

**WYROK**

Warszawa, 8 września 2025 roku

**Krajowa Izba Odwoławcza** - w składzie:

Przewodnicząca: Agnieszka Trojanowska  
Joanna Stankiewicz-Baraniak  
Ryszard Tetzlaff

Protokolant: Rafał Komoń

po rozpoznaniu na rozprawie, odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej 24 lipca 2025 r. przez wykonawcę Emitel spółka akcyjna z siedzibą w Warszawie, ul. F. Klimczaka 1 w postępowaniu prowadzonym przez zamawiającego – Katowickie Wodociągi spółka akcyjna z siedzibą w Katowicach, ul. Obrońców Westerplatte 89 Uczestnicy po stronie zamawiającego:

wykonawca Polkomtel Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, ul. Konstruktorska 4

wykonawca Orange Polska spółka akcyjna z siedzibą w Warszawie, Al. Jerozolimskie 160

wykonawca T-Mobile spółka akcyjna z siedzibą w Warszawie, ul. Marynarska 12

**orzeka:**

1. Oddala odwołanie,

2. Kosztami postępowania obciąża odwołującego i:

2.1. Zalicza w poczet kosztów postępowania kwotę 15 000 zł. (piętnaście tysięcy złotych zero groszy) tytułem uiszczonego wpisu, kwotę 3 600 zł 00 gr (trzy tysiące sześćset złotych zero groszy) tytułem wydatków pełnomocnika odwołującego, kwotę 3 600 zł 00 gr (trzy tysiące sześćset złotych zero groszy) tytułem wydatków pełnomocnika zamawiającego,

2.2. Zasądza od odwołującego na rzecz zamawiającego kwotę 3 600 zł 00 gr (trzy tysiące sześćset złotych zero groszy) tytułem zwrotu wydatków pełnomocnika zamawiającego.

Na orzeczenie – w terminie 14 dni od jego doręczenia przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Warszawie- Sądu Zamówień Publicznych.

Przewodnicząca:.....

.....

.....

**Sygn. akt KIO 3078/25**

**Uzasadnienie**

Postępowanie o udzielenie zamówienia, prowadzone w trybie przetargu nieograniczonego, w postępowaniu pt. „Dostawa, wdrożenie i obsługa systemu smart City w zakresie monitoringu sieci wodociągowej” ogłoszono w Dzienniku Urzędowym Unii Europejskiej numer Dz. U. S: 132/2025 458218-2025 z 14 lipca 2025 r.

24 lipca 2025 r. wykonawca Emitel spółka akcyjna z siedzibą w Warszawie, ul. F. Klimczaka 1 wniósł odwołanie przez pełnomocnika działającego na podstawie pełnomocnictwa z 18 lipca 2025 r. udzielonego przez prezesa i członka zarządu. Do odwołania dołączono dowód jego opłacenia oraz dowód przekazania zamawiającemu.

Odwołujący zarzucił zamawiającemu:

1/ naruszenie art. 99 ust. 1, 2 oraz 4 ustawy i art. 16 ust. 1 oraz ust. 3 ustawy — przez opisanie przedmiotu zamówienia w sposób, który mógłby utrudniać uczciwą konkurencję oraz równe traktowanie wykonawców, nieproporcjonalny a także w sposób niejednoznaczny i niewyczerpujący za pomocą niedostatecznie dokładnych i zrozumiałych określeń, nieuwzględniający wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty, nieproporcjonalnie do celów przetargu, z uwagi na postawienie wymogu by system musiał korzystać z komunikacji radiowej w licencjonowanych pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych (I Opis ogólny pkt. 1 Przedmiot zamówienia ppkt. 1.1 Opis Przedmiotu Zamówienia — pkt 1.1.1 OP Z) w szczególności przez:

-posłużenie się pojęciem „pasma licencjonowanego” co jest pojęciem nieznanym na gruncie ustawy Prawo komunikacji elektronicznej,

-tworzenie nieproporcjonalnych warunków dla realizacji zamówienia przez wymuszenie „licencji na pasmo” przy czym

system odczytowy można zbudować również na pasmach częstotliwości otwartych przeznaczonych w tym celu przez przepisy powszechnie obowiązującego prawa co również dopuszcza Zamawiający ale w ilości nie więcej aniżeli 100/0 lokalizacji,

-utrudnianie warunków konkurowania przez wskazanie „pasma licencjonowanego” co predysponuje do realizacji usługi operatorów mobilnych posiadających rezerwację częstotliwości a jednocześnie wyklucza innych przedsiębiorców telekomunikacyjnych mogących świadczyć usługi na rzecz zamawiającego ale nie posiadających rezerwacji częstotliwości,

-postawienie wymogu „pasma licencjonowanego dla 90 % lokalizacji, nie znajduje żadnego obiektywnego uzasadnienia ani funkcjonalnego bowiem zarówno transmisja w paśmie licencjonowanym, jak i w nalicencjonowanym ma zamawiającemu zapewnić identyczne parametry jakościowe — w tym m.in.: odczyt z co najmniej 900/0 urządzeń 24 godziny na dobę, z 950/0 raz w tygodniu, i z 980/0 raz w miesiącu. Zatem — skoro wymagania SLA są jednakowe bez względu na zastosowaną technologię transmisji, to narzucenie obowiązku stosowania pasma licencjonowanego w 90% przypadków jest nieproporcjonalne oraz prowadzi do bezpodstawnego ograniczenia konkurencji.

2/ naruszenie art. 99 ust. 1,2 oraz 4 ustawy i art. 16 ust. 1 oraz ust. 3 ustawy zw. z art. 3531 w. zw. z art. 58 par. 1 i 2 Kodeksu cywilnego — przez opisanie przedmiotu zamówienia w sposób, który mógłby utrudniać uczciwą konkurencję, wskazujący na usługi dostarczane przez konkretnych wykonawców co prowadzi do ich uprzywilejowania a także w sposób niejednoznaczny i niewyczerpujący, za pomocą niedostatecznie dokładnych i zrozumiałych określeń, nieuwzględniający wszystkich. wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty a także nieproporcjonalnie do celów przetargu, z uwagi na postawienie wymogu by system musi opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną Wykonawcy (V Infrastruktura systemu odczytowego — wymagania ogólne pkt. 1 Wymagania ogólne ppkt. 1 Opisu Przedmiotu Zamówienia — pkt V.I OPZ), w szczególności przez: - wymóg korzystania z wydzielonej podsieci APN oraz posiadania własnej infrastruktury w co najmniej 900/0 uprzywilejowuje spółkę Orange Polska S.A. jako wykonawcę, ponieważ tylko ten podmiot posiada własną infrastrukturę telekomunikacyjną mobilną na obszarze aglomeracji Katowickiej. Wyklucza pozostałych uczestników rynku, w tym wielu wykonawców posiadających kompetencje techniczne i organizacyjne do realizacji zamówienia, którzy korzystają z infrastruktury dzierżawionej lub współdzielonej (np. MVNO, integratorzy, operatorzy hurtowi lub podmioty które leasingują infrastrukturę jak P4 Sp z o.o. lub Polkomtel Sp. z o.o.). Preferuje określony model biznesowy, tj. operatorów posiadających własną sieć fizyczną, przy czym nawet ci wykonawcy nie są w stanie w pełni spełnić tego warunku.

-wymóg posiadania co najmniej 900/0 własnej infrastruktury nie został uzasadniony realnymi potrzebami zamawiającego. Dla zapewnienia niezawodnej transmisji danych istotny jest poziom SLA, bezpieczeństwo transmisji, dostępność usług czy zgodność z wymaganiami prawnymi (np. RODO), a nie własność fizycznej infrastruktury. Dopuszczenie do przetargu podmiotów korzystających z infrastruktury dzierżawionej lub współdzielonej (np. MVNO, operatorzy hurtowi) mogłoby skutkować uzyskaniem oferty bardziej konkurencyjnej cenowo, a jednocześnie spełniającej wszystkie techniczne i bezpieczeństwa wymagania.

„Podsiec APN dedykowana zamawiającemu” — brak wyjaśnienia, czy chodzi o fizycznie odseparowaną sieć, logiczną separację (np. za pomocą VPN/MPLS), czy też konfigurację w ramach standardowego APN. Nie wiadomo, czy wystarczy np. prywatny APN z tunelem IPSec czy wymagana jest fizyczna izolacja.

„W co najmniej 90% wykorzystywać własną infrastrukturę” — nie określono, co dokładnie oznacza „własna infrastruktura” — czy chodzi o fizyczne nadajniki, urządzenia końcowe, serwery, a może tylko o kanały transmisyjne? Brak kryteriów pomiaru (czy procent ma być liczony wg długości sieci, liczby lokalizacji, przepustowości?) powoduje niepewność co do sposobu oceny oferty.

-brak doprecyzowania kwestii technicznych i sposobu spełnienia wymogów (np. czy dozwolone są dzierżawy, kolokacja, redundancja u innych operatorów) może skutkować błędami w ofertach lub nieporównywalnością ofert. To z kolei może prowadzić do odrzucenia ofert nie z powodu braku jakości usług, ale błędnej interpretacji niejasnych wymagań.

-wymogi są wewnętrznie sprzeczne, z jednej bowiem strony zamawiający wymaga by wydzieloną dedykowaną zamawiającemu sieć APN charakterystyczną dla łączności mobilnej komórkowej (co powinno nastąpić w terminie 30 dni od podpisania umowy a z drugiej wszystkie urządzenia jakie dostarczają wykonawcy w 2025 roku nie muszą pracować w technologii mobilnej w 2025 roku, wykonawcy mogą dostarczyć nie więcej jak 1500 nakładek w 2025 roku a więc nie muszą dostarczać nakładek w technologii mobilnych.

3/ naruszenie art. 112 ust. 1 ustawy przez ukryte i nieproporcjonalne warunki udziału w postępowaniu, gdyż zamawiający wymaga, aby system wykorzystywał „w co najmniej 900/0 własną infrastrukturę telekomunikacyjną wykonawcy” (pkt V. 1 OPZ). W rzeczywistości jest to ukryty warunek udziału w postępowaniu, który nie został wyraźnie określony w SWZ. Zamawiający nie wykazał, że takie ograniczenie jest uzasadnione przedmiotem zamówienia. Istotą zamówienia jest zapewnienie ciągłości i bezpieczeństwa transmisji danych oraz spełnienie parametrów SLA, a nie własność fizycznej

infrastruktury. Kryteria związane z własnością sieci nie są adekwatne do celu zamówienia i prowadzą do nieuzasadnionego ograniczenia konkurencji, eliminując wykonawców, którzy mogą zapewnić pełną funkcjonalność i niezawodność systemu przy użyciu infrastruktury współdzielonej lub dzierżawionej.

Wniósł o uwzględnienie odwołania i nakazanie zamawiającemu dokonania modyfikacji treści

OPZ w następującym zakresie:

1/ Nadanie punktowi I Opis ogólny pkt. 1 Przedmiot zamówienia ppkt. 1.1 Opis Przedmiotu Zamówienia (pkt 1.1.1 OPZ) następującego brzmienia:

, 1.1 Wdrożenie oraz obsługa systemu odczytowego na terenie miasta Katowice opartego na technologii Internetu Reco (IoT) stanowiącego element smart City w zakresie monitoringu sieci wodociągowej. ~~[System musi korzystać z komunikacji radiowej w licencjonowanych pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych]~~

[[System musi wykorzystywać bezprzewodową transmisję danych przy zastosowaniu technologii zapewniającej stabilność, bezpieczeństwo i ciągłość komunikacji na całym obszarze działania zamawiającego.

Wykonawca może zastosować zarówno pasma radiowe licencjonowane, jak i nielicencjonowane — pod warunkiem zapewnienia niezawodnego działania systemu, zgodności z obowiązującymi przepisami prawa oraz spełnienia pozostałych wymagań funkcjonalnych i jakościowych określonych w OPZ.]]

2/ Nadanie punktowi V Infrastruktura systemu odczytowego — wymagania ogólne pkt. 1 Wymagania ogólne ppkt. 1 Opisu Przedmiotu Zamówienia (pkt V. 1 OPZ) następującego brzmienia:

l) Zakres zamówienia:

a. Wykonawca zobowiązuje się do wdrożenia systemu odczytowego umożliwiającego odczyt danych urządzeń pomiarowych na całym obszarze działania zamawiającego. System musi ~~opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej Zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną Wykonawcy]~~

[[wykorzystywać technologię bezprzewodowej transmisji danych zapewniającą niezawodne, bezpieczne i ciągłe przesyłanie danych, z zachowaniem wymagań określonych w niniejszym OPZ. Wykonawca może wykorzystać własną infrastrukturę telekomunikacyjną lub dostępne publiczne zasoby sieciowe, pod warunkiem zapewnienia pełnej funkcjonalności i niezależności systemu odczytowego oraz spełnienia wymagań w zakresie SLA, bezpieczeństwa danych oraz pokrycia zasięgiem.]]

b. System odczytowy musi zostać uruchomiony w ciągu 30 dni od podpisania Umowy, to obejmuje:

Udostępnienie zamawiającemu dostępu do Platformy odczytowej i aplikacji mobilnej.

Zapewnienie transmisji danych całego obszaru działania zamawiającego [[z wykorzystaniem technologii komunikacji bezprzewodowej.]]

Wyjaśnienie sposobu redakcji tekstu OPZ: 1) żądany do usunięcia tekst wykreślono oraz ujęto w nawias kwadratowy [, 2) proponowany nowy tekst pogrubiono oraz ujęto w podwójny nawias kwadratowy

Wniósł o przeprowadzenie w toku postępowania odwoławczego dowodów z dokumentów wskazanych w treści niniejszego odwołania w celu wykazania, że na rynku funkcjonują różne technologie transmisji danych z wodomierzy oraz, że odwołujący zrealizował taką sieć telekomunikacyjną transmisji danych dla spółki wodociągowej obejmującą obszar aglomeracji Wrocławia całkowicie w paśmie nielicencjonowanym.

Nadto o zasądzenie od zamawiającego kosztów postępowania odwoławczego, zgodnie z treścią art. 575 ustawy, w tym zasądzenie od zamawiającego kosztów zastępstwa prawnego.

Odwołujący wskazał, że posiada legitymację do wniesienia odwołania do Krajowej Izby Odwoławczej, zgodnie z art. 505 ust. 1 ustawy, ponieważ ma interes w uzyskaniu przedmiotowego zamówienia oraz może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy.

Odwołujący prowadzi działalność gospodarczą polegającą na m.in. świadczeniu usług transmisji danych na potrzeby zdalnych odczytów wodomierzy, dedykowanych dla przedsiębiorstw wodociągowych. Jako wykonawca, który posiada odpowiedni potencjał techniczny oraz doświadczenie w realizacji usług tego rodzaju, odwołujący ma realny interes w uzyskaniu zamówienia będącego przedmiotem postępowania.

Zamawiający opisał przedmiot zamówienia w sposób, który narusza zasady uczciwej konkurencji oraz proporcjonalności, przez sformułowanie wymagań technicznych i warunków udziału w postępowaniu w sposób nadmiernie restrykcyjny i nieadekwatny do rzeczywistego celu zamówienia. W efekcie, uniemożliwił odwołującemu złożenie oferty mimo posiadania zdolności do realizacji zamówienia, co prowadzi do ryzyka poniesienia szkody majątkowej.

Zamawiający w dokumentacji przetargowej wymaga, aby w ramach przedmiotu zamówienia wykonawca zaprojektował, wdrożył oraz obsługiwał stacjonarny system odczytowy, oparty w co najmniej 90% lokalizacji na komunikacji w pasmach radiowych licencjonowanych. Tymczasem odwołujący, jako podmiot niezależny od operatorów sieci mobilnych, nie

posiada rezerwacji częstotliwości (licencji na użytkowanie pasma), co wyklucza jego możliwość uczestnictwa w postępowaniu mimo dysponowania technologią zdolną do spełnienia wszystkich wymagań jakościowych i funkcjonalnych zawartych w OPZ, w tym dotyczących poziomu SLA.

Taki sposób sformułowania wymagań prowadzi do uprzywilejowania określonej grupy wykonawców — operatorów mobilnych — oraz ogranicza dostęp do zamówienia podmiotom oferującym alternatywne, lecz równoważne technologicznie rozwiązania. Kwestionowane postanowienia dokumentacji przetargowej mają zatem charakter dyskryminacyjny i skutkują ograniczeniem konkurencji.

Odwołujący jest podmiotem uprawnionym do skorzystania ze środków ochrony prawnej, o których mowa w Dziale IX ustawy Prawo zamówień publicznych, w tym wniesienia odwołania.

Odwołujący przytoczył treść art. 16, 99 ust 1, 2 4 oraz art. 112 ust. 1 ustawy, a także art. 353(1) i 58 par. 1 i 2 kc.

Sporządzenie opisu przedmiotu zamówienia jest jedną z najważniejszych czynności związanych z przygotowaniem postępowania o udzielenie zamówienia publicznego.

Czynność ta stanowi jednocześnie obowiązek zamawiającego, ale i jego uprawnienie, bowiem zamawiający opisując przedmiot zamówienia odzwierciedla swoje rzeczywiste potrzeby, które chce zaspokoić przez udzielenie zamówienia publicznego.

W ramach rozważań natury ogólnej, pamiętać trzeba, że opisu przedmiotu zamówienia w postępowaniu o udzielenie zamówienia publicznego dokonuje wyłącznie zamawiający - stosownie do swoich potrzeb. Może tego dokonać przez opisanie parametrów technicznych przedmiotu zamówienia. Taki opis obowiązuje w sposób równy i obiektywny wszystkich wykonawców, którzy są zainteresowani udziałem w danym postępowaniu o udzielenie zamówienia publicznego.

Zamawiający, działając w granicach określonych przepisami prawa, ma prawo sprecyzować przedmiot zamówienia o określonych minimalnych standardach jakościowych i technicznych. Takie standardy zostały określone w OPZ oraz SWZ dla dostarczonych Modułów radiowych 10T które mają zapewnić rejestrację danych i przekazanie danych do Systemu odczytowego za pomocą transmisji danych. Zaliczyć do nich można m.in.: konieczność szyfrowania przekazywanych danych, zapewnienie terminowego dostarczenia danych z wodomierzy, zapewnienie odpowiedniej żywotności baterii urządzeń. Niezależnie jakim standardem transmisji danych postuluje się będą wykonawcy i dostarczone przez nich Moduły radiowe IoT muszą zgodnie z pkt. V ppkt. 5 spełniać restrykcyjne wymogi dotyczące SLA które nie może być mniejsze niż:

- (a) 90% objętych nim modułów radiowych 10T -1 raz w ciągu doby.
- (b) 95% objętych nim modułów radiowych IoT -1 raz na 7 dni kalendarzowych.
- (c) 98% objętych nim modułów radiowych IoT - przynajmniej 1 raz w miesiącu.

Zamawiający nie różnicuje parametrów SLA względem różnych Modułów radiowych IoT wykorzystywanych w ramach zamówienia. Zarówno Moduły radiowe IoT pracujące w paśmie nielicencjonowanym jak i pracując w paśmie licencjonowanym muszą spełnić postawiony standard.

Pomimo tego, że zamawiający przyjął, że każdy z tych standardów transmisji spełnia standard jakościowy lub techniczny (wymogi jakościowe dla różnych standardów transmisji danych nie zostały zróżnicowane) to zastrzegł że Moduły radiowe IoT postępujące się transmisją danych w paśmie nielicencjonowanym nie mogą stanowić więcej niż 10% wszystkich zamontowanych Modułów radiowych IoT (zob. Opis ogólny pkt. 1 Przedmiot zamówienia ppkt. 1.1 OPZ). Stan taki jest niezrozumiały skoro odwołujący będzie dysponował produktem spełniającym wymogi zamawiającego ale pracującym w „paśmie nielicencjonowanym” to nie powinno się tworzyć jakichkolwiek ograniczeń w kontraktowaniu wobec takiego produktu gdyż stanowi to naruszenie zasad uczciwej konkurencji. Naruszenie bowiem zasady uczciwej konkurencji zachodzi w takich przypadkach gdy tworzy się ograniczenia wobec oferenta mimo że jego produkt lub usługa odpowiadają potrzebom przetargu zarówno co do jakości, funkcjonalności, czy też wymaganych parametrów technicznych (tak wyrok KIO z dnia 12 listopada 2008 r., sygn. akt KIO/UZP 1155/08).

Samo zestawienie wymogów SWZ z jednej strony wymogów jakościowych w tym SLA które ma spełnić każdy Moduł radiowy IoT niezależnie jaką postuluje się transmisją danych (niezależnie czy działa w paśmie licencjonowanych czy też nie) przy jednoczesnym ograniczeniu że Moduły radiowe IoT postępujące się transmisją danych w paśmie nielicencjonowanym mają stanowić nie więcej jak 10% dostawy tworzy stan uprawdopodobnienia, że przedmiot zamówienia utrudnia uczciwą konkurencję.

Na zamawiającym ciąży obowiązek udowodnienia braku naruszenia przepisów w opisie przedmiotu zamówienia, co wynika z ugruntowanej linii orzecznictwa Krajowej Izby Odwoławczej (tak wyrok KIO z 18 listopada 2008 r., sygn. akt KIO/UZP 1240/08). Odwołujący natomiast ma obowiązek uprawdopodobnić, że wymagania zamawiającego odnoszące się do przedmiotu zamówienia mogą utrudnić uczciwą konkurencję. To na zamawiającym ciąży obowiązek dowiedzenia, że nie utrudnił on uczciwej konkurencji (tak wyrok KIO z 02 sierpnia 2008 r., sygn. akt UZP/ZO/0-943/07).

Pomimo że to na zamawiającym ciąży ciężar dowodu w dalszej części odwołania odwołujący wykaże że całe rozległe

sieci zdalnego odczytu wodomierzy wyposażone wyłącznie Moduły radiowe IoT pracujące w pasmach nielicencjonowanych mogą dać zamawiającemu jakość usługi wyższą aniżeli wymaga w postępowaniu co stawia je jako rozwiązania techniczne nowoczesne i powszechnie stosowane w kontekście odczytu wodomierzy. Nie bez znaczenia jest również że rozwiązanie pracujące w pasmach nielicencjonowanych są rozwiązaniami znacznie tańszymi we wdrożeniu w porównaniu w do rozwiązań pracujących w pasmach licencjonowanych. Skoro wykonawcy muszą kalkulować wielomilionowe opłaty za „licencje pasma”. Opis dostępnych technologii zdalnego odczytu wodomierzy przedstawia Opracowanie eksperckie sporządzone przez mgr inż. P.Z. Prezesa Zarządu Krajowego Stowarzyszenia Budowniczych Telekomunikacji.

Dowód: Opracowanie eksperckie sporządzone przez mgr inż. P.Z. Prezesa Zarządu Krajowego Stowarzyszenia Budowniczych Telekomunikacji. Eksperta rynku telekomunikacyjnego, legitymujący się uprawnieniami budowlanymi w telekomunikacji do projektowania i kierowania robotami budowlanymi w specjalnościach instalacyjnych w telekomunikacji Przewodowej wraz infrastrukturą towarzyszącą w zakresie linii, instalacji i urządzeń liniowych i stacyjnych. Nr uprawnień budowlanych: 0994/ 98/ U.

Dodatkowo w przypadku w którym właściciele zamawiającego tj. samorząd dopuściłby instalacji urządzeń stacji bazowych (urządzeń telekomunikacyjnych odbierających sygnały z Modułów radiowych IoT) na obiektach samorządu np. dachach szkół, szpitali lub urzędów za odpłatnością samorząd mógłby uzyskać dodatkowe korzyści we wdrożeniu tego rozwiązania.

Ograniczenia postanowione przez zamawiającego są istotne i mogą mieć istotny wpływ na wynik postępowania dlatego odwołujący zdecydował o skierowaniu odwołania do Izby (art. 554 ust. 1 pkt 1 ustawy). Odwołanie służy konwalidacji sprzecznych z prawem czynności zamawiającego, które stają na drodze wykonawcom podczas ubiegania się o zamówienie publiczne.

Kluczowe postanowienie SWZ kwestionowane przez odwołującego będzie bowiem punktem wyjścia dla opisu poszczególnych zarzutów.

Zgodnie z pkt. I Opis ogólny pkt. 1 Przedmiot zamówienia pkt. 1.1 Opis Przedmiotu Zamówienia

1.1 Wdrożenie oraz obsługę systemu odczytowego na terenie miasta Katowice opartego na technologii Internetu Rzeczy (IoT) stanowiącego element smart City w zakresie monitoringu sieci wodociągowej. System musi korzystać z komunikacji radiowej w licencjonowanych Pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych.

Zgodnie natomiast pkt. V Infrastruktura systemu odczytowego — wymagania ogólne pkt. 1 Wymagania ogólne ppkt. 1 Opisu Przedmiotu Zamówienia

1 / Zakres zamówienia.

- a/ Wykonawca zobowiązuje się do wdrożenia systemu odczytowego umożliwiającego odczyt danych urządzeń pomiarowych na całym obszarze działania zamawiającego. System musi opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną Wykonawcy.

b/ System odczytowy musi zostać uruchomiony w ciągu 30 dni od podpisania Umowy, co obejmuje:

- Udostępnienie Zamawiającemu dostępu do platformy odczytowej i aplikacji mobilnej.

- Zapewnienie transmisji danych całego obszaru działania zamawiającego.

Zarzut nr. 1

I/ Zamawiający dokonał ograniczenia grupy usługodawców przez wskazanie, że będzie się kontraktował tylko z przedsiębiorcami którzy w 90% instalacji wykorzystają Moduły radiowe IoT pracujące w paśmie licencjonowanym.

Nie jest jasne co należy rozumieć przez pojęcie „licencjonowanego pasma”. Pojęcie licencji to określenie występujące w prawie własności intelektualnej oraz w publicznym prawie gospodarczym. W prawie własności intelektualnej licencja stanowi upoważnienie do korzystania z cudzego dobra niematerialnego. W publicznym prawie gospodarczym jest to jeden z instrumentów reglamentowania działalności gospodarczej. Pojęcie to nie jest znane ustawie Prawo komunikacji elektronicznej. Na gruncie ustawy Prawo komunikacji elektronicznej uprawnienie do wyłącznego wykorzystania pasma częstotliwości określanej jest rezerwacją częstotliwości. Zgodnie bowiem z przepisem art. 82 ust. ustawy z dnia 13 lipca 2024 roku Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 dalej również „Pke”), Prezes UKE "daje decyzję w sprawie rezerwacji częstotliwości w terminie 6 tygodni od dnia złożenia wniosku przez podmiot ubiegający się o rezerwację częstotliwości,

Nie wszyscy przedsiębiorcy telekomunikacyjni dysponują jednak takimi licencjami (rozumianymi jako rezerwacje częstotliwości). Takimi rezerwacjami dysponują spółki: Polkomtel Sp z o.o. (również podmiot zależny), Orange Polska SA, T-Mobile Polska SA oraz P4 Sp. z o.o. („dalej również „Operatorzy mobilni” lub „Operatorzy komórkowi”) o czym stanowi informacja o zajętości pasma 800 / 900 MHz prezentowana przez Prezesa Urzędu Komunikacji Elektronicznej.

Rezerwacjami częstotliwości dysponuje również odwołujący ale nie w zakresach które są przeznaczone dla zdalnego

odczytu z Modułów radiowych IoT.

Dowód: Wydruk strony UKE zajętości pasma 800 MHz oraz Pasma 900 MHz. – odwołujący wkleił grafikę obrazującą rezerwację pasma: Zajętość częstotliwości w zakresie 880 - 915 MHz i 925 • 960 MHz przez P4 spółka z ograniczoną odpowiedzialnością, Polkomtel spółka z ograniczoną odpowiedzialnością, T-Mobile spółka akcyjna i Orange spółka akcyjna oraz Zajętość częstotliwości w zakresie 791-821 MHz i 832-862 MHz przez Orange spółka akcyjna, P4 spółka z ograniczoną odpowiedzialnością, T-Mobile spółka akcyjna oraz wskazanie na planowaną procedurę selekcyjną.

Warunek udziału w postępowaniu opisany przez zamawiającego ogranicza znacząco krąg potencjalnych wykonawców mogących ubiegać się o udzielenie zamówienia.

Jednocześnie, ograniczenie to nie znajduje obiektywnego uzasadnienia w potrzebach zamawiającego.

Potrzebą zamawiającego jest bowiem by otrzymywał terminowo dane o określonej jakości. Narzucona przez zamawiającego struktura technologiczna — 90% transmisji w paśmie licencjonowanym — wyklucza elastyczne i efektywne modele realizacji zamówienia, które są wykorzystywane przez wielu profesjonalnych wykonawców systemów IoT dla wodociągów.

Przykładem może być wykonawca, który:

1/ w pierwszym roku obowiązywania umowy wykorzystuje karty SIM operatora mobilnego, zapewniając pełną zgodność z wymogami SLA w oparciu o pasmo licencjonowane (np. NB-IoT, LTE-M),

2/ w drugim roku buduje własną sieć odczytową w paśmie nielicencjonowanym (np. LoRaWAN), co pozwala na organicznie korzystania z abonamentów SIM operatora mobilnego wdrożenie konkurencyjnej sieci względem operatora mobilnego na obszarze danej aglomeracji.

Taki model działania — określany mianem sieci hybrydowej — pozwala wykonawcy osiągnąć wysoką niezawodność, optymalizując jednocześnie koszty eksploatacji, co przekłada się na niższą cenę oferty i oszczędności po stronie zamawiającego w całym okresie obowiązywania umowy.

Rozwiązanie to:

1/ spełnia wszystkie wymagania OPZ, w tym SLA, szyfrowanie danych i czas odczytu,

2/ umożliwia zamawiającemu realizację inwestycji z większą kontrolą kosztów i bez uzależniania od stałych opłat za transmisję do operatora,

3/ jest z powodzeniem wykorzystywane w innych miastach i projektach wodociągowych, gdzie sieć prywatna (np. LoRaWAN) współdziała z usługą SIM w ramach jednego systemu odczytowego.

Tymczasem aktualna treść OPZ całkowicie eliminuje taką możliwość, pozbawiając wykonawców swobody w projektowaniu architektury sieci, mimo że to właśnie wiedza i doświadczenie wykonawcy powinny decydować o doborze środków technicznych, pozwalających osiągnąć wymagane przez zamawiającego efekty w najtańszy sposób.

W świetle powyższego, narzucony przez zamawiającego model transmisji:

1/ nie ma charakteru proporcjonalnego do celu zamówienia, jakim jest zapewnienie odczytów z urządzeń pomiarowych w zadanym czasie i z określoną jakością (SLA),

2/ narusza zasadę uczciwej konkurencji, ponieważ wyklucza wykonawców stosujących inne, równoważne — a niekiedy nowocześniejsze — technologie,

3/ prowadzi do nadmiernego uprzywilejowania operatorów mobilnych, co skutkuje zawężeniem rynku oraz ryzykiem nieuzasadnionego wzrostu ceny.

Zamawiający nie wykazał, że tylko zastosowanie transmisji w 90% przypadków w paśmie licencjonowanym jest jedyną drogą do osiągnięcia celów zamówienia. Wręcz przeciwnie — opis przedmiotu zamówienia powinien pozwalać na zastosowanie różnych modeli transmisji, pod warunkiem, że spełnią one identyczne, określone w OPZ wymagania funkcjonalne.

Cel zamówienia może również przeciwieństwo spełnić model w którym 50% przypadków instalacji modułów radiowych IoT będzie pracować w paśmie licencjonowanym a 50% przypadków instalacji modułów radiowych IoT będzie pracować w paśmie nielicencjonowanym.

Odwołujący wskazał, że dysponuje własną, rozległą infrastrukturą transmisji danych opartą wyłącznie na technologii pracującej w paśmie nielicencjonowanym, działającą w modelu LoRaWAN na całym obszarze aglomeracji wrocławskiej, obejmującej zarówno teren miasta Wrocław, jak i przyległe gminy.

Co istotne, sieć ta obsługuje aktualnie projekt wdrożony na zlecenie Miejskiego Przedsiębiorstwa Wodociągów i Kanalizacji we Wrocławiu (MPWiK Wrocław), realizowany w ramach przetargu publicznego, którego skala — mierzona liczbą urządzeń pomiarowych przekracza zakres objęty tym postępowaniem prowadzonym przez Katowickie Wodociągi S.A. aktualnie obejmuje ponad 60.000 Modułów radiowych IoT.

W ramach tej inwestycji odwołujący zainstalował i z powodzeniem utrzymuje w działaniu infrastrukturę zdalnego odczytu wodomierzy wykorzystującą wyłącznie pasmo nielicencjonowane, która:

1/ spełnia wymogi SLA określone przez MPWiK Wrocław,

2/ uzyskuje parametry wyższe niż wymagane obecnie przez Katowickie Wodociągi S.A., w każdym z wymaganych kategorii częstotliwości odczytu danych oraz dostępności transmisji.

Na dowód skuteczności technologii wykorzystywanej przez odwołującego oraz potwierdzenia jakości świadczenia usług, odwołujący przedstawił zrzut z systemu obejmujący jeden z ostatnich miesięcy świadczenia usługi oraz protokół przyjęcia usługi przez MPWiK Wrocław.

Przedstawione dowody, które potwierdzają:

1/ skuteczność realizacji usługi w paśmie nielicencyjny np. w sieci LoRaWAN

2/ osiąganie parametrów transmisji danych znacząco lepszych niż wymagane przez zamawiającego (co przekracza wymagania OPZ Katowickich Wodociągów),

3/ oraz pełne bezpieczeństwo i niezawodność rozwiązania.

W świetle powyższego brak uzasadnienia dla ograniczania udziału technologii pracujących w paśmie nielicencjonowanym do poziomu 10% w tym postępowaniu, skoro odwołujący dowodzi, że całościowe wdrożenie w takiej technologii:

1/ jest możliwe,

2/ zostało już zrealizowane z sukcesem u innego dużego zamawiającego sektora wodociągowego dla sieci znacznie większej aniżeli organizuje zamawiający

3/ i zapewnia wyższy poziom jakości transmisji niż wymagany obecnie.

Stanowi to dowód na brak proporcjonalności i obiektywnego uzasadnienia technicznego dla obecnych wymagań zamawiającego, jak również naruszenie zasady uczciwej konkurencji przez wykluczenie rozwiązań, które spełniają— a nawet przewyższają— oczekiwania techniczne wskazane w OPZ.

Dowód: Informacja systemu obejmujący jeden z ostatnich miesięcy świadczenia usługi oraz. protokół przyjęcia usługi MPWiK Wrocław (Tajemnica Przedsiębiorstwa Emitel S.A. wyłącznie do wiadomości Krajowej Izby Odwoławczej oraz zamawiającego),

Przekładając powyższą argumentację na grunt przepisów ustawy wskazać należy, że zamawiający nie może naruszać reguł, o których mowa w art. 99 ust. 1, 2 i 4 ustawy, ale też nie może być zmuszony nabywać świadczenia, które nie odpowiada jego uzasadnionym potrzebom. Istotne znaczenie ma w tym zakresie ocena, co jest potrzebą uzasadnioną.

W Świetle wymogów usługi jest to jakość dostarczanych danych oraz terminowości ich dostarczenia. Tworzenie wymogów co do licencjonowanego pasma w jakim mają pracować Moduły radiowe IoT mimo że w paśmie nielicencjonowanym również należy wypełnić takie same wymogi jakości i terminowości dostarczenia danych (a nawet znacznie lepsze) jest nieproporcjonalne oraz narusza warunki konkurowania dla przedsiębiorców którzy takich licencji (rezerwacji częstotliwości) nie posiadają. Postawiony wymóg by Moduły radiowe IoT pracowały w paśmie licencjonowanym nie skutkuje brakiem możliwości zrealizowania uzasadnionych potrzeb zamawiającego które sprowadzają się do jakości danych oraz terminowości ich dostarczenia.

Powyższą argumentację dotyczącą opisu przedmiotu zamówienia potwierdza także orzecznictwo Krajowej Izby Odwoławczej: wyrok KIO z dnia 18 listopada 2008r., sygn. akt KIO/UZP 1240/08.

Dodatkowo należy wskazać, że znane są wcześniejsze praktyki zamawiających w zakresie organizacji zamówień publicznych na Świadczenie usług transmisji danych z wodomierzy, które w sposób systemowy faworyzują dotychczasowych wykonawców, dysponujących już istniejącą infrastrukturą telekomunikacyjną którą to infrastrukturę inni przedsiębiorcy musieli by dopiero zbudować. Przykładowo, w postępowaniu prowadzonym przez Miejskie Wodociągi i Kanalizacja w Bydgoszczy sp. z o.o., ww. zamawiający w dokumentacji przetargowej wskazał na potrzebę uruchomienia sieci transmisji danych w terminie 30 dni od podpisania umowy, co — biorąc pod uwagę czasochłonność procesu budowy infrastruktury — de facto uniemożliwiało innym wykonawcom zaprojektowanie i wdrożenie własnej niezależnej sieci transmisji danych (np. w paśmie nielicencjonowanym). Pomimo tego wymogu, w praktyce nie doszło do żadnej instalacji urządzeń odczytowych a takim terminie 30 dni od dnia podpisania umowy a samo postępowanie przetargowe prowadzone było przewlekle i trwało ponad rok czasu. Takie działanie ww. zamawiającego należy ocenić jako instrumentalne — termin został sformułowany nie po to, aby wymusić realne działanie, lecz aby wykluczyć potencjalnych nowych wykonawców, nieposiadających uprzednio wdrożonej infrastruktury ani dostępu do pasm licencjonowanych operatorów. Z powodu nieadekwatnych wymagań wykluczony z tego postępowania przetargowego został min. Emitel SA, a okoliczności złożonych deklaracji o potrzebie niezwłocznego uruchomienia sieci telekomunikacyjnej (deklarowanymi min. w SWZ lub przed postępowaniem przed KIO sygn. KIO 32/24) a faktycznymi terminami realizacji zamówienia stały się przedmiotem kontroli Prezesa Urzędu Zamówień Publicznych, na wniosek wykluczonej spółki.

Przykład ten obrazuje, że niektóre zamówienia publiczne są formułowane w oparciu o rzekome potrzeby techniczne i organizacyjne, które w praktyce nie znajdują odzwierciedlenia w realizacji usługi, co prowadzi do faktycznego ograniczenia konkurencji i naruszenia zasady równego traktowania wykonawców, wynikającej z art. 16 ust. 1 i 3 ustawy.

Dowód: Kopia wniosku o przeprowadzenie kontroli wraz załącznikami.

Dlatego odwołanie w zakresie powyższego zarzutu powinno zostać uwzględnione a w konsekwencji zamawiający powinien zostać zobowiązany do dokonania modyfikacji SWZ i OPZ zgodnie z żądaniem odwołującego w pkt. II ppkt. I i 2. Zarzut nr. 2

Zamawiający w rozdziale V „Infrastruktura systemu odczytowego — wymagania ogólne”, pkt 1 ppkt 1 OPZ określił, że:

„System musi opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną Wykonawcy.

Wymóg ten jest sformułowany w sposób:

- niejednoznaczny (brak definicji, pomiaru i odniesień technicznych),
- nieproporcjonalny do celu zamówienia (gwarancji SLA, bezpieczeństwa i dostępności danych),
- diskryminujący, ponieważ uprzywilejowuje wykonawców posiadających własną fizyczną sieć — de facto ograniczając możliwość udziału w postępowaniu do 1—2 konkretnych operatorów komórkowych, jak Orange Polska S.A. lub T-mobile SA

#### 1. Faworyzowanie konkretnego modelu działalności i wykonawcy

Wskazanie, że 900/0 transmisji danych musi odbywać się w oparciu o własną infrastrukturę telekomunikacyjną Wykonawcy, w praktyce preferuje podmioty działające jako operatorzy infrastrukturalni (MNO — Mobile Network Operator), a nie integratorzy, MVNO, dostawcy rozwiązań hybrydowych czy operatorzy hurtowi.

Na obszarze aglomeracji katowickiej w praktyce wyłącznie Orange Polska S.A. lub T-Mobile SA dysponuje pełnym, własnym, fizycznym zapleczem telekomunikacyjnym umożliwiającym spełnienie warunku dosłownego „własności infrastruktury” w rozumieniu SWZ. Pozostali uczestnicy rynku, mimo posiadania wiedzy, zaplecza technologicznego oraz zdolności do realizacji SLA, korzystają z rozwiązań:

- kolokacyjnych,
- dzierżawionych,
- infrastruktury współdzielonej (np. NetWorks!, P4 Sp z o.o., czy Polkomtel Sp z o.o.) lub
- nowoczesnych systemów prywatnych sieci LoRaWAN z zapewnieniem zgodności z RODO i wysokimi parametrami dostępności.

W efekcie opisana konstrukcja zamówienia prowadzi do niedopuszczalnego uprzywilejowania określonych wykonawców, co w świetle art. 99 ust. 4 ustawy stanowi niedopuszczalne ograniczenie konkurencji.

Dowód: Artykuł strony internetowej pt: „Play sprzedał infrastrukturę pasywną za 6, 7 mld zł” (Wirtualne Media), Artykuł ze strony internetowej: „Spółka Z.S. za miliardy złotych sprzeda maszty i wieże Polkomtela Hiszpanom (Business Insider)

Obie transakcje to element szerszego trendu outsourcingu infrastruktury pasywnej do wyspecjalizowanych podmiotów, pozwalający operatorom mobilnym skupić się na usługach, rozwijając jednocześnie swoje sieci dzięki długoterminowym umowom serwisowym. Nie jest więc konieczne by przedsiębiorca telekomunikacyjny dysponował własną infrastrukturą jeżeli chce świadczyć usługi mobilne.

#### 2. Brak jasności pojęć: APN i „własna infrastruktura”

Pojęcia użyte przez zamawiającego nie są zdefiniowane i pozostają nieprecyzyjne, co utrudnia jednoznaczne przygotowanie oferty. W szczególności:

- „Podsieć APN dedykowana zamawiającemu” — nie wiadomo, czy chodzi o: o fizycznie wydzielony kanał transmisyjny, o prywatny APN z tunelem VPN lub IPSec, o czy może tylko logiczną separację (np. warstwa MPLS w sieci operatora), o oraz kto ma być właścicielem takiego APN i kto ma go utrzymywać.

„Własna infrastruktura telekomunikacyjna” — nie wyjaśniono:

- czy chodzi o stacje bazowe, punkty dostępu, urządzenia końcowe, sieć rdzeniową, serwery, transmisję danych, czy inny zasób, o jak ma być mierzony 90% udział — wg liczby lokalizacji, liczby pakietów, objętości danych, czasu pracy urządzeń, czy może wg zasięgu sieci.

Brak tych definicji uniemożliwia wykonawcom obiektywną ocenę, czy spełniają warunki techniczne, a tym samym — narusza zasadę przejrzystości oraz jednoznaczności opisu przedmiotu zamówienia (art. 99 ust. 1 Ustawy, art. 16 ust. 2 Ustawy).

#### 3. Niezgodność z celem i funkcją zamówienia (brak proporcjonalności)

Zgodnie z art. 99 ust. 2 oraz art. 16 ust. 3 ustawy, wymagania zamawiającego powinny być proporcjonalne do celu zamówienia, którym w tym przypadku jest zapewnienie:

- nieprzerwanego odczytu danych z urządzeń pomiarowych,
- niezawodnej dostępności danych tzw. odpowiedniego poziomu SLA (określonego w OPZ),
- bezpieczeństwa transmisji (np. szyfrowanie, RODO),

Wszystkie te cele mogą zostać osiągnięte również przy wykorzystaniu infrastruktury współdzielonej lub dzierżawionej, a także przy zastosowaniu modeli hybrydowych (np. połączenie NB-IoT i LoRaWAN), które nie wymagają własności

fizycznej infrastruktury. To nie własność sieci przesądza o jakości transmisji, ale jej dostępność, architektura, redundancja i umowy pomiędzy operatorami telekomunikacyjnymi.

Jednocześnie APN jest pojęciem wyłącznie stosowanym w sieciach komórkowych. Technologia APN jest stosowana wyłącznie w sieciach GSM/LTE i nie znajduje żadnego technicznego zastosowania w rozwiązaniach LPWAN pracujących w paśmie nielicencjonowanym. W takich technologiach transmisja odbywa się niezależnie od operatorów komórkowych i nie wymaga kart SIM, punktów APN ani infrastruktury GSM. Narusza tym samym zasadę uczciwej konkurencji, ograniczając dostęp do postępowania podmiotom, które wykorzystują inne rozwiązania nieoparte o rozwiązania operatorów GSM wykorzystujące pasma nielicencjonowane.

Zamawiający nie wykazał w dokumentacji, dlaczego tylko własna sieć wykonawcy może zapewnić oczekiwaną jakość, co jest wymagane zgodnie z art. 99 ust. 4 ustawy i stanowi naruszenie zasady proporcjonalności.

4. Sprzeczność wewnętrzna i brak wykonalności wymogu Postanowienia OPZ są wewnętrznie sprzeczne, gdyż:

• wymagają uruchomienia systemu z dedykowanym APN w ciągu 30 dni od podpisania umowy, jednocześnie dopuszczają, że w 2025 roku mogą zostać dostarczone tylko urządzenia działające w paśmie nielicencjonowanym, co nie wymaga żadnego APN ani własnej infrastruktury operatora mobilnego (Zob. załącznik do OPZ dotyczący harmonogramu dostaw w 2025 roku zamawiający przewiduje dostawę 1500 nakładek a więc tylko 6,25 % z zakładanych dostaw. Tym samym oznacza że cały 2025 rok można dostarczać nakładki wyłącznie w technologii w paśmie nielicencjonowanym). Jednocześnie w paśmie nielicencjonowanym nie ma możliwości utworzenia APN bo to jest technologia właściwa dla sieci GSM w której pracują karty sim.

Tym samym:

• część wymogu jest zbędna na etapie realizacji pierwszych dostaw, pozostała część (90% transmisji przez sieć własną) jest nieweryfikowalna i technicznie nieprzejrzysta.

Wykonawcy nie mają podstaw do prawidłowego zaplanowania architektury rozwiązania, co skutkuje realnym ryzykiem błędnej interpretacji, złożenia nieporównywalnych ofert, a w konsekwencji — odrzucenia ofert nie z uwagi na jakość, ale niejasność dokumentacji.

Zarzut 3

Zamawiający naruszył art. 112 ust. 1 ustawy Prawo zamówień publicznych, określając w sposób nieproporcjonalny i de facto ukryty warunek udziału w postępowaniu, przez wymaganie, aby system wykorzystywał „w co najmniej 90% własną infrastrukturę telekomunikacyjną Wykonawcy” (pkt V. 1 OPZ). W rzeczywistości, choć wymaganie to nie zostało formalnie ujęte jako warunek udziału w postępowaniu w sekcji SWZ przeznaczonej na ich przedstawienie, ma ono charakter eliminacyjny i wpływa bezpośrednio na możliwość skutecznego ubiegania się o zamówienie przez większość potencjalnych wykonawców. Takie postanowienie pełni funkcję warunku udziału ponieważ przesądza o możliwości technicznego zrealizowania zamówienia — a nie zostało wprost wskazane w SWZ w części przewidzianej dla takich warunków. Tym samym doszło do naruszenia zasad transparentności, przejrzystości i uczciwej konkurencji. Wymóg posiadania 90% własnej infrastruktury telekomunikacyjnej nie został uzasadniony realnymi potrzebami przedmiotowymi. Zamawiający nie wykazał, że tylko własność fizycznej infrastruktury — rozumiana jako sieć będąca wyłączną własnością wykonawcy — jest niezbędna dla osiągnięcia zakładanych parametrów SLA, ciągłości przesyłu danych czy zgodności z wymogami prawnymi (w tym RODO).

Co więcej, sama definicja „własnej infrastruktury” nie została zdefiniowana — nie wiadomo, czy chodzi o urządzenia końcowe, łącza transmisyjne, stacje bazowe, czy też całość elementów sieciowych, a także w jaki sposób liczony jest próg 90% — np. względem liczby lokalizacji, długości trasy przesyłowej, objętości danych czy czasu pracy sieci. Brak tych wyjaśnień skutkuje tym, że wymaganie to nie pozwala wykonawcom na rzetelną ocenę, czy są w stanie spełnić wymogi zamawiającego, a tym samym uniemożliwia im udział w postępowaniu.

Taki sposób sformułowania wymogu narusza także zasadę proporcjonalności, ponieważ cel zamówienia — tj. zapewnienie ciągłej, bezpiecznej transmisji danych w systemie smart City — może zostać w pełni osiągnięty również przy zastosowaniu infrastruktury współdzielonej, dzierżawionej lub hybrydowej, np. w modelach MVNO, LoRaWAN czy NB-IoT, które gwarantują odpowiedni poziom SLA i bezpieczeństwa transmisji, bez konieczności posiadania infrastruktury na własność.

W efekcie, wymaganie to prowadzi do nieuzasadnionego zawężenia kręgu potencjalnych wykonawców i preferuje wyłącznie operatorów infrastrukturalnych, którzy de facto jako jedyni spełniają literalnie postawione przez zamawiającego wymagania. Pozostali wykonawcy, mimo że są w stanie zapewnić pełną funkcjonalność i niezawodność systemu, zostają z postępowania wykluczeni.

Odwołujący podkreślił, że na zamawiającym ciąży obowiązek wykazania, że określone wymagania są proporcjonalne do przedmiotu zamówienia (wyrok KIO z 18.11.2008 r., sygn. akt KIO/UZP 1240/08). W przypadku braku takiego wykazania — co ma miejsce w tym postępowaniu — odwołujący uznał, że wymaganie to stanowi naruszenie art. 112 ust. 1 ustawy.

W konsekwencji, powyższe postanowienie OPZ powinno zostać zmodyfikowane w sposób, który nie ogranicza

konkurencji, a jednocześnie pozwala na osiągnięcie celów zamówienia, tj. zapewnienie jakości, bezpieczeństwa i ciągłości przesyłu danych. Wystarczające będzie wskazanie, że wykonawca ma zapewnić działanie systemu zgodne z wymaganiami SLA, przy czym może wykorzystać zarówno własną infrastrukturę, jak i infrastrukturę dzierżawioną lub współdzieloną.

Biorąc powyższe pod uwagę odwołujący wniósł o uwzględnienie zarzutu i orzeczenie zgodnie z żądaniem w pkt II ppkt. 2.

Uzasadnienie zastrzeżenia dowodów jako tajemnicy przedsiębiorstwa przedstawia zrzut z systemu obejmujący jeden z ostatnich miesięcy świadczenia usługi oraz protokół przyjęcia usługi przez MPWiK Wrocław za taki miesiąc.

Odwołujący, działając zgodnie z art. 18 ust. 3 ustawy Prawo zamówień publicznych, a także z utrwaloną praktyką przed Krajową Izbą Odwoławczą, tym zastrzega przedłożone dowody — w szczególności:

- zrzut ekranu z systemu telemetrii dla projektu MPWiK Wrocław, prezentujący dane z realizacji wymagań SLA (w tym częstotliwość i dostępność transmisji danych),

- protokół przyjęcia systemu zdalnego odczytu przez MPWiK Wrocław, zawierający ocenę jakości świadczonej usługi jako informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2022 r. poz. 1233 ze zm.).

Na podstawie art. 545 ust. 3 ustawy odwołujący wniósł o ograniczenie przystępującym prawa wglądu do materiału dowodowego załączonego do akt sprawy w odniesieniu do załączników nt 7, z uwagi na okoliczność, że udostępnienie tego materiału groziłoby ujawnieniem informacji stanowiącej tajemnicę chronioną na podstawie odrębnych przepisów

Wymienione dokumenty zawierają dane techniczne, operacyjne oraz organizacyjne, które:

- odnoszą się do know-how odwołującego w zakresie organizacji transmisji danych w technologii LoRaWAN,

- przedstawiają konkretne parametry realizacyjne systemu wdrożonego na rzecz innego zamawiającego sektora wodociągowego, obejmują konfiguracje systemowe oraz statystyki odczytowe, stanowiące efekt doświadczenia i inwestycji technologicznych odwołującego, mają istotną wartość gospodarczą oraz operacyjną, i nie są powszechnie znane ani łatwo dostępne.

Ich ujawnienie innym wykonawcom (w tym konkurentom rynkowym) mogłoby doprowadzić do utrudnienia konkurowania odwołującego z innymi wykonawcami na rynku na poziomie jakości realizowanych usług a tym samym do wykorzystania ich do stworzenia ofert konkurencyjnych na nieuczciwych zasadach. Odwołujący wniósł, aby:

- wskazane dokumenty zostały przyjęte do wiadomości wyłącznie Krajowej Izby Odwoławczej oraz zamawiającego,

- nie były udostępniane innym uczestnikom postępowania ani publikowane w Biuletynie Zamówień Publicznych czy na platformie zakupowej zamawiającego,

- zostały rozpatrzone przez Izbę z zachowaniem zasad poufności, zgodnie z dotychczasową linią orzecniczą KIO dotyczącą zastrzeżeń tajemnicy przedsiębiorstwa.

25 lipca 2025 r. zamawiający poinformował o wniesieniu odwołania.

28 lipca 2025 r. wykonawca Polkomtel Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, ul. Konstruktorska 4 zgłosił swój udział w postępowaniu odwoławczym po stronie zamawiającego przez pełnomocnika działającego na podstawie pełnomocnictwa z 26 marca 2025 r. udzielonego przez prezesa zarządu, wiceprezesa i prokurenta. Do zgłoszenia dołączono dowody jego przekazania stronom. Przystępujący wskazał na interes w uzyskaniu rozstrzygnięcia na korzyść zamawiającego albowiem przedmiotem wniesionego odwołania są zarzuty dotyczące dokumentacji przetargowej. W jego ocenie odwołujący bezzasadnie kwestionuje zgodność dokumentacji z przepisami ustawy.

28 lipca 2025 r. wykonawca Orange Polska spółka akcyjna z siedzibą w Warszawie, Al. Jerozolimskie 160 zgłosił przystąpienie do postępowania odwoławczego po stronie zamawiającego przez pełnomocnika działającego na podstawie pełnomocnictwa z 12 maja 2023 r. udzielonego przez pełnomocnika działającego na podstawie pełnomocnictwa z 7 lutego 2022 r. udzielonego przez prezesa zarządu (w dacie udzielania pełnomocnictwa) i członka zarządu. Do zgłoszenia dołączono dowody jego przekazania stronom. Przystępujący oświadczył, że posiada interes w uzyskaniu rozstrzygnięcia na korzyść zamawiającego. Zamawiający opisał przedmiot zamówienia w sposób jednoznaczny, uwzględniający wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty, a także w sposób zapewniający zachowanie zasady uczciwej konkurencji i równego traktowania. Przystępujący jest w stanie złożyć ofertę i zrealizować przedmiot zamówienia zgodnie z wymaganiami określonymi przez zamawiającego. Uwzględnienie odwołania pozwoli złożyć oferty i wziąć udział w postępowaniu wykonawcom, którzy nie są w stanie zrealizować zamówienia w sposób zapewniający spełnienie wszystkich obiektywnie uzasadnionych potrzeb zamawiającego, co utrudni przystępującemu uzyskanie zamówienia w postępowaniu. Oddalenie odwołania sprawi, że prawidłowy opis przedmiotu zamówienia, sporządzony przez zamawiającego nie zostanie zmieniony i oferty będą mogły złożyć jedynie wykonawcy, którzy są w stanie zrealizować zamówienie zgodnie z wymaganiami Zamawiającego, co zwiększy szanse na uzyskanie przedmiotowego zamówienia przez przystępującego. W konsekwencji, należy uznać

przystępującego za podmiot, który ma interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje, w rozumieniu art. 525 ust. 1 ustawy. Wniósł o oddalenie odwołania w całości.

29 lipca 2025 r. wykonawca T-Mobile spółka akcyjna z siedzibą w Warszawie, ul. Marynarska 12 zgłosił swój udział w postępowaniu odwoławczym po stronie zamawiającego działając przez pełnomocnika na podstawie pełnomocnictwa z 19 lipca 2017 r. udzielonego przez dwóch członków zarządu. do zgłoszenia dołączono dowody jego przekazania stronom. Wskazał, że jest wykonawcą, który zamierza ubiegać się o przedmiotowe zamówienie. Kwestionowane przez odwołującego postanowienia dokumentacji przetargowej w zakresie dokonanego przez zamawiającego opisu przedmiotu zamówienia nie naruszają przepisów ustawy. Interes uczestnika polega na tym, że uwzględnienie odwołania doprowadzi do zmiany treści SWZ, w sposób, który utrudni uczestnikowi ubieganie się o udzielenie zamówienia i złożenie konkurencyjnej oferty oraz uzyskanie zamówienia. W konsekwencji uczestnik poniesie szkodę, a zatem posiada interes w rozstrzygnięciu na korzyść zamawiającego. Wniósł o oddalenie odwołania.

21 sierpnia 2025 r. wykonawca Polkomtel przedstawił dodatkowe stanowisko:

Zarzut naruszenia art. 99 Pzp (pasma licencjonowane)

Odnosząc się do tego zarzutu przystępujący wskazał, że jest on w całości niezasadny, a takie określenie warunków zamówienia w OPZ było w pełni uzasadnione potrzebami zamawiającego oraz proporcjonalne, co zostanie szczegółowo wykazane poniżej.

Przedmiotem zamówienia jest dostawa, wdrożenie i obsługa systemu smart city w zakresie monitoringu sieci wodociągowej”. W tym zakresie należy wskazać, że systemy służące zbiorowemu zaopatrzeniu w wodę, stanowią zgodnie z art. 3 pkt 2 lit. f ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r. poz. 122 z późn. zm.) jeden z elementów infrastruktury krytycznej dla której to infrastruktury niezbędne jest zapewnienie odpowiedniego poziomu ochrony oraz bezpieczeństwa.

Oznacza to, że podlega ona szczególnej ochronie z punktu widzenia bezpieczeństwa państwa oraz ciągłości funkcjonowania podstawowych usług dla ludności. W tym kontekście monitoring sieci wodociągowej nie jest wyłącznie rozwiązaniem technicznym o charakterze eksploatacyjnym, ale pełni rolę strategiczną w zapewnieniu:

- a) Bezpieczeństwa dostaw wody – niezakłócone funkcjonowanie systemów wodociągowych ma bezpośredni wpływ na zdrowie i życie mieszkańców oraz działalność gospodarczą.
- b) Ochrony przed skutkami awarii i incydentów – szybkie wykrywanie wycieków, spadków ciśnienia czy skażeń umożliwia natychmiastową reakcję i ograniczenie skutków zdarzeń kryzysowych.
- c) Odporności na zagrożenia zewnętrzne – systemy wodociągowe mogą być celem działań o charakterze terrorystycznym, sabotażowym czy cybernetycznym; zastosowanie odpowiednio chronionych rozwiązań teleinformatycznych minimalizuje to ryzyko.
- d) Spełnienia wymagań prawnych i organizacyjnych – podmioty zarządzające infrastrukturą krytyczną zobowiązane są do utrzymywania odpowiedniego poziomu bezpieczeństwa, a wdrożenie systemu monitoringu stanowi jeden z podstawowych elementów realizacji tego obowiązku.

Z powyższych względów system Smart City w zakresie monitoringu sieci wodociągowej należy traktować jako element infrastruktury krytycznej, co determinuje konieczność zapewnienia mu odpowiedniego poziomu ochrony fizycznej, teleinformatycznej i organizacyjnej, a także stosowania rozwiązań technologicznych gwarantujących wysoki poziom niezawodności, bezpieczeństwa transmisji danych oraz odporności na zakłócenia i ingerencje nieuprawnionych podmiotów. Wybór technologii transmisji danych, architektury systemu oraz modelu jego obsługi musi być więc podporządkowany wymaganiom wynikającym z charakteru infrastruktury krytycznej i powinien uwzględniać standardy bezpieczeństwa określone w przepisach krajowych i unijnych.

O tym jak istotna jest kwestia bezpieczeństwa takiej infrastruktury przekonują chociażby wydarzenia z ostatnich dni, kiedy miała miejsce próba ataku hakerskiego na sieć wodociągową w jednym z dużych polskich miast<sup>1</sup>. Nie są to jednocześnie przypadki odosobnione<sup>2</sup>, co pokazuje rangę i znaczenie problemu.

Co istotne, analogiczne zarzuty, jak zarzuty przedstawione w przedmiotowym postępowaniu były już stawiane przez Emitel w innym postępowaniach dotyczących usług smart city dla sieci wodociągowych. Kwestia ta była przedmiotem wyroku KIO z 5.02.2024 r., KIO 32/24, LEX nr 3694088 oraz wyroku KIO z 22.09.2023 r., KIO 2516/23, LEX nr 3694050. W obu przypadkach odwołania Emitel zostały oddalone. Jak trafnie wskazano w wyroku KIO z 5.02.2024 r.: „Nie narusza przepisów p.z.p. takie sporządzenie opisu przedmiotu zamówienia, który uwzględnia potrzeby zamawiającego, nawet jeżeli utrudnia lub uniemożliwia niektórym podmiotom dostęp do zamówienia. Zamawiający nie ma bowiem obowiązku zapewnienia możliwości realizacji przedmiotu zamówienia wszystkim podmiotom działającym na rynku w danej branży, bowiem pojęcie uczciwej konkurencji nie może być utożsamiane z konkurencją absolutną. Jednakże w przypadku opisu przedmiotu zamówienia w sposób uprzywilejowujący lub eliminujący niektórych wykonawców lub produkty, po stronie zamawiającego istnieje obowiązek przedstawienia rzeczowych argumentów uzasadniających taki opis.”

Powyższe rozstrzygnięcia pozostają w pełni adekwatne do rozpatrywanej sprawy. Co jednak istotne, za oddaleniem

odwołania Emitel przemawia także szereg innych argumentów, które zostaną szczegółowo omówione poniżej, a które dodatkowo uzasadniają powyższą tezę z wyroku KIO. Warto także podkreślić, że obecne postanowienia OPZ pozwalają na zachowanie pełnej konkurencyjności postępowania (jest wiele podmiotów mogących wziąć udział w przetargu). W konsekwencji, wbrew twierdzeniom odwołującego wymogi określone w OPZ są uzasadnione z szeregu istotnych powodów związanych z realizacją opisanych powyżej celów tj.

- a) terminu uruchomienia usług
  - b) interoperacyjności systemu monitorowania i możliwości zmiany dostawcy
  - c) bezpieczeństwa sieci oraz bezpieczeństwa świadczonych usług
  - d) zapewnienia odpowiedniej stabilności i jakości świadczonych usług
- [termin uruchomienia usług]

Zamawiający wymaga, aby uruchomienie systemu smart city, w tym zapewnienie dostępu do platformy odczytowej i aplikacji mobilnej oraz transmisji danych z całego obszaru działania zamawiającego nastąpiło w terminie 30 dni od podpisania umowy. W tym kontekście należy podkreślić okoliczność skrzętnie pominiętą przez odwołującego, że sieci operatorów komórkowych działające w paśmie licencjonowanym są już wybudowane i uruchomione, a w konsekwencji wykorzystanie ich do realizacji usług we wskazanym terminie nie jest obciążone jakimkolwiek ryzykiem. Ewentualne problemy zasięgowe mogą dotyczyć pojedynczych lokalizacji zamawiającego.

Tymczasem sieć LoRaWAN Emitel nie istnieje i musi być dopiero wybudowana, co zresztą pośrednio przyznaje sam odwołujący wskazując na str. 9 odwołania, że uruchomienie usług wymagałoby od niego wykorzystania modelu hybrydowego tj. korzystania w pierwszy roku obowiązywania umowy z kart SIM operatora mobilnego, które zapewniają zgodność z wymogami SLA w oparciu o pasmo licencjonowane, a dopiero w drugim roku wybudowania własnej sieci odczytowej w paśmie nielicencjonowanym.

Przystępujący podkreślił, że co do zasady taki scenariusz wydaje się również niemożliwy do realizacji, gdyż w przedmiotowym zamówieniu, zamawiający wymaga, aby podmiot realizujący usługi na rzecz zamawiającego dysponował własną infrastrukturą telekomunikacyjną wykonawcy. Zamawiający pod pojęciem „własną infrastrukturę”, co zostało wprost wyjaśnione przez zamawiającego, rozumie: „Sieci będą własnością wykonawcy; Sieci dzierżawione, kolokacyjne; infrastruktura współdzielona. W OPZ pojęcie „własna infrastruktura” należy rozumieć jako infrastrukturę, do której wykonawca posiada wyłączne prawo dysponowania na poziomie operacyjnym i konfiguracyjnym.” Jak zostanie to poniżej wyjaśnione, taki wymóg jest w pełni uzasadniony. Jednocześnie w modelu hybrydowym do którego odnosi się Emitel, nie będzie on dysponował własną siecią, a będzie jedynie odsprzedawał usługi świadczone na jego rzecz przez operatora sieci ruchomej, nie tylko nie mając jakiegokolwiek kontroli „dysponowania na poziomie operacyjnym i konfiguracyjnym”, ale de facto nie mając żadnego wpływu na jakość, stabilność oraz dostępność tych usług.

Również założenie dotyczące budowy własnej sieci oraz związanej z tym konieczności migracji świadczonych usług niesie za sobą szereg ryzyk dla bezpieczeństwa i integralności świadczonych usług.

Po pierwsze, wątpliwe jest założenie, że operator będzie w stanie wybudować rozległą sieć LoRaWAN na obszarze całego miasta w terminie 12 miesięcy od podpisania umowy. Przystępujący zauważył, że budowa takiej sieci jest procesem złożonym i w istotnej mierze uzależnionym od czynników będących poza kontrolą operatora.

Budowa rozległej sieci LoRaWAN wymaga bowiem odpowiedniego planowania radiowego, pozyskania zgód i praw do nieruchomości, zapewnienia zasilania, które to czynniki mogą opóźnić i utrudniać realizację zaplanowanej inwestycji. Poniżej pokrótce charakteryzujemy poszczególne etapy takich prac. Operator w pierwszej kolejności musi zaplanować sieć, uwzględniając topologię miasta, lokalizację urządzeń odczytowych, zasięg bramek (gatewayów) oraz możliwość ich instalacji. Już tylko te czynności zajmą co najmniej 2-3 miesiące, co oznacza, że Emitel czy jakiegokolwiek inny podmiot pragnący wykorzystać sieć LoRaWAN nie jest w stanie dotrzymać terminu określonego w OPZ, a jak wskazano powyżej sieć hybrydowa i wykorzystanie kart SIM innego operatora nie jest dopuszczalna.

Co jednak istotne, także dalsze czynności nie dają gwarancji, aby operator był w stanie wybudować i uruchomić sieć nie tylko w terminie 30 dni, ale być może także w deklarowanym terminie 12 miesięcy. Przystępujący bowiem zauważył, że w dalszej kolejności operator musi uzyskać tytuły prawne do nieruchomości tzw. prawo drogi pozwalające mu na instalację jego urządzeń np. na nieruchomościach, czy na słupach lub innych obiektach. Uwzględniając uwarunkowania prawne, w wielu wypadkach operator musi liczyć się z ryzykiem odmowy ze strony uprawnionych podmiotów, co wymaga albo szukania lokalizacji zastępczych (przykładowo przy budowie jednej stacji bazowej operatorzy z reguły typują 3-4 lokalizacje i prowadzą równoległe rozmowy z właścicielami każdej z nich) albo uzyskanie decyzji zastępującej umowę na podstawie art. 33 ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych (co zajmie około 2-3 lat). W następnym kroku operator musi zakupić stosowne urządzenia, w tym tzw. bramki (ang. gateway) oraz zapewnić zasilanie i łączność do tych urządzeń. Cały ten proces również zajmuje wiele tygodni i w wielu aspektach pozostaje poza kontrolą operatora.

Dopiero po realizacji powyższych kroków, operator może przystąpić do fizycznego montażu i konfiguracji urządzeń oraz

uruchomienia sieci, obejmującej również niezbędne testy oraz optymalizację sieci, co w środowisku miejskim również nie stanowi czynności łatwej i szybkiej. Tym samym, w praktyce — pokrycie siecią LoRaWAN tak dużego miasta jak Katowice to okres co najmniej kilkunastu miesięcy, a nie 30 dni jak wymaga tego zamawiający. Co istotne, przy modelu wskazanym przez odwołującego dodatkowym krokiem, w ogóle nie przewidzianym w OPZ, jest migracja usług z sieci ruchomej dostawcy kart SIM do sieci LoRaWAN, co również niesie za sobą ryzyka przerwy w usłudze, błędów w migracji, braku integralności i kompletności danych.

Wszystkie opisane powyżej czynniki powodują, że uzasadnione jest oczekiwanie zamawiającego, aby sieć monitoringu oprzeć o istniejącą infrastrukturę operatorów komórkowych z założeniem, że w niewielkim stopniu i w niewielkim zakresie (maksymalnie do 10%) ewentualne braki w tej sieci zostaną uzupełnione, aniżeli opieranie się na nieistniejącej sieci LoRaWAN, która dopiero ma zostać wybudowana.

[interoperacyjności systemu monitorowania i możliwości zmiany dostawcy]

Kolejnym istotnym czynnikiem przemawiającym przeciwko dopuszczeniu sieci LoRaWAN jest brak możliwości zmiany dostawcy na innego operatora, którego to problemu nie niesie za sobą wybór jednego z operatorów sieci ruchomych. Przystępujący zaznaczył, że w przypadku gdy zamawiający z jakichś przyczyn będzie musiał zmienić dostawcę usług to zgodnie z wymaganiami określonymi w OPZ taka zmiana będzie stosunkowo prosta do przeprowadzenia, gdyż wystarczająca będzie wymiana kart SIM w modułach, aby nowy dostawca mógł świadczyć usługi.

Tymczasem w przypadku zastosowania sieci LoRaWAN, zamawiający musiałby de facto wybudować lub zamówić nową sieć, gdyż wybudowana przez Emitel sieć pozostaje w pełni jego własnością i pod jego kontrolą. Wskazuje na to zresztą także opracowanie załączone przez odwołującego (załącznik nr 10 do odwołania) w którym wprost wskazano: „w przypadku LoRaWAN inwestor jest właścicielem całej infrastruktury systemu IoT”(str. 8), Oznacza to konieczność budowy sieci od nowa, gdyż z oczywistych względów Emitel jako operator sieci we własnym zakresie zarządza kluczami bezpieczeństwa i nie może ich udostępnić podmiotowi trzeciemu. Również bramki (gateways) zainstalowane i uruchomione przez Emitel nie mogą zostać wykorzystane przez inny podmiot.

[bezpieczeństwa sieci oraz bezpieczeństwa świadczonych usług]

Jak już była o tym mowa, jednym z kluczowych czynników w przypadku usług objętych postępowaniem prowadzonym przez zamawiającego jest zapewnienie bezpieczeństwa zarówno sieci wodociągowej, jak i bezpieczeństwa świadczonych usług. Chociaż w przypadku obu tych sieci, zapewnione jest szyfrowanie transmisji danych to nie ma wątpliwości, że świadczenie usług w paśmie licencjonowanym zapewnia większe bezpieczeństwo sieci, jak i świadczonych usług.

Przede wszystkim odwołujący pomija fakt, że w przypadku wykorzystania pasma licencjonowanego to wyłącznie operator świadczący usługę posiada uprawnienie do korzystania z tego pasma, a dzięki wykorzystaniu wydzielonego APN może też odpowiednio izolować i zabezpieczać ruch w sieci.

Tymczasem w przypadku wykorzystania tzw. pasma nielicencjonowanego sieć znacznie bardziej narażona jest na zakłócenia i pogorszenia jakości świadczonych usług. Przystępujący zauważył, że z pasma z którego korzysta sieć LoRaWAN może korzystać każdy użytkownik. Jest to szczególnie istotne w dużych miastach, gdzie pasmo nielicencjonowane jest mocno przeciążone w związku z wykorzystaniem przez sieci Wi-Fi, Bluetooth, bramki IoT, czujniki i inne aplikacje, co prowadzi do spadków zarówno zasięgu, jak i jakości świadczonych usług.

Pasmo nielicencjonowane jest również bardziej narażone na zakłócenia, na skutek wykorzystywania nielegalnych urządzeń typu wzmacniacze sygnału.

Dodatkowo, jak każda transmisja w paśmie „otwartym”, transmisja danych w paśmie nielicencjonowanym może zostać łatwiej przechwycona, chociaż w tym zakresie bez dostępu do kluczy szyfrujących, nie ma ryzyka odczytu takich danych.

Kluczowe jest jednak, że uwzględniając opisane powyżej przypadki ataków hakerskich na sieci wodociągowe, realizacja usług w paśmie nielicencjonowanym jest znacznie bardziej narażona na zakłócenia ze strony podmiotów atakujących takie sieci.

Transmisja w sieci LoRaWAN w paśmie nielicencjonowanym jest łatwa do zakłócenia – wystarczy generowanie zakłóceń radiowych w danym kanale, co może prowadzić do uniemożliwienia komunikacji pomiędzy czujnikami a bramkami.

W przypadku sieci w paśmie licencjonowanym powyższe ryzyko jest znacznie niższe i łatwiejsze do zapobieżenia. Przede wszystkim operator w paśmie licencjonowanym ma wyłączne prawo do korzystania z częstotliwości, więc unika zakłóceń od innych użytkowników i ma szersze możliwości w zakresie ochrony przed zakłóceniami.

[zapewnienia odpowiedniej stabilności i jakości świadczonych usług]

Co istotne, również w zakresie zapewnienia odpowiedniej stabilności i jakości usług, sieć w paśmie licencjonowanym posiada znacznie szersze możliwości gwarantujące odbiorcą odpowiednią stabilność i poziom SLA.

W sieci LoRaWAN, gdzie pasmo dzielone jest przez wszystkich użytkowników, a operator nie ma wpływu na zakres

użytkownicy takiej sieci, nie ma on możliwości zapewnienia gwarancji dla odpowiedniej dostępności i jakości usług. Operator sieci ruchomej jako wyłączny dysponent pasma, samodzielnie kontroluje sieć, ale dzięki zastosowaniu wydzielonego APN ma również możliwość zapewnienia lepszej priorytetyzacji i SLA dla określonych usług, zgodnie z obowiązującymi przepisami prawa w zakresie neutralności sieci. Ponadto, operator sieci w pełni kontroluje pojemność takiej sieci i dzięki wysokiej skalowalności sieci może zwiększać jej pojemność zarówno poprzez zwiększanie zasobów pasma, jak i zagęszczanie obszaru nowymi stacjami bazowymi.

Co istotne, uwzględniając okres obowiązywania umowy, który został określony na 10 lat, należy również pamiętać o jednym istotnym czynnikiem jakim jest pełna kontrola nad częstotliwościami, co powoduje, że w licencjonowanym paśmie nie ma ryzyka, że nagle pojawi się nowa technologia masowo wykorzystująca te same częstotliwości. Tymczasem korzystając z pasma nielicencjonowanego, w perspektywie 10 lat, żaden racjonalnie działający operator nie jest w stanie zagwarantować, że będzie w stanie zapewnić odpowiednią jakość usług. Na ryzyko braku zapewnienia odpowiedniej jakości w sieciach wykorzystujących pasmo nielicencjonowane i potrzebę wykorzystania sieci w paśmie licencjonowanym zwraca również uwagę Komisja Europejska, która wprost wskazuje, że chociaż prawo do korzystania z widma w pasmach częstotliwości zwolnionych z obowiązku licencji przysługuje urządzeniom spełniającym określone warunki techniczne umożliwiające współdzielenie widma to użytkownicy urządzeń zwolnionych z obowiązku licencjonowania nie są chronieni przed zakłóceniami i nie otrzymują żadnej gwarancji jakości usług.

Reasumując, nie ma wątpliwości, że w okolicznościach przedmiotowej sprawy zarzut Emitel jest niezasadny i nie może zostać uwzględniony.

## II. Zarzut naruszenia art. 99 Pzp (własna infrastruktura telekomunikacyjna)

Przystępujący podkreślił, że na gruncie praktyki telekomunikacyjnych zamówień publicznych pojęcie „własnej infrastruktury telekomunikacyjnej” nie jest rozumiane jako dysponowanie prawem własności do takiej infrastruktury. Takie rozumienie pojęcia całkowicie mijaloby się ze sposobem pozyskiwania infrastruktury przez operatorów telekomunikacyjnych. Rozumie to także Zamawiający, który w dniu 11 sierpnia br. w ramach wyjaśnienia SWZ udzielił następującej odpowiedzi: Zamawiający pod pojęciem „własnej infrastruktury” rozumie: Sieci będą własnością 29/41 wykonawcy; Sieci dzierżawione, kolokacyjne; infrastruktura współdzielona. W OPZ pojęcie „własna infrastruktura” należy rozumieć jako infrastrukturę, do której wykonawca posiada wyłączne prawo dysponowania na poziomie operacyjnym i konfiguracyjnym.

Tym samym zarzut podniesiony przez odwołującego należy uznać za chybiony.

W szczególności nie jest prawdą, że z możliwości ofertowania są wyłączeni tacy wykonawcy jak Polkomtel Sp. z o.o. (Przystępujący), czy inni telekomunikacyjni operatorzy.

Sam Odwołujący przyznał, że jego sieć nie istnieje i wymaga budowy, a w okresie przejściowym chciałby wykorzystywać karty SIM innych dostawców usług, niewątpliwie taki model realizacji usług nie spełnia wymogu „dysponowania własną infrastrukturą”.

Biorąc pod uwagę powyższe, zarzut nie zasługuje na uwzględnienie.

## III. Zarzut naruszenia art. 112 ust. 1 Pzp (własna infrastruktura telekomunikacyjna)

Odwołujący zakwestionował treści żadnego z warunków udziału w postępowaniu (w rozumieniu art. 112 Pzp), a jedynie treść opisu przedmiotu zamówienia. Odwołujący wskazał na „ukryty warunek udziału” sformułowany w treści opisu przedmiotu zamówienia.

Biorąc pod uwagę powyższe, zarzut ten zasługuje na oddalenie. Nie jest bowiem możliwe doszukiwanie się „ukrytych warunków udziału” w treści OPZ. Należy pamiętać, że: Postępowanie o udzielenie zamówienia publicznego stanowi sformalizowaną procedurę, która dzięki regulacjom ustawowym stanowi gwarancję realizacji zasad prawa zamówień publicznych takich jak równe traktowanie wykonawców w postępowaniu o udzielenie zamówienia oraz zachowanie konkurencyjności między wykonawcami. Każde odstępstwo od formalizmu postępowania o udzielenie zamówienia publicznego prowadzi do naruszenia procedury o zamówienie publiczne, a w konsekwencji naruszenie zasad prawa zamówień publicznych w stosunku do wykonawców, którzy składają w postępowaniu oferty. Jak dodaje Izba5: przypomnienia wymaga, że ocena spełniania przez wykonawcę ustanowionych przez zamawiającego w danym postępowaniu o udzielenie zamówienia publicznego warunków udziału w postępowaniu winna być oceniana ściśle wedle reguł, zasad wyartykułowanych przez zamawiającego w postanowieniach SWZ i to tak co do odczytywania samych warunków, jak i sposobu wykazywania ich spełniania. W innej sprawie KIO słusznie zauważyła6: Podstawą twierdzeń Odwołującego jest odnoszenie treści opisu warunku udziału w postępowaniu do opisu przedmiotu zamówienia i przez ten pryzmat nadawanie brzmienia opisowi warunku. Powyższe działanie należy uznać za nieuprawnione. Opis warunku udziału w postępowaniu dokonywany w oparciu o art. 22 ust. 4 ustawy jest odrębną instytucją od opisu przedmiotu zamówienia dokonywanego w oparciu o art. 29 ustawy.

Biorąc pod uwagę powyższe, nie ma podstaw do doszukiwania się „ukrytych” warunków udziału w postępowaniu w treści opisu przedmiotu zamówienia. Takie działanie jest pozbawione podstaw prawnych. Tym samym zarzut

naruszenia art. 112 ustawy w kontekście brzmienia opisu przedmiotu zamówienia, jest całkowicie chybiony.

29 sierpnia 2025 r. zamawiający złożył odpowiedź na odwołanie, wnosząc o:

1) oddalenie odwołania wykonawcy w całości;

2) dopuszczenie, na podstawie art. 534 ustawy dowodów z dokumentów w postaci:

- mapa dzielnic Katowic z uwzględnieniem ilości mieszkańców i trudnych lokalizacji pod względem możliwości stacjonarnego odczytu wodomierzy wraz wykaz tabelaryczny trudnych lokalizacji - wniosek o ograniczenie jawności zgodnie z pkt 3) pisma;

- Notatka wewnętrzna z przeprowadzonego pilotażu;

- wyrok KIO z dnia 22.09.2023 r. sygn. KIO 2516/23;

- wyrok KIO z dnia 5.02.2024r. sygn. KIO 32/24.

3) ograniczenie, na podstawie art. 545 ust. 3 ustawy innym stronom niż zamawiający oraz uczestnikom postępowania odwoławczego prawa wglądu do materiału dowodowego w postaci mapy dzielnic Katowic z uwzględnieniem ilości mieszkańców i trudnych lokalizacji pod względem możliwości stacjonarnego odczytu wodomierzy wraz wykazu tabelarycznego trudnych lokalizacji z uwagi na okoliczność, że udostępnienie tego materiału groziłoby ujawnieniem informacji stanowiącej zdaniem zamawiającego tajemnicę chronioną na podstawie odrębnych przepisów;

4) niedopuszczenie dowodu z Opracowania eksperckiego mgr inż. P.Z. Prezesa Zarządu Krajowego Stowarzyszenia Budowniczych Telekomunikacji na okoliczności wskazane na str. 6 Odwołania, jako niemających istotnego znaczenia dla rozstrzygnięcia sprawy oraz nie wymagających dowodzenia (art. 531 ustawy oraz art. 541 ustawy);

5) zasądzenie na rzecz zamawiającego kosztów postępowania według norm przepisanych.

Uzasadnienie wniosku o ograniczenie dostępu do materiału dowodowego - art. 545 ust. 3 ustawy

Zamawiający wskazał, że informacje zawarte w wykazie tabelarycznym trudnych lokalizacji zawierają m.in. dane adresowe pozwalające na identyfikację odbiorców usług zbiorowej dostawy wody, a więc dane osobowe w rozumieniu rozporządzenia ( UE ) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych . ( RODO).

RODO definiuje dane osobowe jako wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"), przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 pkt 1). Pojęcie danych osobowych ma szeroki zakres przedmiotowy i obejmuje różnego rodzaju informacje, które dotyczą konkretnej osoby - także informacje, które chociażby pośrednio identyfikują daną osobę. W kategorii tej znajdują się zarówno dane bezpośrednie takie jak imię i nazwisko, adres zamieszkania, nr telefonu, nr PESEL. Adres zamieszkania odgrywa kluczową rolę w identyfikacji osoby. Gdy jest połączony z innymi danymi, jak imię i nazwisko czy nr telefonu może umożliwić jednoznaczne rozpoznanie danej osoby. To samo połączenie może dotyczyć informacji dostępnych publicznie lub w bazach danych np. baza elektronicznych Księgi Wieczystych, baza nr działek itd. Wtedy posiadany adres może prowadzić do pełnej identyfikacji danej osoby. Identyfikacja taka może opierać się na różnego rodzaju informacjach, które rozpatrywane jednostkowo nie pozwolą na ustalenie tożsamości, ale zestawione ze sobą mogą pozwolić na zidentyfikowanie konkretnej osoby. Oznacza to że o możliwości identyfikacji przesądza nie tylko charakter posiadanych informacji, ale także kontekst w jakim informacje te występują. Adres zamieszkania jest uznawany za daną osobową zgodnie z RODO, co zobowiązuje organizację do jego ochrony przed nieautoryzowanym dostępem i przetwarzaniem. Na Katowickich Wodociągach S.A jako administratorze danych osobowych ciąży obowiązek zabezpieczenia i przetwarzania danych osobowych naszych klientów zgodnie z wymogami RODO. Zamawiający określa cel i zakres ich przetwarzania, ale musi być on zawsze zgodny z wymogami RODO.

Zamawiający w pierwszej kolejności podniósł, że zarzuty odwołującego skupione są w głównej mierze na naruszeniu normy art. 99 ust. 1 i 2 oraz art. 4 ustawy i art. 16 ust. 1 oraz ust. 3 ustawy a więc opisu przedmiotu zamówienia w sposób m.in. utrudniający uczciwą konkurencję oraz równe traktowanie wykonawców, w sposób nieproporcjonalny a także w sposób niejednoznaczny czy niewyczerpujący [...] w zasadniczym stopniu w zakresie wymogu korzystania z komunikacji radiowej w licencjonowanym paśmie radiowym.

Zamawiający wskazał, że ugruntowanym w orzecznictwie Krajowej Izby Odwoławczej jest podgląd, wedle którego zamawiający jako podmiot dokonujący zakupów, jest uprawniony do określenia swoich oczekiwań dotyczących przedmiotu zamówienia, jego cech i funkcjonalności. Każde z takich wymagań w większym lub mniejszym stopniu może ograniczać konkurencję, jednak tak długo, jak wymagania te są podyktowane obiektywnie uzasadnionymi potrzebami zamawiającego, a ich celem nie jest zawężenie kręgu wykonawców mogących je wykonać, to zamawiający jest uprawniony do ich sformułowania. Nie jest natomiast celem systemu zamówień publicznych i obowiązującej w nim zasady uczciwej konkurencji. umożliwienie uzyskania zamówienia wszystkim wykonawcom działającym w danej branży.

bez względu na to jakie cechy i właściwości ma przedmiot zamówienia, który mogą lub chcą zaoferować i bez uwzględnienia potrzeb zamawiającego. Nadto jednostki sektora finansów publicznych są obowiązane stosować zasady wynikające z art. 44 ust. 3 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, zgodnie z którym, wydatki publiczne powinny być dokonywane w sposób celowy i oszczędny z zachowaniem zasad uzyskiwania najlepszych efektów z danych nakładów oraz optymalnego doboru metod i środków służących osiągnięciu założonych celów (zob. wyrok KIO z dnia 6.09.2024r. sygn. KIO 2918/24). Zatem nie stanowi utrudniania uczciwej konkurencji takie opisanie przedmiotu zamówienia, które znajduje odbicie w obiektywnie uzasadnionych potrzebach zamawiającego, nawet jeżeli utrudnia lub uniemożliwia niektórym podmiotom dostęp do zamówienia. Celem postępowania nie jest zapewnienie możliwości realizacji przedmiotu zamówienia wszystkim podmiotom działającym na rynku w danej branży, ale zaspokojenie uzasadnionych potrzeb publicznych. Jednocześnie to na wykonawcy spoczywa ciężar dowodu, że wymagania określone w opisie przedmiotu zamówienia nie wynikają ze zobiektywizowanych (rzeczywistych) potrzeb zamawiającego. (zob. wyrok KIO z dnia 30.08.2024r. sygn. KIO 2830/24; wyrok KIO z dnia 10.05.2024r. sygn. KIO 1321/24).

W tym zakresie błędny jest pogląd odwołującego jakoby to na zamawiającym ciążył ciężar dowodowy braku naruszenia przepisów w opisie przedmiotu zamówienia. Zgodnie z art. 534 ust. 1 ustawy strony i uczestnicy postępowania odwoławczego są obowiązani wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne. Zatem, zasadą jest, że w postępowaniu odwoławczym że ciężar dowodu w zakresie podstaw odwołania spoczywa na odwołującym, a nie na zamawiającym. Wprawdzie w ustawie Prawo zamówień publicznych brak jest odpowiednika art. 6 Kodeksu cywilnego, który wprowadza ogólną regułę rozkładu ciężaru dowodu w postępowaniu cywilnym, jednak zasada wyrażona w tym przepisie ma na tyle uniwersalny charakter, że nie tylko może, ale i powinna znaleźć zastosowanie również w postępowaniu odwoławczym. Zgodnie z tym przepisem ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne. Procesowym odpowiednikiem tego przepisu jest art. 232 KPC, który nakłada na strony obowiązki procesowe stanowiące wyraz reguły rozkładu ciężaru dowodu mające zapewnić jej realizację. W tym zakresie w ustawie znalazł się art. 534, zgodnie z którym strony i uczestnicy postępowania odwoławczego są obowiązani wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne (zob. wyrok KIO z dnia 5.02.2025r. sygn. KIO 22/25). W rezultacie, wbrew twierdzeniom odwołującego, to wyłącznie na nim spoczywa ciężar dowodowy wykazania okoliczności faktycznych będących podstawą odwołania i uzasadniających jego wnioski. To odwołujący, jako profesjonalista działający w obszarze, w którym ubiega się o zamówienie, w oparciu o swoją profesjonalną wiedzę i doświadczenie zobowiązany jest podjąć inicjatywę dowodową w celu wykazania zasadności swoich twierdzeń. Odwołujący bowiem, a nie zamawiający, a tym bardziej uczestnik postępowania, wywodzi z okoliczności podnoszonych w odwołaniu korzystne dla siebie skutki prawne, opierając na nich żądanie odwołania, a co za tym idzie oczywistym jest, że okoliczności te powinien wykazać właśnie odwołujący (zob. wyrok KIO z dnia 21.01.2024r. sygn. KIO 3503/24; z dnia 26.08.2024r. sygn. KIO 2741/24).

W rezultacie zamawiający, jako gospodarz postępowania ma prawo opisać przedmiot zamówienia w sposób uwzględniający jego rzeczywiste potrzeby. To właśnie uzasadnione potrzeby zamawiającego determinują opis przedmiotu zamówienia, w tym również jakie cechy techniczne są istotne z punktu widzenia jego rzeczywistych potrzeb. Zamawiający podkreślił, że z jednej strony wymóg zachowania uczciwej konkurencji w zamówieniach publicznych nie ma charakteru abstrakcyjnego i bezwzględnego, a z drugiej przepisy obecnego prawa zamówień publicznych nie obligują do zapewnienia przez zamawiającego takich warunków postępowania i opisu przedmiotu zamówienia aby potencjalnie każdy podmiot i w każdej sytuacji miał możliwość złożenia oferty

Zamawiający wskazał, że treść odwołania wskazuje na „otwarty” katalog zarzutów sformułowanych względem zamawiającego, o czym świadczy użycie przez odwołującego wyrażen „w szczególności dla zarzutu pierwszego i drugiego. Przedmiotowa okoliczność ma istotne znaczenie albowiem Krajowa Izba Odwoławcza Dalej KIO), stosownie do treści art. 555 PZP nie może orzekać co do zarzutów, które nie były zawarte w odwołaniu. Zakres rozpoznania sprawy przez KIO jest ściśle ograniczony zarzutami odwołania sprowadzającymi się do czynności lub zaniechań zamawiającego opartych na konkretnej i precyzyjnej podstawie faktycznej. Stąd też odwołujący w odwołaniu zobowiązany jest wskazać treść przepisu, który został przez zamawiającego naruszony, a w uzasadnieniu faktycznym podać wszystkie okoliczności potwierdzające zasadność twierdzeń wyrażonych w odwołaniu. Zarzut jest substratem okoliczności faktycznych i prawnych, które powinny być wskazane w odwołaniu i to właśnie one określają granice rozpoznania odwołania. Powyższe oznacza, że niezależnie od podstawy prawnej wskazanego naruszenia, nowe okoliczności faktyczne podnoszone dopiero na rozprawie stanowią nowe zarzuty, które nie były zawarte w odwołaniu. Nie mogą one zatem być brane pod uwagę w trakcie rozpoznania odwołania przez KIO (zob. szerzej wyrok KIO z dnia 08.03.2024r. sygn. KIO 576/24).

Zamawiający wskazał, że wybór systemu odczytowego na System Stacjonarny w oparciu o rozwiązania IoT był poprzedzony pilotażem, zawierającym analizę rynku z udziałem wybranych podmiotów oferujących usługi w zakresie

systemów zdalnego odczytu, których celem było określenie łączności i efektywności przesyłu danych. Testy te dotyczyły obszaru, na jakim działa zamawiający, a więc Miasta Katowice, przy uwzględnieniu lokalnych uwarunkowań co pozwoliło zamawiającemu na sprecyzowanie swoich potrzeb oraz priorytetów związanych z wdrożeniem Stacjonarnego Systemu odczytowego.

Dowód: Notatka służbowa z pilotażu.

Zamawiający oświadczył, że kwestionuje w pełni zarzuty odwołującego wskazujące co następuje:

Zgodnie z treścią zarzutu odwołujący wskazuje na naruszenie przez zamawiającego przepisów art. 99 ust. 1, 2 oraz 4 ustawy i art. 16 ust. 1 oraz ust. 3 ustawy przez postawienie wymogu by system musiał korzystać z komunikacji radiowej w licencjonowanych pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych (I Opis ogólny pkt 1 Przedmiot zamówienia ppkt 1.1, Opis Przedmiotu Zamówienia - pkt 1.1.1. OPZ) przez:

1) Posłużeniem się pojęciem „pasma licencjonowanego” co jest pojęciem nieznanym na gruncie ustawy Prawo komunikacji elektronicznej;

2) Tworzenie nieproporcjonalnych warunków dla realizacji zamówienia poprzez wmuszanie „licencji na pasmo” przy czym system odczytowy można zbudować również na pasmach częstotliwości otwartych przeznaczonych w tym celu przez przepisy powszechnie obowiązującego prawa co również dopuszcza Zamawiający ale w ilości nie więcej aniżeli 10% lokalizacji;

3) Utrudnianie warunków konkurencji poprzez wskazanie „pasma licencjonowanego” co predysponuje do realizacji usługi operatorów mobilnych posiadających rezerwację częstotliwości a jednocześnie wyklucza innych przedsiębiorców telekomunikacyjnych mogących świadczyć usługi na rzecz Zamawiającego ale nie posiadających rezerwacji częstotliwości;

4) Postawienie wymogu pasma licencjonowanego dla 90% lokalizacji, nie znajduje żadnego obiektywnego uzasadnienia technicznego ani funkcjonalnego bowiem zarówno transmisja w paśmie licencjonowanym, jak i w nielicencjonowanym ma zamawiającemu zapewnić identyczne parametry jakościowe - w tym m.in. odczyt z co najmniej 90% urządzeń raz dziennie, z 95% raz w tygodniu, i z 98% raz w miesiącu. Zatem - skoro wymagania SLA są jednakowe bez względu na zastosowaną technologię transmisji, to naruszenie obowiązku stosowania pasm licencjonowanego w 90% przypadków jest nieproporcjonalne oraz prowadzi do bezpodstawnego ograniczenia konkurencji.

Posłużeniem się pojęciem „pasma licencjonowanego” co jest pojęciem nieznanym na gruncie ustawy Prawo komunikacji elektronicznej,

Tworzenie nieproporcjonalnych warunków dla realizacji zamówienia poprzez wymuszanie „licencji na pasmo” przy czym system odczytowy można zbudować również na pasmach częstotliwości otwartych przeznaczonych w tym celu przez przepisy powszechnie obowiązującego prawa co również dopuszcza zamawiający ale w ilości nie więcej aniżeli 10% lokalizacji;

Zamawiający wskazał, że zgodnie z pkt 1.1.1.1. OPZ w ramach zamówienia wykonawca ma obowiązek m.in. wdrożenia oraz obsługi systemu odczytowego na terenie miasta Katowice opartego na technologii Internetu Rzeczy (IoT) stanowiącego element smart City w zakresie monitoringu sieci wodociągowej. System musi korzystać z komunikacji radiowej w licencjonowanych pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych.

Mając na względzie powyższe, jak również obecnie obowiązujące przepisy ustawy z dnia 12 lipca 2024r. Prawo komunikacji elektronicznej (Dz. U. z 2024r. poz. 1221), a także przez wzgląd na ustawę z dnia 12 lipca 2024r. Przepisy wprowadzające ustawę — Prawo komunikacji elektronicznej (Dz. U. z 2024r. poz. 1222) oraz w znacznej mierze nie obowiązującą już ustawę z dnia 16 lipca 2004r. Prawo telekomunikacyjne (tj. Dz. U. z 2024 poz. 34 z późn. zm.), pod pojęciem pasma licencjonowanego należy rozumieć pasmo radiowe jako zakres częstotliwości radiowych, którego używanie do emisji i odbioru sygnałów radiowych wymaga uzyskania zezwolenia (rezerwacji) od właściwego organu regulacyjnego, tj. Prezes Urzędu Komunikacji Elektronicznej (UKE). Zgodnie z art. 2 pkt 50) PKE za rezerwację częstotliwości uznaje się określenie częstotliwości lub zasobów orbitalnych, które we wskazanym w rezerwacji okresie pozostają w dyspozycji podmiotu na rzecz którego dokonano rezerwacji, przeniesiono uprawnienia do częstotliwości lub uprawnienia do dysponowania częstotliwościami na cele związane z uzyskiwaniem pozwoleń radiowych. Ponadto, w świetle art. 69 PKE rezerwacja częstotliwości jest dokonywana o ile podmiot wnioskujący spełnia m.in. warunki dotyczące należytej ochrony przed szkodliwymi zakłóceniami, a także mogą być wykorzystywane przez urządzenie radiowe bez powodowania szkodliwych zakłóceń lub kolizji z przyznanymi na rzecz innych podmiotów rezerwacjami, przydziałami częstotliwości, pozwoleń radiowymi lub decyzjami, o których mowa w art. 152 ust. 1 lub art. 153 ust. 1 PKE.

Zamawiający wskazał, że przeciwieństwem pasma licencjonowanego jest pasmo otwarte, nielicencjonowane (publiczne) które posiada ze swej istoty słabszą ochronę przez zewnętrzną ingerencją, jest podatne za zakłócenia lub

utrata danych, jak również podlega ograniczeniom technicznym. Technologie wykorzystujące pasmo otwarte tracą bowiem zasięg w funkcji zajętości tych pasm, co przekłada się na utratę transmisji danych w zwartych, gęstych lokalizacjach, jak ma miejsce na obszarze Gminy Katowice. Jednocześnie fakt, że technologie te działają na pasmach nielicencjonowanych powoduje, że pasma te mogą być współdzielone z nieograniczoną liczbą innych transmisji, co skutkuje spadkiem efektywności przekazu danych, coraz gorszymi parametrami przesyłu danych, a nakładanie się wielu transmisji może prowadzić do utraty danych. Stąd bez wątpienia zaletą pasma licencjonowanego jest m.in.:

- operator (np. telekomunikacyjny) otrzymuje wyłączne prawo do wykorzystywania danego fragmentu widma radiowego na określonym obszarze i przez określony czas;
- inne podmioty nie mogą nadawać w tym paśmie bez zgody adresata zezwolenia;
- organ regulacyjny zapewnia ochronę przed zakłóceniami i egzekwuje przestrzeganie zasad technicznych (np. moc, modulacja, czas pracy);
- gwarancja jakości transmisji: brak ryzyka interferencji z nieautoryzowanymi źródłami (w przeciwieństwie do pasm otwartych);

- kontrola regulacyjna: parametry techniczne są zatwierdzane i nadzorowane przez UKE; bezpieczeństwo i niezawodność: umożliwia stabilną i przewidywalną transmisję danych szczególnie istotne w systemach krytycznych.

Z kolei w systemie pracującym w paśmie nielicencjonowanym zamawiający nie ma żadnej gwarancji, że dana lokalizacja nie zostanie zakłócona przez inne źródło emisji - np. urządzenia LoRaWAN innego podmiotu, sieci miejskie lub przemysłowe. Stąd dopuszczenie takiej transmisji tylko w maksymalnie 10% lokalizacji:

- jest proporcjonalne, bo nie eliminuje technologii LoRa całkowicie,
- jest racjonalne, bo pozwala wykorzystać tę technologię w sytuacjach szczególnych (np. brak zasięgu GSM),
- jest uzasadnione, bo chroni interes publiczny i zapewnia zgodność z przepisami bezpieczeństwa.

Zamawiający prezentuje poniżej porównanie tabelaryczne technologii wykorzystywanych w pasmach licencjonowanych oraz nielicencjonowanych:

Kryterium	Pasmo licencjonowane (np. NB-10T, LTE-M)	Pasmo nielicencjonowane (np. LoRa 868 MHz)
Regulacja prawna	Pasmo przydzielane i kontrolowane przez UKE (licencje krajowe dla operatorów)	Pasmo ogólnodostępne (ISM), bez gwarancji ochrony przed zakłóceniami
Zarządzanie dostępem	Gwarantowana przepustowość, kontrola przeciążenia i harmonogramu transmisji	Brak koordynacji - wielu użytkowników może powodować interferencje i kolizje pakietów
Odporność na zakłócenia	Wysoka - dostęp kontrolowany, chronione stacje bazowe z innych urządzeń (np. smart home, alarmy, automatyka)	Niska — możliwe zakłócenia
Zasięg	Stabilny w obszarach miejskich, wykorzystanie istniejącej infrastruktury (antena co 0,5-3 km w miastach), zależność od lokalizacji	Wymaga budowy własnej sieci
Bezpieczeństwo transmisji	Szyfrowanie na poziomie sieci komórkowej, pełna kontrola transmisji	Konieczność stosowania własnych protokołów szyfrowania; otwarte medium transmisji podatne na ataki Gamming, sniffing)
Niezależność od własnej sieci	Tak - brak konieczności instalacji anten przez zamawiającego	Nie - wymagana instalacja i utrzymanie infrastruktury (anteny, gatewaye, serwery)
Koszty początkowe	Niższe - brak kosztów budowy infrastruktury	Wyższe - zakup, montaż, utrzymanie, serwisowanie infrastruktury transmisyjnej
Utrzymanie/serwis	Oparte o umowy z operatorem GSM (dostępność 24/7)	Ryzyko awarii własnej infrastruktury, wymagane własne zasoby utrzymaniowe
Zgodność z wymaganiami NIS2 /UKSC	Tak - pełna segmentacja, tunel VPN, transmisja w paśmie nadzorowanym	Wymaga wielu dodatkowych zabezpieczeń; większe ryzyko nieautoryzowanego dostępu lub awarii systemu krytycznego

Zamawiający podniósł również, że istotnym czynnikiem mającym wpływ na określenie warunków zamówienia, w tym wybór systemu komunikacji radiowej jest szczególny charakter zamawiającego jako przedsiębiorstwa wodociągowo-kanalizacyjnego w rozumieniu art. 2 pkt 4) ustawy z dnia 7 czerwca 2001r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (tj. Dz. U. z 2024r. poz. 757 z późn. zm.), które posiada i zarządza infrastrukturą krytyczną jaką są m.in. systemy zaopatrzenia w wodę lub odprowadzania ścieków. Zgodnie ze stanowiskiem Rządowego Centrum Bezpieczeństwa do infrastruktury krytycznej zaliczyć należy systemy zaopatrzenia w wodę czy sieci teleinformatyczne. Istotnym zadaniem związanym z infrastrukturą krytyczną jest nie tylko powinnośc zapewnienia jej ochrony przed zagrożeniami, ale również zapewnienie by ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki (zob. <https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej>; podobnie Śląski Urząd Wojewódzki w Katowicach, Wydział Bezpieczeństwa i Zarządzania Kryzysowego, <https://www.katowice.uw.gov.pl/wydzial/wydzial-bezpieczenstwa-i-zarządzania-kryzysowego/infrastruktura-krytyczna-l>). Stąd, tak istotnym jest ukształtowanie wymogu korzystania z

licencjonowanego pasma radiowego do zdalnego odczytu wodomierzy na poziomie 90%, z jednoczesnym dopuszczeniem zaledwie 10% korzystania z pasma otwartego, co w sposób bezpośredni wpływa na zapewnienia bezpieczeństwa Spółki i jej zasobów infrastrukturalnych.

Zamawiający podkreślił, że ustanowienie powyższego wymogu uzasadnione jest również charakterem działalności zamawiającego jako podmiotu kluczowego w rozumieniu dyrektywy NIS2 (dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) art. 3 pkt 1 lit. e) - Dz.Urz.UE.L 2022 Nr 333, str. 80). Zgodnie bowiem z art. 3 ust. 1 lit. e) Dyrektywy za podmioty kluczowe uznaje się inne podmioty w rodzaju tych, o których mowa w załączniku I lub II, które zostały wskazane przez państwo członkowskie jako podmioty kluczowe zgodnie z art. 2 ust. 2 lit. b)-e) Dyrektywy. Załącznik nr I lub II wskazuje, że sektorem kluczowym jest zarówno woda pitna, realizowana przez dostawców i dystrybutorów wody przeznaczonej do spożycia przez ludzi zdefiniowanej w art. 2 pkt 1 lit. a) dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/2184, jak również ścieki realizowane przez przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe lub przemysłowe zgodnie z definicją w art. 2 pkt 1, 2 i 3 dyrektywy Rady 91/271/EWG.

Zamawiający podlega podmiotowo pod Krajowy System Cyberbezpieczeństwa zarówno jako spółka prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz.U. z 2021r. poz. 679), jak również jako operator usługi kluczowej, którą jest zaopatrzenie w wodę pitną i jej dystrybucja (zob. załącznik nr 1 do ustawy z dnia 5 lipca 2018r. o Krajowym Systemie Cyberbezpieczeństwa - tj. Dz. U. z 2024r. poz. 1077, dalej ustawa KSC). Wobec tego, zamawiający ma nie tylko prawo, ale obowiązek, by wybierać rozwiązania adekwatne do poziomu ryzyka. Zgodnie z art. 21 ust. 2 dyrektywy NIS2 oraz art. 8 KSC zadaniem zamawiającego jest wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym m.in.:

- a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
- b) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
- c) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągle i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
- d) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;
- e) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
  - 1) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
  - 2) dbałość o aktualizację oprogramowania,
  - 3) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
  - 4) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
  - 5) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Zatem zamawiający ma prawo wymagać technologii o przewidywalnej strukturze zaufania i architekturze zgodnej z NIS2. Publiczna sieć, jaką zdaje się oferować wykonawca to środowisko o nieokreślonym poziomie zaufania. Tymczasem infrastruktura odczytowa wodomierzy stanowi:

- źródło danych rozliczeniowych (wrażliwość prawna i konsumencka), dane topologiczne, eksploatacyjne i symulacyjne (np. analiza wycieków)W świetle NIS2 (załącznik I i III), tego typu systemy muszą być odseparowane od sieci publicznej, jeśli istnieje taka możliwość a technologia GSM z dedykowanym APN i tunelem VPN taką możliwość zapewnia.

Ponadto, zamawiający jako administrator danych osobowych winien również podjąć stosowne działania w celu zapewnienia ochrony danych osobowych odbiorców świadczonych usług. Zgodnie z art. 4 pkt 1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO) „dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. W tym kontekście nie ulega wątpliwości, że dane pomiarowe to informacje wskazujące o wielkości zużycia, rejestrowane przez układ rejestrowopomiarowy u danego

odbiorcy, będącego osobą fizyczną. Na podstawie zebranych informacji o zużyciu mediów, przy wykorzystaniu adresu odbiorcy (np. skrzynka z licznikiem znajdująca się bezpośrednio przy posesji), można ustalić informacje na temat konkretnej osoby oraz inne cechy identyfikujące pośrednio osobę fizyczną np. średnioroczne, okresowe zapotrzebowania na wodę, szacunkową wartość opłat, itp. W takim przypadku zamawiający jako administrator danych osobowych ma obowiązek zapewnienia danym osobowym należyty poziom ochrony przed wystąpieniem naruszenia bezpieczeństwa, a prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, art. 4 pkt. 12) RODO.

W rezultacie przedmiot zamówienia został opisany z uwzględnieniem obiektywnych i uzasadnionych potrzeb zamawiającego jako przedsięwzięcia wodociągowo-kanalizacyjnego, jak również przez pryzmat uwarunkowań prawnych w jakich znajduje się zamawiający. Ich realizacja w sposób naturalny może skutkować tym, że liczba wykonawców zdolnych do wykonania zamówienia będzie ograniczona. Jednakże z okoliczności tej, że na rynku występują wykonawcy nie oferujący danego rodzaju usług lub też dla których jego realizacja jest utrudniona czy wymaga pewnego dostosowania oferowanego przez nich produktu do wymagań zamawiającego, absolutnie nie przesądza automatycznie o naruszeniu zasad postępowania, w tym uczciwej konkurencji.

Ponadto zamawiający wskazał, że przedmiot zamówienia obejmuje wdrożenie systemu odczytu wodomierzy dla infrastruktury wodociągowej w Katowicach - miasta będącego aglomeracją i centrum wojewódzkim, gdzie niezawodność i bezpieczeństwo danych pomiarowych ma bezpośredni wpływ na ciągłość świadczenia usług kluczowych dla ludności. Podkreślił, że poza okolicznościami wymienionymi w pkt II, na treść warunków zamówienia, w tym kwestionowanego warunku by system musiał korzystać z komunikacji radiowej w licencjonowanych pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych (I Opis ogólny pkt 1 Przedmiot zamówienia ppkt 1.1. Opis Przedmiotu Zamówienia - pkt 1.1.1. OPZ) kluczowy wpływ miały również czynniki związane z typem zabudowy i topografią miasta Katowice oraz powiązanej z tym ilością mieszkańców poszczególnych dzielnic, ilością studni wodomierzowych na terenie miasta i szacunkowej ilości trudnych lokalizacji.

Zamawiający przedstawił:

- 1) przybliżoną liczbę ludności poszczególnych dzielnic miasta Katowice (Tabela nr 1 oraz grafika);
- 2) liczbę studni wodomierzowych poszczególnych dzielnic Katowice (Tabela nr 2 oraz grafika);
- 3) liczbę ludności/studni wodomierzowych w poszczególnych dzielnicach wraz z opisem typu zabudowań (Tabela nr 3).

Tabela 1 - „Liczba ludności w poszczególnych dzielnicach Katowic”

Dzielnica	Liczba Ludności
Śródmieście	25320
Koszutka	10121
Bogucice	13426
Osiedle Paderewskiego-Muchowiec	11336
Wetnowiec-Józefowiec	13741
Dąb	6914
Załęże	8589
Osiedle Witosa	12123
Osiedle Tysiąclecia	20831
Załęska Hałda-Brynów (część zachodnia)	13681
Brynów-Osiedle Zgrzebniocka (część wschodnia)	6384
Ligota-Panewniki	28286
Zawodzie	10835
Dąbrówka Mała	4619
Szopienice-Burowiec	13557
Janów-Nikiszowiec	9136
Giszowiec	15409
Piotrowice-Ochojec	22369
Zarzecze	2851
Kostuchna	11518
Podlesie	6645
Murcki	4840
SUMA	272531

Ilość mieszkańców poszczególnych dzielnic w Katowicach

•Śródmieście

KostuchnapodlesMurcki            Śródmieście  
 Koszutka  
 Piotrowice-Ochojec            Bogucice  
 Bogucice  
 •Osiedle Paderewskiego5%  
 Osiedle            Muchowiec  
 Paderewskiego-            Welnowiec-Józefowiec  
 Giszowiec  
 Muchowiec  
 6%• Dąb  
 WelnowiecJanów-NikiszowiecJózefowiec            • Załęże  
 Osiedle Witosy  
 Dąb  
 Szopienice-Burowiec  
 5%            • Osiedle Tysiąclecia  
 Załęże  
 Dąbrówka Mała  
 Załęska Hałda-Brynów (część  
 Zawodzie            Osiedle Witosy            zachodnia)  
 4%            4%            • Brynów-Osiedle Zgrzebnika  
 (część wschodnia)  
 Ligota-Panewniki  
 2%            5%

Tabela 2 - „Liczba studni wodomierzowych w poszczególnych dzielnicach Katowic”

Dzielnica	Liczba studni
Podlesie	185
Piotrowice - Ochojec	155
Ligota - Panewniki	136
Kostuchna	117
Zarzecze	111
Szopienice - Burowiec	64
Śródmieście	64
Załęska Hałda - Brynów (część zachodnia)	50
Murcki	47
Osiedle Zgrzebnika - Brynów (część wschodnia)	45
Welnowiec - Józefowiec	37
Osiedle Witosy	35
Giszowiec	34
Janów - Nikiszowiec	31
Osiedle Paderewskiego - Muchowiec	31
Dąb	29
Zawodzie	27
Dąbrówka Mała	26
Bogucice	22
Załęże	21
Koszutka	19
Osiedle Tysiąclecia	8

Liczba lokalizacji studni w poszczególnych dzielnicach Katowic

09

Dzielnica

Tabela 3 - „Liczba ludności/studni wodomierzowych w poszczególnych dzielnicach Katowic wraz z opisem typu zabudowań”

Dzielnica	Liczba Ludności	Liczba studni	yp zabudowy
Śródmieście	25320	64	kamienice z XIX i XX w., biurowce, obiekty publiczne, bloki

Koszutka	10121	19	przedwojenne kamienice, bloki powojenne, zwarta zabudowa	
Bogucice	13426	22	przedwojenne kamienice, bloki powojenne, osiedla robotnicze	
Osiedle Paderewskiego	Muchowiec	11336	31	wysokie wielkopłytowe loki mieszkalne z lat o. i 90. xx w., zabudowa apartamentowa
Welnowiec-Józefowiec	13741	37	zabudowa jednorodzinna, stare kamienice, nowe osiedla	
Dąb	6914	29	stare ceglane kamienice, nowe budownictwo mieszkaniowe	
Załęże	8589	21	stare ceglane kamienice, nowe budownictwo mieszkaniowe, tereny przemysłowe	
Osiedle Witosa	12123	35	wielkopłytowe osiedle mieszkaniowe	
Osiedle Tysiąclecia	20831	8	wielkopłytowe osiedle mieszkaniowe, wysokie loki	
Załęska Hałda-Brynów (część zachodnia)	13681	50	ceglane domy, bloki, nowe osiedla deweloperskie	
Brynów-Osiedle Zgrzebnioła (część wschodnia)	6384	45	ceglane domy, bloki, nowe osiedla deweloperskie	
Ligota-Panewniki	28286	136	Domy jednorodzinne, wille, zabudowa wielorodzinna	
Zawodzie	10835	27	stare domy i kamienice, współczesne osiedla	
Dąbrówka Mała	4619	26	stare domy i kamienice, współczesne osiedla, zabudowa przemysłowa	
Szopienice-Burowiec	13557	64	przedwojenne kamienice, bloki z wielkiej płyty, obszary przemysłowe	
Janów-Nikiszowiec	9136	31	Historyczne osiedl robotnicze (kolonia górnicza), teren przemysłowe	
Giszowiec	15409	34	Historyczne osiedl robotnicze (kolonia górnicza) wysokie bloki wielkiej płyty	
Piotrowice-Ochojec	22369	155	Budownictwo jednorodzinne, nowsze bloki i apartamenty	
Zarzecze	2851	111	zabudowa jednorodzinna	
Kostuchna	11518	117	zabudowa jednorodzinna	
Podlesie	6645	185	zabudowa jednorodzinna	
Murcki	4840	47	Dawne osiedle górnicze, zabudowa jednorodzinna	

Jak wynika z powyższego liczba mieszkańców poszczególnych dzielnic Katowic, powiązany z tym rozkład studni wodomierzowych, a także ukształtowanie terenu i urbanistyka mają kluczowe znaczenie dla realizacji oczekiwanego od zamawiającego zamówienia, wpływając bezpośrednio na jakość i stabilność transmisji danych.

Zamawiający poinformował, że obszarem realizacji przyszłego zamówienia jest miasto Katowice. Katowice leżą na pograniczu Wyżyny Śląskiej i Pogórza Karpackiego, z lokalnymi wzniesieniami i obniżeniami (np. doliny Rawy, Kłodnicy). Różnice wysokości terenu (w granicach 100-120 m) mogą wpływać na tłumienie sygnału radiowego, szczególnie w dolinach, zagłębieniach terenu lub za barierami naturalnymi (np. wzgórza leśne w Ligocie, Panewnikach, Murckach). Propagacja fal radiowych może być w niektórych przypadkach ograniczana przez przesłonięcia terenowe — zwłaszcza przy gęstym zabudowaniu i braku widoczności anten bazowych. W zakresie charakterystyki zabudowy należy wskazać, że w obszarze dzielnic Śródmieście, Koszutka, Załęże, Zawodzie występuje gęsta i zwarta zabudowa wielorodzinna oraz kamieniczna, często o grubych ścianach, co znacznie osłabia sygnał wewnątrz budynków. Z kolei Nikiszowiec oraz Giszowiec to wysokie bloki (Giszowiec), historyczna zabudowa familokowa z grubymi murami ceglanymi i zwartą strukturą, która utrudnia propagację fal. Obszary dzielnic Ligota, Panewniki, Kostuchna, Zarzecze cechuje wysokie rozproszenie zabudowy jednorodzinnej z większymi odległościami między budynkami, co może prowadzić do luk w zasięgu. W obiektach podziemnych (np. wodomierze w piwnicach) sygnał radiowy może być niedostateczny bez zastosowania retransmiterów lub anten zewnętrznych.

Ponadto w obszarach tych występują zjawiska propagacyjne zakłócające jakość i powodujące utratę stabilności transmisji. Bez wątpienia zastosowane w obiektach budowlanych materiały budowlane (żelbet, cegła, stal konstrukcyjna) oraz zjawisko wielodrożności występujące w środowisku miejskim wpływa negatywnie na jakość transmisji w technologiach LPWAN. W przypadku pomiarów instalowanych w piwnicach, szachtach technicznych lub metalowych obudowach - również skutkuje brakiem stabilnej łączności. Stąd pomimo szerokiego zasięgu NB-IoT i LTE-M, warunki terenowe i urbanistyczne Katowic mogą prowadzić do problemów z dostępnością sygnału w pojedynczych lokalizacjach, szczególnie przy instalacjach:

- w podziemiach lub wnętrzach klatek schodowych,
- w budynkach z grubymi ścianami nośnymi lub ekranowaniem metalowym,
- w dolinach i depresjach terenowych.

Zamawiający podkreślił, że przez wzgląd na opisane powyżej uwarunkowania - zróżnicowane ukształtowanie terenu,

gęstość i typ zabudowy, a także występujące zjawiska propagacyjne zamawiający w sposób świadomy i technicznie uzasadniony dopuścił możliwość zastosowania transmisji danych w paśmie nielicencjonowanym (np. LoRaWAN) w ograniczonym zakresie, do maksymalnie 10% lokalizacji.

Dowód: 1) Mapa dzielnic Katowic z uwzględnieniem ilości mieszkańców i trudnych lokalizacji pod względem możliwości stacjonarnego odczytu wodomierzy; 2) Wykaz tabelaryczny trudnych lokalizacji

•wniosek zamawiającego o zastrzeżenie tajemnicy - art. 545 ust. 3 ustawy

Na podstawie powyższych ustaleń zamawiający dopuszcza użycie pasm nielicencjonowanych na maksymalnie 10 % lokalizacji, aby:

•Zapewnić łączność tam, gdzie zakres licencjonowany może zawodzić z powodu topografii (dolina, załamania terenu), zabudowy (grube mury, piwnice), czy zakłóceń środowiskowych.

•Zachować ogólnie wysoką efektywność systemu w pasmach licencjonowanych (np. NB-IoT, LTE-M), korzystając jednocześnie z elastyczności technologii alternatywnych tam, gdzie potrzebna jest niezawodność odczytu.

Zamawiający określając warunki zamówienia w żaden sposób, nie miał na celu ograniczenie konkurencji, lecz zapewnienie elastyczności technologicznej w trudnych lokalizacjach, gdzie sygnał w paśmie licencjonowanym może być niewystarczający z powodów fizycznych i technicznych - np. przy głębokim osadzeniu wodomierzy w piwnicach, braku widoczności stacji bazowej, zaburzeniach propagacji w zwartej zabudowie historycznej lub zakłóceniach elektromagnetycznych. Dopuszczenie ograniczonego udziału technologii działających w paśmie nielicencjonowanym stanowi zatem racjonalny kompromis, który umożliwia spełnienie wymagań funkcjonalnych (m.in. niezawodny odczyt), przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa transmisji i zgodności z obowiązującymi regulacjami w zakresie cyberbezpieczeństwa, ochrony danych i zarządzania infrastrukturą krytyczną.

Zgodnie z art. 99 ust. 4 ustawy, przedmiotu zamówienia nie wolno opisywać w sposób nieuzasadniony, który mógłby utrudniać uczciwą konkurencję. W tym przypadku jednak ograniczenie techniczne wynika bezpośrednio z obiektywnych potrzeb zamawiającego i charakterystyki zamówienia. KIO w analogicznej sprawie podkreśliła, że zamawiający ma prawo określić konkretne wymagania techniczne, jeśli dyktują to uzasadnione potrzeby - wówczas nie dochodzi do naruszenia art. 99 ustawy. Wymóg użycia licencjonowanego pasma służy realizacji ustawowych obowiązków zamawiającego w zakresie ochrony infrastruktury krytycznej i zapewnienia ciągłości usług kluczowych. Nie jest on kaprysem ani próbą preferowania określonego wykonawcy, lecz racjonalnym środkiem technicznym proporcjonalnym do założonych celów (bezpieczeństwo i jakość systemu). Podkreślił, że rynek wcale nie jest zamknięty na jednego dostawcę - wręcz przeciwnie, obecnie kilku operatorów komórkowych (np. T-Mobile, Orange, Plus) oferuje rozwiązania NB-IoT, LTE-M, a moduły odczytowe produkuje wielu renomowanych producentów (w tym firmy polskie). Alternatywne technologie radiowe zaś - choć pozornie tańsze (bez uwzględnienia budowy sieci) - nie gwarantują spełnienia wymagań stabilności transmisji w długim horyzoncie. Dlatego utrzymanie tego wymogu w OPZ jest w pełni uzasadnione i zgodne z zasadą proporcjonalności. Zamawiający dopuszcza wykorzystanie pasm otwartych wyłącznie w uzasadnionych przypadkach (maksymalnie 10% lokalizacji) tj. gdy niemożliwe jest uzyskanie w danej lokalizacji zasięgu w paśmie licencjonowanym.

Ad 3) Utrudnianie warunków konkurowania poprzez wskazanie „pasma licencjonowanego” co predysponuje do realizacji usługi operatorów mobilnych posiadających rezerwację częstotliwości a jednocześnie wyklucza innych przedsiębiorców telekomunikacyjnych mogących świadczyć usługi na rzecz Zamawiającego ale nie posiadających rezerwacji częstotliwości;

Zamawiający nie narzucił konkretnej marki, producenta ani protokołu. Narzuca wymóg skuteczności i niezawodności, które w jego ocenie — popartej okolicznościami wskazanymi powyżej w niniejszym piśmie mogą być spełnione przede wszystkim przez systemy działające w paśmie licencjonowanym. Zamawiający wskazał, co zresztą przyznaje sam odwołujący, że na rynku usług telekomunikacyjnych są podmioty zdolne do przesyłu danych pasmami licencjonowanymi (w ramach otrzymanych rezerwacji częstotliwości) jak np. Polkomtel sp. z o.o., Orange Polska S.A., T-Mobile Polska S.A. czy P4 sp. z o.o. Zatem nie może być mowy o jakikolwiek ograniczeniu konkurencji, a rolą zamawiającego nie jest dostosowanie OPZ pod warunki konkretnego wykonawcy, co przy uwzględnieniu żądań odwołującego miałyby niewątpliwie miejsce.

Zamawiający wskazał, że stosownie do treści art. 96 ustawy Prawo komunikacji elektronicznej podmiot dysponujący rezerwacją częstotliwości może wydzierżawić lub przekazać do użytkowania na podstawie innego tytułu prawnego częstotliwości objęte rezerwacją częstotliwości, na rzecz innego podmiotu. W rezultacie odwołujący, w drodze np. umowy cywilnoprawnej może stać się posiadaczem rezerwacji częstotliwości, a więc świadczyć usługę w oczekiwany przez zamawiającego paśmie licencjonowanym. Nie sposób zatem mówić o ograniczeniu konkurencji, czy nierównym traktowaniu wykonawców albowiem zapewnienie dostępu do danej częstotliwości leży po stronie wykonawcy, oraz to w interesie danego wykonawcy jest podjęcie wszelkich kroków prawnych zmierzających do zapewnienia tego dostępu na dowolnych zasadach rynkowych w toku realizacji umowy.

Ad 4) Postawienie wymogu pasma licencjonowanego dla 90% lokalizacji, nie znajduje żadnego obiektywnego uzasadnienia technicznego ani funkcjonalnego bowiem zarówno transmisja w paśmie licencjonowanym, jak i w nielicencjonowanym ma zamawiającemu zapewnić identyczne parametry jakościowe w tym m.in. odczyt z co najmniej 90% urządzeń raz dziennie, z 95% raz w tygodniu, i z 98% raz w miesiącu. Zatem - skoro wymagania SLA są jednakowe bez względu na zastosowaną technologię transmisji, to naruszenie obowiązku stosowania pasm licencjonowanego w 90% przypadków jest nieproporcjonalne oraz prowadzi do bezpodstawnego ograniczenia konkurencji.

Zgodnie z pkt V.2.5) OPZ oczekiwaniem zamawiającego jest by wykonawca zapewnił określony poziom odczytywania danych (SLA), który nie może być mniejszy niż:

- a. 90% objętych nim modułów radiowych IoT - 1 raz w ciągu doby;
- b. 95% objętych nim modułów radiowych IoT - 1 raz na 7 dni kalendarzowych;
- c. 98% objętych nim modułów radiowych IoT - przynajmniej 1 raz w miesiącu;

Poziom odczytu będzie ustalany na podstawie faktycznie działających modułów radiowych IoT, a skuteczny odczyt obejmuje przesłanie wszystkich wymaganych danych (w tym indeksów, alarmów, i danych historycznych, itd.) do platformy odczytowej.

Zamawiający wskazał, że rzeczywiście OPZ określa jednolite progi SLA (tj. 90% odczytów dziennie, 95% tygodniowo, 98% miesięcznie), co w żaden sposób nie oznacza, że wszystkie technologie transmisji oferują takie samo prawdopodobieństwo osiągnięcia tych progów w warunkach rzeczywistych. Zamawiający, bazując na praktyce operacyjnej, testach wdrożeniowych analizach ryzyka, ma świadomość, że:

Transmisja w paśmie nielicencjonowanym (np. LoRa) jest obciążona istotnymi ograniczeniami:

ograniczenie duty-cycle (cykl pracy) do 1% (lub mniej), co wpływa na możliwość retransmisji, o brak gwarancji jakości transmisji (brak QoS - Quality of Service), o brak ochrony przed zakłóceniami i interferencją z innymi systemami (np. smart home, systemy alarmowe), o brak wsparcia operatora i egzekwowania odpowiedzialności za zakłócenia, Transmisja w paśmie licencjonowanym (np. NB-IoT, LTE-M):

- korzysta z pasma chronionego regulacyjnie, wyłączanego dla operatora,
- umożliwia centralne zarządzanie parametrami transmisji (moc, QoS),
- posiada mechanizmy retransmisji, szyfrowania i uwierzytelniania wynikające ze standardów 3GPP.

W rezultacie to właśnie transmisja w paśmie licencjonowanym gwarantuje znacznie większe prawdopodobieństwo realizacji SLA a także minimalizuje konieczność interwencji serwisowych i odczytów manualnych.

Ad zarzut wymogu korzystania z wydzielonej podsieci APN oraz posiadania własnej infrastruktury w co najmniej 90% uprzywilejowuje spółkę Orange Polska S.A. jako wykonawcę, ponieważ tylko ten podmiot posiada własną infrastrukturę telekomunikacyjną mobilną na obszarze aglomeracji Katowickiej. Wyklucza pozostałych uczestników rynku, w tym wielu wykonawców posiadających kompetencje techniczne i organizacyjne do realizacji zamówienia, którzy korzystają z infrastruktury dzierżawionej lub współdzielonej (np. MVNO, integratorzy, operatorzy hurtowi lub podmioty które leasingują infrastrukturę jak P4 sp. z o.o. lub Polkomtel sp. z o.o.). Preferuje określony model biznesowy, tj. operatorów posiadających własną sieć fizyczną, przy czym nawet ci wykonawcy nie są w stanie w pełni spełnić tego wymogu.

Zgodnie z pkt V.I.I) OPZ [Wymagania ogólne] wykonawca zobowiązuje się do wdrożenia systemu odczytowego umożliwiającego odczyt danych z urządzeń pomiarowych na całym obszarze działania zamawiającego. System musi opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną wykonawcy.

Zamawiający wskazał, że wymóg OPZ korzystania z dedykowanej podsieci APN oznacza, że dane telemetryczne nie mogą być przesyłane przez publiczny Internet (pasmem otwartym). Jak już wskazano powyżej w odpowiedzi na zarzut pierwszy, wymóg ten podyktowany jest przede wszystkim charakterem zamawiającego jako podmiotu publicznego zarządzającego infrastrukturą krytyczną, a także pozostaje w pełnej zgodzie z:

- praktyką sektorową w zakresie IoT w infrastrukturze krytycznej,
  - wytycznymi Ministerstwa Cyfryzacji dla podmiotów kluczowych,
- wymaganiami wynikającymi z art. 21 ust. 2 lit. e dyrektywy NIS2: „wprowadzenie segmentacji i kontroli komunikacji”.

Dedykowany APN

- umożliwia utworzenie logicznej, wydzielonej sieci transmisji danych - izolowanej od publicznych zasobów sieciowych.
- Ułatwia szyfrowanie end-to-end (moduł system - API Zamawiającego), zgodnie z wymaganiami TLS 1.3 i AES 128-bit wskazanymi w OPZ.
- Pozwala operatorowi świadczącemu usługę transmisji lepiej kontrolować opóźnienia, priorytetyzację pakietów, redundancję tras i alarmowanie.

Wymaganie dedykowanego APN nie narusza zasad uczciwej konkurencji - jest technicznie uzasadnione, a jego wdrożenie jest dostępne dla wszystkich renomowanych wykonawców dysponujących siecią GSM.

W zakresie zarzutu dotyczącego „własnej infrastruktury” to należy wskazać, że nie odpowiada prawdzie, jako wolą

Zamawiającego jest preferowanie spółki ORANGE POLSKA S.A. jako jedynej posiadającej taką infrastrukturę. Odwołujący, na str. 7 odwołania sam wskazuje, że podmiotami które mogą świadczyć usługę są m.in. Polkomtel sp. z o.o., Orange Polska S.A., T-Mobile Polska S.A. czy P4 sp. z o.o.

Zamawiający wyjaśnił, że nie stawia wymogu posiadania infrastruktury fizycznej w znaczeniu prawa własności, lecz wymaga, aby wykonawca miał pełną, niezależną kontrolę nad infrastrukturą transmisyjną wykorzystywaną w minimum 90% przypadków w tym w szczególności:

- możliwość stałego monitorowania i zarządzania ruchem IP,
  - gwarancję poziomu SLA (Service Level Agreement),
- niezależność operacyjną w zakresie dostępności, rekonfiguracji i rozliczalności danych,
- możliwość jednoznacznego zapewnienia integralności i bezpieczeństwa danych w warstwie sieciowej.

W rezultacie pojęcie „własna infrastruktura” należy rozumieć jako infrastrukturę, do której wykonawca posiada wyłączne prawo dysponowania na poziomie operacyjnym i konfiguracyjnym, a nie jako konieczność bycia właścicielem masztów lub światłowodów. Oznacza to, że:

- wykonawca może korzystać z infrastruktury dzierżawionej lub leasingowanej, o ile ma pełną kontrolę nad usługą transmisji danych (np. APN, VPN, routing, adresacja),
  - celem wymogu jest ograniczenie ryzyka związanego z usługą przekazywaną „w podwykonawstwo kaskadowe” lub przez model dzielonej odpowiedzialności (np. MVNO bez bezpośredniej umowy SLA z operatorem sieci dostępowej).

Zamawiający podkreślił, że istotnym czynnikiem, który uwzględnił przy formułowaniu warunków OPZ było „wykorzystanie istniejącej infrastruktury telekomunikacyjnej” umożliwiającej realizację zamówienia, wykluczając tym samym możliwość jest „budowy nie jako ad hoc na potrzeby zamówienia. Budowa infrastruktury telekomunikacyjnej nie jest przedmiotem zamówienia, stąd wykonawca musi dysponować możliwie najszerszym prawem do korzystania z niej, by zapewnić wykonanie i ochronę posiadanej przez zamawiającego infrastruktury krytycznej. Wykorzystanie istniejącej infrastruktury oraz skorzystanie z technologii w ramach pasma licencjonowanego umożliwia przesył istniejącą siecią komórkową, eliminując potrzebę budowy własnej sieci komunikacyjnej przez Spółkę a w tym samym uniknięcia:

- Problemów z wejściem w teren;

Potrzebę wykorzystania elementów urbanistycznych - koszty dzierżawy i energii elektrycznej;

- Zaangażowanie służb technicznych do obsługi sieci;
- Dewastacje i kradzieże;
- Aspekt społeczny.

Zatem wykorzystanie istniejącej infrastruktury oraz zastosowanie odpowiedniej technologii w ramach pasm radiowych licencjonowanych cechuje się m.in.:

- 1) szerokim zasięgiem i dobrą penetracją sygnału pozwalając na pozyskanie odczytu z trudnych lokalizacji tj. piwnice, studzienki wodomierzowe itd.;
- 2) niezawodnością - dostępność i odporność sieci komunikacyjnej są fundamentalne dla zapewnienia ciągłości przepływu danych. Zastosowane technologie będą korzystały z potencjalnie niezawodnych sieci operatorskich GSM. Dostępna duża ilość BTS-ów (stacji bazowych) w Katowicach jest gwarantem pokryciem zasięgiem całego miasta;
- 3) skalowalnością - system zdolny do obsługi dużej liczby punktów pomiarowych oraz przetwarzania generowanej przez nie objętości danych. Technologie stosowane w ramach pasm licencjonowanych zostały zaprojektowane z myślą o masowych połączeniach;
- 4) stabilnością i niezawodnością - działanie w licencjonowanym paśmie minimalizuje zakłócenia i zapewnia większą skuteczność odczytów;
- 5) bezpieczeństwo - ochrona danych podczas transmisji i przechowywania jest absolutnym priorytetem dla podmiotów kluczowych. Systemy IoT wprowadzają nowe potencjalne wektory ataków. Technologie stosowane w pasmach licencjonowanych wykorzystują najwyższe standardy bezpieczeństwa sieci komórkowych - zgodne z UKSC oraz dyrektywą NIS2;
- 6) żywotność modułów radiowych - czas pracy baterii jest krytycznym czynnikiem, szczególnie dla wodomierzy zainstalowanych w trudno dostępnych miejscach. Technologie takie jak np. NB-IoT i LTE CAT-M1 są projektowane pod kątem niskiego zużycia energii, celując w żywotność baterii na poziomie 10 lat lub więcej.
- 7) konserwacja - korzystanie z sieci komórkowej GSM do transmisji danych niweluje potrzebę konserwacji elementów sieci transmisyjnej;
- 8) standaryzacja - jako standardy 3GPP stosowane na rynku technologie są globalnie uznane i standaryzowane, co może ułatwiać interoperacyjność i dostępność urządzeń.

Zamawiający wskazał, że odwołujący w treści odwołania niejako przyznaje się do braku posiadania pożądanej infrastruktury umożliwiającej, nawet w pasmie otwartym realizację zamówienia. Jak czytamy, na str. 9 odwołania,

odwołujący posiada infrastrukturę ale na terenie miasta Wrocławia i przyległych gmin, opartą w głównej mierze na pasmie nielicencjonowanym (publicznym), działającą w modelu LoRaWAN. Okoliczność ta może oznaczać z jednej strony, że usługa oferowana będzie świadczona głównie pasmem nielicencjonowanym (brak posiadania rezerwacji częstotliwości dla zdalnego odczytu z Modułów radiowych IoT - oświadczenie odwołującego się na str. 7 in fine), a ponadto może zaistnieć konieczność stworzenia systemu odczytu w standardzie LoRaWAN. W ostatnim przypadku, stworzenie systemu wymaga analizy dyfrakcyjnej modelu propagacji fal radiowych z uwzględnieniem cyfrowego modelu ukształtowania terenu, na podstawie której planuje się rozmieszczenie anten (punktów dostępowych). Następnie opracowywany jest projekt oraz pozyskiwane są zgody na dostęp do obiektów wysokościowych (wraz z podpisaniem stosownych umów). Budowa sieci transmisji i instalacja anten zgodnie z projektem, jest jednak pierwszym etapem działań wymaganych podczas wdrożenia tego typu infrastruktury. Najbardziej żmudna i czasochłonna jest jej rozbudowa i rozwój w trakcie użytkowania. Sama konieczność rozbudowy sieci ujawnia się co do zasady dopiero w trakcie montażu urządzeń (modułów radiowych IoT) podłączonych do tej sieci, ponieważ dopiero wówczas dochodzi do sprawdzenia, czy po zamontowaniu modułu w konkretnej lokalizacji osiąga się zasięg zbudowanej sieci. Z uwagi na to, że moduły IoT będą montowane w trudnych warunkach i pod powierzchnią terenu, skuteczna symulacja warunków w modelu propagacji fal radiowych jest znacznie utrudniona - co z kolei wpływa na plan rozmieszczenia anten.

Ad zarzut 2 i 4, 5).

2) Wymóg posiadania co najmniej 90% własnej infrastruktury nie został uzasadniony realnymi potrzebami zamawiającego. Dla zapewnienia niezawodnej transmisji danych istotny jest poziom SLA, bezpieczeństwo transmisji, dostępność usług czy zgodność z wymaganiami prawnymi (np. RODO), a nie własność fizycznej infrastruktury. Dopuszczenie do przetargu podmiotów korzystających z infrastruktury dzierżawionej lub współdzielonej (np. MVNO, operatorzy hurtowi) mogłoby skutkować uzyskaniem oferty bardziej konkurencyjnej cenowo a jednocześnie spełniającej wszystkie techniczne i bezpieczeństwa wymagania; oraz

4) W co najmniej 90% wykorzystywać własną infrastrukturę" - nie określono, co dokładnie oznacza „własna infrastruktura" czy chodzi o fizyczne nadajniki, urządzenia końcowe, serwery, a może tylko o kanały transmisyjne? Brak kryteriów pomiaru (czy procent ma być liczony wg długości sieci, liczby lokalizacji, przepustowości?) powoduje niepewność co do sposobu oceny oferty;

Zamawiający ponownie wskazał, że nie stawia wymogu posiadania infrastruktury fizycznej w znaczeniu prawa własności, lecz wymaga, aby wykonawca miał pełną, niezależną kontrolę nad infrastrukturą transmisyjną wykorzystywaną w minimum 90% przypadków - w tym w szczególności:

- możliwość stałego monitorowania i zarządzania ruchem IP,
- gwarancję poziomu SLA (Service Level Agreement),
- niezależność operacyjną w zakresie dostępności, rekonfiguracji i rozliczalności danych,
- możliwość jednoznacznego zapewnienia integralności i bezpieczeństwa danych w warstwie sieciowej.

Wskazany w OPZ wymóg 90% transmisji przez infrastrukturę będącą pod bezpośrednią kontrolą wykonawcy:

- nie eliminuje żadnego typu podmiotu, który dysponuje techniczną i organizacyjną zdolnością do zapewnienia niezależnego kanału transmisji (operatorzy, integratorzy, MVNE), jest proporcjonalny - pozostałe 10% lokalizacji może być realizowane w modelu mniej kontrolowanym (np. nielicencjonowane pasmo), zapewnia realizację zamówienia zgodnie z wymogami prawa, bez ryzyka naruszenia ciągłości działania systemu przez czynniki zewnętrzne.

Zamawiający zakwestionował w pełni stanowisko odwołującego, jakoby sformułowanie warunków 90% własnej infrastruktury nie było uzasadnione realnymi potrzebami zamawiającego. Nie powielając przywołanej powyżej argumentacji o szczególnej roli zamawiającego, jako podmiotu publicznego posiadającego i zarządzającego infrastrukturą krytyczną podkreślił, że przed ogłoszeniem o zamówieniu przeprowadził testy pilotażowe w warunkach operacyjnych dla czterech niezależnych technologii transmisji danych:

- 1.LTE-M (Orange/SmartMetering24)
- 2.NB-10T (T-Mobile/Plum)
- 3.WIZE 169 MHz (AquaRD)
- 4.LoRaWAN 868 MHz (Aiut)

Testy realizowane były we współpracy z dostawcami urządzeń oraz operatorami sieci, w rzeczywistych lokalizacjach wodomierzy - szczególnie tam, gdzie dotychczasowe moduły wykazywały niską skuteczność (studnie, zabudowa zwarta, strefy podziemne). Celem pilotażu było obiektywne porównanie technologii pod kątem:

- niezawodności transmisji danych,
  - bezpieczeństwo transmisji,
- zasięgu i propagacji sygnału,
- kosztów operacyjnych i eksploatacyjnych,

Na podstawie przeprowadzonego pilotażu dokonano wyboru GSM (pasmo licencjonowane) jako rozwiązania

preferowanego, gdzie zastosowanie technologii np. LTE-M i NB-IoT przynosiło niższe wymienione zalety, jak:

- Brak potrzeby budowy sieci - wykorzystanie istniejącej infrastruktury telekomunikacyjnej;
- Bardzo dobra propagacja sygnału wewnątrz budynków, piwnic, studni wodomierzowych;
- Niska podatność na zakłócenia - transmisja w paśmie licencjonowanym pod nadzorem UKE;
- Komunikacja zgodna z europejskimi standardami szyfrowania danych;
- Zgodność z profilem rozwoju rynku i długofalowym wsparciem technologicznym (standardy 3GPP).

Z kolei technologie WIZE 169 MHz i LoRaWAN wykorzystywane w pasmach otwartych nielicencjonowanych, cechuje:

- Konieczność budowy własnej infrastruktury transmisyjnej (od 6 do 60 anten na obszar Katowic);
- Zasięg w pełni zależny od ilości i lokalizacji anten oraz wzmacniaczy sygnału;
- Znacznie większe ryzyko interferencji z innymi systemami szczególnie w LoRaWAN (brak gwarancji jakości transmisji);
- Brak regulacji pasma - technologia oparta na otwartych zakresach częstotliwości;
- Negatywny aspekt społeczny - potrzeba montażu dziesiątek anten emitujących pole elektromagnetyczne.

Rozwiązanie w technologii LoRaWAN 868 Mhz prezentowała firma Aiut uznany dostawca systemowych rozwiązań dla wody, gazu i ciepła, który ma na swoim koncie wdrożenia systemów zdalnego odczytu obsługujących kilka miast na terenie Polski. Firma Emitel proponuje tożsame rozwiązanie pod względem technologicznym. Pilotaż rozwiązania technologii LoRaWAN 868 Mhz przy uczestnictwie firmy Aiut pozwolił na poznanie działania rozwiązania opartego na otwartym paśmie LoRa w specyficznych warunkach urbanistycznych miasta Katowice.

Dowód: Notatka wewnętrzna z przeprowadzonego pilotażu

W rezultacie wybór technologii GSM (NB-IoT / LTE-M) jako dominującej w wymaganiach OPZ (min. 90%) był bezpośrednim rezultatem praktycznej oceny wdrożeniowej, przeprowadzonej z udziałem czterech niezależnych dostawców. Technologie oparte na paśmie licencjonowanym:

- zapewniły najlepszy bilans niezawodności, kosztów i bezpieczeństwa,
- wykazały znaczną przewagę nad rozwiązaniami wymagającymi budowy własnej infrastruktury (LoRaWAN, WIZE),
- są skalowalne i zgodne z wymogami cyberbezpieczeństwa, ciągłości działania i RODO,
- nie wymagają montażu dodatkowej (nowej) infrastruktury narażonej na akty wandalizmu, kradzież czy niechęć społeczności lokalnych.

Dlatego wymóg stosowania technologii GSM nie jest arbitralny ani dyskryminujący, lecz wynika wprost z doświadczenia eksploatacyjnego oraz oceny ryzyka związanego z funkcjonowaniem systemów infrastruktury krytycznej.

Ad Zarzut 3)

„Podsieć APN dedykowana zamawiającemu” - brak wyjaśnienia, czy chodzi o fizycznie odseparowaną sieć, logiczną separację (np. za pomocą VPN/MPLS), czy też konfigurację w ramach standardowego APN, Nie wiadomo, czy wystarczy np. prywatny APN z tunelem IPsec czy wymagana jest fizyczna izolacja;

Zamawiający wskazał, że zarzut, jakoby wymóg ustanowienia „podsięci APN dedykowanej zamawiającemu” był niejednoznaczny lub nieprecyzyjny, nie znajduje uzasadnienia, gdyż:

- 1.termin ten posiada ugruntowane znaczenie w praktyce operatorów komórkowych,
- 2.wymogi OPZ są zgodne z powszechnie oferowanymi i wdrażanymi rozwiązaniami klasy enterprise,
- 3.Zamawiający nie wymaga fizycznej separacji sieci transmisyjnej, lecz zapewnienia logicznie wydzielonego kanału transmisji, realizowanego z zachowaniem wymogów cyberbezpieczeństwa i prywatności danych.

W rozumieniu stosowanym w sektorze telekomunikacyjnym i potwierdzonym praktykami operatorów (np. Orange BizData VPN, T-Mobile BizNet VPN, Plus DMP) „dedykowana podsieć APN” oznacza:

- logicznie wydzielony kanał transmisji danych, z zapewnieniem separacji ruchu od sieci publicznej Internet umożliwiający transmisję tylko pomiędzy urządzeniami IoT a infrastrukturą Zamawiającego, zabezpieczony najczęściej poprzez tunel VPN (IPSec, GRE lub MPLS), zarządzany przez operatora na poziomie warstwy APN oraz adresacji prywatnej IP (niepublicznej).

W kontekście OPZ, wystarczające i zgodne z wymaganiami jest wdrożenie rozwiązania w modelu: Prywatny APN z tunelem VPN/IPSec zakończonym w infrastrukturze zamawiającego, z jednoznacznym ograniczeniem komunikacji tylko do wskazanych adresów IP (whitelisting), bez możliwości dostępu do publicznych usług sieciowych.

Zamawiający nie wymaga fizycznego odseparowania transmisji danych (np. w postaci własnych światłowodów, osobnej sieci szkieletowej czy fizycznych VLAN na poziomie operatora). Wymagane jest natomiast, aby ruch:

nie przechodził przez Internet (czyli nie korzystał z publicznej routowalności IP),

był kierowany przez dedykowany kanał z punktem zakończenia po stronie Zamawiającego (np. router brzegowy, UTM, firewall),

był logicznie odizolowany od ruchu innych klientów operatora, co standardowo realizowane jest przez:

APN prywatny (Private Access Point Name), o statyczne adresy IP lub prywatne pule, o dedykowane tunele IPSec/GRE/MPLS

W ocenie zamawiającego powyższe wymagania:

- nie stanowią bariery konkurencyjnej, gdyż są powszechnie dostępne u wszystkich operatorów GSM w Polsce,
- mogą być wdrożone zarówno przez operatorów infrastrukturalnych, jak i integratorów czy MVNO, o ile posiadają umowę z operatorem umożliwiającą realizację usług APN/VPN.

W rezultacie:

Zamawiający wymaga logicznie wydzielonej, dedykowanej podsieci APN, zabezpieczonej poprzez tunel VPN lub usługę MPLS/IPSec - nie wymaga fizycznego odseparowania transmisji.

Wymóg ten jest w pełni zgodny z wymogami cyberbezpieczeństwa oraz RODO i KSC, a także odpowiada realnym zagrożeniom związanym z transmisją danych pomiarowych.

Rozwiązanie to jest powszechnie dostępne na rynku i nie ogranicza konkurencji, lecz zabezpiecza interes publiczny oraz obowiązki ustawowe zamawiającego jako podmiotu kluczowego.

Zarzut 6), Wymogi są wewnętrznie sprzeczne, z jednej bowiem strony zamawiający wymaga by wydzielić dedykowaną zamawiającemu sieć APN charakterystyczną dla łączności mobilnej komórkowej (co powinno nastąpić w terminie 30 dni od podpisania umowy a z drugiej wszystkie urządzenia jakie dostarczają wykonawcy w 2025 roku nie muszą pracować w technologii mobilnej w 2025 roku, wykonawcy mogą dostarczyć nie więcej jak 1500 nakładek w 2025 roku a więc nie muszą dostarczać nakładek w technologii mobilnych.

Zarzut, że istnieje sprzeczność między wymaganiem uruchomienia dedykowanej podsieci APN w ciągu 30 dni od podpisania umowy a możliwością dostarczenia modułów radiowych w technologii innej niż mobilna w 2025 roku, jest niezasadny i wynika z niezrozumienia proporcji oraz intencji OPZ. Zgodnie z pkt V.I.I) b. OPZ system odczytowy musi zostać uruchomiony w ciągu 30 dni od podpisania Umowy, co obejmuje: - udostępnienie zamawiającemu dostępu do platformy odczytowej i aplikacji mobilnej, oraz zapewnienia transmisji danych z całego obszaru działania zamawiającego. Zatem w roku 2025 zamawiający przewidział odbiór nie więcej niż 1500 sztuk modułów radiowych, moduły te co do zasady mają pracować w technologii licencjonowanej (np. NBIoT, LTE-M) a jedynie w uzasadnionych technicznie przypadkach (brak zasięgu GSM) zamawiający dopuszcza zastosowanie transmisji w paśmie nielicencjonowanym (np. LoRa). Wobec tego:

- 1.Zamawiający nie przewiduje pełnej dowolności technologicznej dla 1500 urządzeń dostarczanych w 2025 r.,
- 2.Dopuszczenie innej technologii niż GSM ma charakter wyjątkowy i warunkowy,
- 3.Wymóg uruchomienia APN w ciągu 30 dni jest w pełni uzasadniony, ponieważ:

\*stanowi element gotowości operacyjnej wykonawcy do świadczenia transmisji w modelu docelowym, o umożliwi uruchomienie i testy modułów w technologii GSM nawet w ograniczonym zakresie, o jest niezbędny do rozpoczęcia integracji z systemem IT zamawiającego, przeprowadzenia prób komunikacyjnych i odbiorów technicznych.

Zamawiający jako podmiot kluczowy w rozumieniu NIS2 i UKSC nie może dopuścić do sytuacji, w której:

\*system masowego odczytu opierałby się głównie na technologii podatnej na interferencje, niepodlegającej regulacji;

\*infrastruktura transmisyjna musiałaby być budowana od zera (LoRa) - co generuje ryzyka techniczne, eksploatacyjne i społeczne.

Dlatego też zastosowanie technologii nielicencjonowanej może dotyczyć wyłącznie punktów pomiarowych położonych poza zasięgiem licencjonowanej sieci GSM i to pod warunkiem zgody Zamawiającego na takie odstępstwo, zgodnie z zapisami OPZ.

W rezultacie:

Wymóg uruchomienia dedykowanego APN w terminie 30 dni dotyczy gotowości środowiska technicznego, a nie liczby aktywnych urządzeń w 2025 r.

Moduły dostarczane w pierwszym roku mają być domyślnie oparte o transmisję GSM, a zastosowanie innej technologii ma charakter uzasadnionego wyjątku.

Konstrukcja OPZ jest w pełni spójna, logiczna i wpisuje się w harmonogram stopniowego, bezpiecznego wdrożenia systemu, z zachowaniem wymogów cyberbezpieczeństwa.

Naruszenia art. 112 ust. 1 ustawy przez ukryte i nieproporcjonalne warunki udziału w postępowaniu, gdyż zamawiający wymaga, aby system wykorzystywał „w co najmniej 90% własną infrastrukturę telekomunikacyjną wykonawcy” (pkt V.I OPZ). W rzeczywistości jest to ukryty warunek udziału w postępowaniu, który nie został wyraźnie określony w SWZ. Zamawiający nie wykazał, że takie ograniczenie jest uzasadnione przedmiotem zamówienia. Istotą zamówienia jest zapewnienia ciągłości i bezpieczeństwa transmisji danych oraz spełnienie parametrów SLA, a nie własności fizycznej infrastruktury. Kryteria związane z własnością sieci nie są adekwatne do celu zamówienia i prowadzą do nieuzasadnionego ograniczenia konkurencji, eliminując wykonawców, którzy mogą zapewnić pełną funkcjonalność i niezawodność systemu przy użyciu infrastruktury współdzielonej lub dzierżawionej.

Zamawiający zakwestionował w pełni podniesiony zarzut. Wymóg posiadania co najmniej 90% własnej infrastruktury telekomunikacyjnej nie dotyczy, jak już wskazano wyżej w tym piśmie, wykazania po stronie wykonawcy tytułu prawnego

w postaci prawa własności do infrastruktury telekomunikacyjnej. W OPZ pojęcie „własna infrastruktura” należy rozumieć jako infrastrukturę, do której wykonawca posiada wyłączone prawo dysponowania na poziomie operacyjnym i konfiguracyjnym, a nie jako konieczność bycia właścicielem masztów lub światłowodów. Oznacza to, że: wykonawca może korzystać z infrastruktury dzierżawionej lub leasingowanej, o ile ma pełną kontrolę nad usługą transmisji danych (np. APN, VPN, routing, adresacja),

celem wymogu jest ograniczenie ryzyka związanego z usługą przekazywaną „w podwykonawstwo kaskadowe” lub przez model dzielonej odpowiedzialności (np. MVNO bez bezpośredniej umowy SLA z operatorem sieci dostępowej).

Z kolei, w odniesieniu do progu 90% to jego ustanowienie dotyczy pasm licencjonowanych, a wynika z:

czynności rozeznania rynku, o którym mowa powyżej;

Technologie NB-IoT i LTE-M działające w pasmach licencjonowanych wykazały wyższą skuteczność w trudnych warunkach (piwnice, studnie wodomierzowe);

Technologie LoRa/WIZE wymagałyby instalacji od kilkunastu do kilkudziesięciu anten tylko dla jednego obszaru miejskiego, co jest nieefektywne i ryzykowne;

Szczególne wymogi prawne i bezpieczeństwa, jakie musi spełniać zamawiający, jako podmiot publiczny, posiadający i zarządzający infrastrukturą krytyczną, oraz jako podmiot kluczowy, którego zadaniem jest stosować środki gwarantujące ciągłość działania i cyberbezpieczeństwo (art. 21 ust. 2 NIS2, art. 8 UKSC);

Transmisja danych systemów infrastruktury krytycznej nie może opierać się głównie na medium otwartym i niezarządzanym, bez gwarancji jakości i ochrony transmisji. Ograniczenie powierzchni ataku i łatwiejsze zarządzanie ryzykiem;

Wymóg 90% GSM pozwala ograniczyć:

ryzyko awarii infrastruktury własnej (LoRa), o ryzyko interferencji i braku transmisji w godzinach szczytu, o kosztowność monitoringu i utrzymania wielu równoległych sieci, o zagrożenia związane z atakami typu jamming, spoofing, replay w sieciach otwartych.

Zachowanie proporcjonalności i otwartości na wyjątki

Zamawiający nie wyklucza całkowicie technologii nielicencjonowanej, lecz:

dopuszcza ją do 10% lokalizacji - tam, gdzie udokumentowane będzie brak zasięgu

GSM lub szczególne warunki fizyczne, o daję tym samym przestrzeń do elastyczności i innowacyjnych rozwiązań.

W rezultacie ustanowienie wymogu minimum 90% urządzeń korzystających z transmisji w paśmie licencjonowanym (GSM) jest:

- proporcjonalny względem potrzeb bezpieczeństwa i niezawodności,
- technicznie uzasadniony wynikami pilotaży,
- zgodny z obowiązkami Zamawiającego jako operatora infrastruktury krytycznej (NIS2,

UKSC),

- nie eliminuje technologii otwartych, ale ogranicza ich udział do przypadków uzasadnionych technicznie, co jest typowe dla systemów klasy infrastrukturalnej.

Zamawiający na zakończenie wskazał, że to postępowanie jest kolejnym, gdzie dwuliczący w odniesieniu do warunków zamówienia posługuje się podobnymi argumentami zarówno faktycznymi, jak prawnymi, a które w ostatecznym rezultacie skutkowały oddaleniem wniesionych odwołań. I tak, w postępowaniu przed Krajową Izbą Odwoławczą, w sprawę o sygn. KIO 2516/23, wszczętej na skutek odwołania EMITEL S.A., Izba rozstrzygnęła podobny spór co do zasadności oparcia się na technologii działającej w paśmie licencjonowanym. Sprawa dotyczyła postępowania o udzielenie zamówienia publicznego na sukcesywne dostawy modułów NB (NB-IoTJ (800 MHz) do przekazu danych z wodomierzy wraz z usługą transmisji danych oraz aplikacją zarządzającą i wdrożeniem (znak postępowania: 649/PN - 57/2023) prowadzonego przez Wodociągi Miasta Krakowa S.A. z siedzibą w Krakowie. W wyroku KIO uznała, że odwołujący nie przedstawił w odwołaniu żadnych argumentów pozwalających Izbie przesądzić, że proponowana przez wykonawcę technologia LoRaWAN jest technologią równoważną do wybranej przez Wodociągi Miasta Krakowa oraz umożliwiającą zamawiającemu należyte świadczenie usług z uwzględnieniem jego potrzeb i specyfiki. Podobnie w wyroku KIO w sprawie o sygn. KIO 32/25, również prowadzonej na skutek odwołania EMITEL S.A. W tym miejscu zamawiający przytoczył fragment uzasadnienia.

Dowód: Wyrok KIO z dnia 22.09.2023 r. sygn. KIO 2516/23; Wyrok KIO z dnia 5.02.2024r. sygn. KIO 32/24

29 sierpnia 2025 r. uczestnik Orange spółka akcyjna złożył pisemne stanowisko podtrzymując wniosek o oddalenie odwołania w całości i poparł stanowisko przedstawione przez zamawiającego w odpowiedzi na odwołanie z dn. 29 sierpnia 2025 r.

Przystępujący wskazał, że zamawiający ma prawo, tak określić przedmiot zamówienia, aby opisać go adekwatnie do wyznaczonego celu, zachowując jednocześnie obiektywizm i precyzję w formułowaniu jego potrzeb. Z orzecznictwa Krajowej Izby Odwoławczej wynika, że nie narusza przepisów ustawy takie sporządzenie opisu przedmiotu zamówienia,

który uwzględnia potrzeby zamawiającego, nawet jeżeli utrudnia lub uniemożliwia niektórym podmiotom dostęp do zamówienia. Zamawiający nie ma bowiem obowiązku zapewnienia możliwości realizacji przedmiotu zamówienia wszystkim podmiotom działającym na rynku w danej branży, bowiem pojęcie uczciwej konkurencji nie może być utożsamiane z konkurencją absolutną. Jednakże w przypadku opisu przedmiotu zamówienia w sposób uprzywilejowujący lub eliminujący niektórych wykonawców lub produkty, po stronie zamawiającego istnieje obowiązek przedstawienia rzeczowych argumentów uzasadniających taki opis.

W związku z powyższym odwołanie zasługiwałoby na uwzględnienie w odniesieniu do zarzutów dotyczących opisu przedmiotu zamówienia, jeśli opis ten byłby nieproporcjonalny i nie miał uzasadnienia w obiektywnych potrzebach zamawiającego.

Okoliczności przedmiotowego postępowania wskazują na to, że wybór technologii, w której ma być realizowany przedmiot zamówienia nie jest przypadkowy, jest proporcjonalny i znajduje uzasadnienie w potrzebach zamawiającego. Został poprzedzony przeprowadzeniem przez zamawiającego pilotażu. Przystępujący uznał, że opis przedmiotu zamówienia nie tylko odpowiada potrzebom zamawiającego wynikającym z uwarunkowań, w jakich funkcjonuje zamawiający (lokalizacje, topografia), szczególnych zadań jako przedsiębiorstwa wodociągowo-kanalizacyjnego, które posiada i zarządza infrastrukturą krytyczną, lecz także zadań związanych z zabezpieczaniem tej infrastruktury, a także statusu zamawiającego jako podmiotu kluczowego w rozumieniu dyrektywy NIS2, co wiąże się z koniecznością wyboru rozwiązań adekwatnych do poziomu ryzyka w zakresie cyberbezpieczeństwa.

Zamawiający podjął działania, aby zweryfikować i przetestować różne technologie w praktyce w drodze pilotażu.

Przystępujący zwrócił uwagę, że zamawiający zaoferował dowody potwierdzające, że wymagania dotyczące technologii transmisji danych w pasmach licencjonowanych LTE-M i NB-IoT, a także inne wymagania dotyczące infrastruktury (90% własnej infrastruktury) są uzasadnione, a nawet, że dokonał praktycznej weryfikacji dostępnych technologii w toku pilotażu.

Odwołujący nie przedstawił, żadnych dowodów na to, że sformułowane przez zamawiającego wymagania są nieproporcjonalne do przedmiotu zamówienia lub nie mają uzasadnienia w obiektywnych potrzebach zamawiającego. Z treści odwołania wynika jedynie, że jest możliwe rozwiązanie oparte na technologii LoRaWAN i że jest stosowane we Wrocławiu. To jednak nie oznacza, że wymaganie transmisji danych w pasmach licencjonowanych LTE-M i NB-IoT w postępowaniu nie jest uzasadnione potrzebami zamawiającego i nieproporcjonalne. To, że odwołujący posiada infrastrukturę LoRaWAN we Wrocławiu, nawet, jeśli liczba wodomierzy jest większa, nie powoduje również, że posiada taką infrastrukturę w Katowicach, a tym samym jest to okoliczność bez znaczenia dla oceny zasadności wymagań Zamawiającego.

Przystępujący poparł stanowisko zamawiającego, odnośnie „pasma licencjonowanego” wyrażone w odpowiedzi na odwołanie. Zdaniem przystępującego sam zarzut odwołania świadczy o tym, że pojęcie to jest dla odwołującego jednoznaczne, skoro buduje wokół pojęcia licencjonowanego pasma argumentację dotyczącą ograniczenia technologii LoRaWAN i potrafi w sposób jednoznaczny zidentyfikować tę technologię jako „nelicencjonowaną”.

W ocenie przystępującego zarzuty odwołania zmierzają do tego, aby zamawiający przystał na realizację zamówienia w technologii LoRaWAN, niezależnie od tego, jakie są potrzeby zamawiającego.

Przystępujący wskazał również na wcześniejsze rozstrzygnięcia Krajowej Izby Odwoławczej w sprawach o sygnaturach KIO 2516/23 i KIO 32/24, które zapadły w analogicznych stanach faktycznych, również dotyczących odczytu wodomierzy i również prób wymuszenia na zamawiającym, aby dopuścił stosowanie technologii LoRaWAN i w których Izba konsekwentnie stała na stanowisku, że wymaganie transmisji danych w pasmach licencjonowanych LTE-M i NB-IoT przez zamawiającego było uzasadnione. W szczególności w wyroku KIO 32/24 Izba stanęła na stanowisku, że „Odwołujący, zdaniem Izby nie wykazał, aby sposób ukształtowania przez zamawiającego opisu przedmiotu zamówienia był nieuzasadniony obiektywnymi potrzebami zamawiającego co z kolei miałyby wpływać na utrudnianie konkurencji. Sam fakt, że wprowadzenie żądanych przez odwołującego zmian w SWZ, umożliwiłoby wykonawcy złożenie oferty w tym postępowaniu, nie jest wystarczający do stwierdzenia, że zamawiający naruszył przepisy ustawy, oraz, że przedmiot zamówienia został opisany w sposób, który mógłby utrudniać - w sposób naruszający przepisy ustawy - uczciwą konkurencję. Zamawiający w tym przetargu nie zamawia sieci telekomunikacyjnej lub infrastruktury telekomunikacyjnej, ale usługę transmisji danych. Z ustaleń w tej sprawie wynika, że kompleksowo i wszechstronnie rozeznał swoje potrzeby, co znalazło odzwierciedlenie w SWZ.”. Analogicznie jak w przedmiotowej sprawie odwołujący nie wykazał ukształtowania opisu przedmiotu zamówienia w sposób nieuzasadniony obiektywnymi potrzebami, a zamawiający, jak w przywołanej sprawie, wybór technologii poprzedził rozeznaniem (w postaci pilotażu).

Wobec powyższego w ocenie przystępującego, należy uznać, że nie zostało wykazane, że wymagania dotyczące transmisji danych nie znajdują oparcia w obiektywnych potrzebach zamawiającego i nie są proporcjonalne do celu postępowania. Przeciwnie, zamawiający przedstawił dowody na to, że wymagania są uzasadnione i proporcjonalne. W konsekwencji nie można mówić o tym, że opis przedmiotu zamówienia narusza przepisy ustawy.

Odnosząc się do zarzutu nr 3, dotyczącego warunku udziału w postępowaniu, to przystępujący wniósł o jego oddalenie, jako bezpodstawnego, co wynika z treści samego zarzutu („W rzeczywistości jest to ukryty warunek udziału w postępowaniu...”), z którego wynika, że warunku tego odwołujący upatruje w treści OPZ, jednak tego warunku nie sformułował zamawiający, a skoro tak, to nie mógł, przynajmniej, co do wymyślonego przez odwołującego warunku, naruszyć przepisów ustawy, w szczególności art. 112 ust. 1 ustawy.

Przystępujący poparł wnioski dowodowe przedstawione przez zamawiającego wniósł o dopuszczenie i przeprowadzenie dowodów w nich zawartych.

Przystępujący wniósł o niedopuszczenie dowodów zgłoszonych przez odwołującego. Po pierwsze, przystępujący zwrócił uwagę, że odwołujący nie sformułował też dowodowych i nie wskazał, jakie fakty mają zostać udowodnione. Po wtóre, wskazane środki dowodowe, nie mogą być dowodami w świetle art. 531 ustawy, gdyż przedmiotem dowodu są jedynie fakty mające znaczenie dla rozstrzygnięcia sprawy istotne znaczenia, a przedstawione środki dowodowe nie mogą mieć takiego znaczenia:

a) Opracowanie eksperckie – stanowi opis dostępnych technologii odczytu wodomierzy, co nie ma znaczenia dla rozstrzygnięcia, a w dodatku jest okolicznością bezsporną, że są różne technologie odczytu wodomierzy, przy czym właściwości technologii nie mają znaczenia dla rozstrzygnięcia, ale to, czy dana technologia jest uzasadniona wedle potrzeb zamawiającego,

b) Informacja o funkcjonowaniu systemu odczytu wodomierzy we Wrocławiu nie ma znaczenia dla tego, czy wybór technologii przez zamawiającego jest uzasadniony jego potrzebami – z samego opisu dokumentu (dokument utajniony) wynika, że odnosi się do innego miasta, a w konsekwencji nie jest adekwatny do opisu przedmiotu zamówienia w postępowaniu,

c) Wniosek o przeprowadzenie kontroli, złożony przez odwołującego w zakresie realizacji innego zamówienia nie ma znaczenia dla tego, czy wybór technologii transmisji danych jest uzasadniony potrzebami zamawiającego, sposób realizacji zamówienia nie ma też znaczenia dla tego, czy określone przez zamawiającego wymagania są uzasadnione – jeśli odwołujący uznał wyrok KIO 32/24 za błędny mógł wnieść skargę do Sądu Zamówień Publicznych,

d) Artykuły prasowe mogą stanowić, co najwyżej dowód tego, jakie informacje i opinie przedstawili w nich autorzy tych artykułów, nie mają znaczenia dla oceny tego, czy wymagania dotyczące infrastruktury mają uzasadnienie w potrzebach zamawiającego.

29 sierpnia 2025 r. uczestnik T-Mobile spółka akcyjna złożył stanowisko pisemne wskazując, wnoszący o:

1) oddalenie odwołania w całości,

2) przeprowadzenie dowodu z opracowania „Sieci rozległe o niskim poborze mocy: Porównanie wydajności LoRaWAN i NB-IoT”, 3) pominięcie dowodu z:

a) opracowania eksperckiego sporządzonego przez mgr inż. P.Z. jako stanowiącego dokument prywatny sporządzony na zlecenie odwołującego, a w konsekwencji niedowodzący okoliczności, na które został powołany, a jedynie wykazujący, że osoba, która go podpisała, złożyła oświadczenie zawarte w dokumencie,

b) zastrzeżonych jako tajemnica przedsiębiorstwa dokumentów odnoszących się do zamówienia realizowanego przez innego zamawiającego (MPWiK Wrocław), a także kopii wniosku o przeprowadzenie kontroli wraz załącznikami jako nieprzydatnych dla rozstrzygnięcia z uwagi na to, że nie dotyczą one postępowania, zamawiającego, ani aglomeracji katowickiej i jej specyfiki,

c) artykuł ze stron internetowych Wirtualne Media i Business Insider jako nieodnoszących się do zarzutów odwołania i nieprzydatnych dla rozstrzygnięcia.

Wbrew zarzutom odwołania, zamawiający nie sformułował opisu przedmiotu zamówienia w sposób naruszający przepisy prawa, a w konsekwencji brak jest również podstaw do zmiany brzmienia OPZ w oczekiwany przez odwołującego sposób.

Ad. ZARZUT NARUSZENIA ART. 99 ust. 1, 2 oraz 4 ustawy i art. 16 ust. 1 oraz ust. 3 ustawy

Zgodnie z ust. 1 pkt. 1.1. OPZ zamawiający wymagał, aby wdrożony system odczytowy korzystał z komunikacji radiowej w licencjonowanych pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych. Postanowienie w takim brzmieniu stanowi opis jednoznaczny i wyczerpujący, nie pozostawiając wątpliwości w zakresie stawianych wykonawcom wymagań i sposobu ich spełnienia i tym samym pozostaje ono w zgodzie z art. 99 ust. 1 ustawy.

Wymóg stosowania pasma licencjonowanego w 90% lokalizacji nie stanowi przy tym wymogu nieproporcjonalnego. Samo istnienie możliwości zbudowania systemu odczytowego wyłącznie na pasmach częstotliwości otwartych nie oznacza, że dopuszczenie takiej możliwości na gruncie przedmiotowego postępowania pozwałoby na zaspokojenie potrzeb zamawiającego i zrealizowanie celu zamówienia. Wbrew twierdzeniom odwołującego, pasma licencjonowane i nielicencjonowane wykazują rozbieżności, które przy innym ukształtowaniu wymagań zamówienia wpływałyby na efektywność i bezpieczeństwo jego realizacji.

Wyjaśnienia w tym kontekście wymaga, że w rozwiązaniach technologii bezprzewodowej, które sprawdzają się w systemach inteligentnego opomiarowania istnieją rozwiązania o niskim poborze mocy i rozległym obszarze - LPWAN. Do najpopularniejszych standardów LPWAN dedykowanych potrzebom Internetu rzeczy (IoT, z ang. Internet of Things) zalicza się:

a) działające w pasmach ogólnodostępnych, nielicencjonowanych:

- LoRaWAN lub LoRa - pasma 868MHz, przepływność: 0,3 kb/s - 50 kb/s,
- Sigfox - pasma 868MHz, przepływność: 100 kb/s - 600 kb/s,

b) działające w chronionych, licencjonowanych pasmach radiowych:

- NB-IoT - działające w pasmach LTE-M (kilkanaście pasm od 450 MHz po 2100 MHz), przepływność: 32,4 kb/s - 66,7 kb/s,
- Cat-M działające w pasmach LTE-M (kilkanaście pasm od 450 MHz po 2100 MHz), przepływność: 200 kb/s - 1 Mb/s.

Technologia NB-IoT wykazuje najlepsze wyniki pod względem efektywności przekazu danych ze studzienek wodomierzowych oraz innych miejsc zainstalowania położonych poniżej poziomu gruntu. Jest to istotne w kontekście tego postępowania, ponieważ przedsiębiorstwo wodociągowe cechuje się jednym z najtrudniejszych miejsc instalacji modułów telemetrycznych. Technologie oparte na pasmach nielicencjonowanych wykazują się natomiast niższą jakością transferu danych i spadkami zasięgu. Różnice pomiędzy obiema technologiami zostały szerzej przedstawione w załączonym jako dowód opracowaniu „Sieci rozległe o niskim poborze mocy: Porównanie wydajności LoRaWAN i NB-IoT”, które jest dostępne także pod adresem: <https://ieeexplore.ieee.org/document/9778216>. W opracowaniu tym wskazano m.in. na następujące aspekty różnicującą technologię opartą na pasie licencjonowanym od tej opartej na pasie nielicencjonowanym:

-NB-IoT zapewnia łączność w górę i w dół z mniej niż 5% wskaźnikiem awaryjności, podczas gdy LoRaWAN ma trudności z zapewnieniem wystarczającego zasięgu w pomieszczeniach,

-NB-IoT oferuje więcej korzyści pod względem niezawodności i odporności na zakłócenia i opóźnienia,

-NB-IoT zapewnia lepszą skalowalność w porównaniu z LoRaWAN, a zatem jest w stanie obsługiwać ogromną liczbę urządzeń przy niskim wskaźniku błędów pakietów,

-NB-IoT wykorzystuje bardziej niezawodny schemat modulacji i kodowania wraz z wysoce niezawodną warstwą łącza, kosztem większego zużycia energii. Dlatego NB-IoT jest bardziej odpowiedni dla zastosowań wymagających niezawodności i przepustowości sieci. Ponadto nie jest on ograniczony żadnymi regulacjami w zakresie prądu stałego, dzięki czemu urządzenia mogą przysyłać dane częściej lub w większych ilościach.

-NB-IoT oferuje zaawansowane protokoły bezpieczeństwa w porównaniu

z LoRaWAN, które są szczególnie niebezpieczne w przypadku korzystania z procedury aktywacji poprzez personalizację.

Powyższe przeczy twierdzeniu Odwołującego, że wymóg pasma licencjonowanego dla 90% lokalizacji nie znajduje obiektywnego uzasadnienia technicznego ani funkcjonalnego, a stwierdzenie o „wymuszaniu” przez zamawiającego „licencji na pasmo” ocenić należy jako nieuprawnione. Bezspornie technologie oparte na pasmach licencjonowanych wykazują odrębne cechy od tych opartych na pasmach nielicencjonowanych i posiadają właściwości kluczowe z perspektywy celu postępowania i potrzeb zamawiającego, w tym w aspekcie bezpieczeństwa, który został zmarginalizowany w odwołaniu. Stanowiska tego nie podważa określenie tożsamyh wymagań SLA dla pasm licencjonowanych i nielicencjonowanych. Oczywistym jest bowiem oczekiwanie, aby wykonawca zapewniał spójny poziom usług. Pewność spełnienia tych oczekiwań, biorąc pod uwagę analizowane powyżej cechy obu rodzajów pasm, przedstawia się jednak odmiennie w odniesieniu do pasma licencjonowanego i pasma nielicencjonowanego. Stąd zrozumiałym jest zróżnicowanie przez zamawiającego poziomu wykorzystania pasm licencjonowanych i nielicencjonowanych oraz ograniczenie korzystania z pasm nielicencjonowanych do uzasadnionych przypadków.

Dopuszczenie wykorzystania pasm nielicencjonowanych na poziomie 10% z jednej strony znacząco ogranicza ryzyko zamawiającego związane z tym rozwiązaniem, a przy tym stanowi rozwiązanie zabezpieczające na wypadek zaistnienia nadzwyczajnej sytuacji powodującej brak możliwości wykorzystania pasma licencjonowanego. Założeniem jest jednak korzystanie z pasm licencjonowanych. Zasadność i racjonalność takie rozwiązania wspiera fakt, że zamawiający jest podmiotem zarządzającym infrastrukturą krytyczną tj. systemami zaopatrzenia w wodę i odprowadzania ścieków, co wymusza zapewnienie pewnego i bezpiecznego rozwiązania.

Odnosząc się do samych pojęć „pasma licencjonowane” i „pasma nielicencjonowane” przystępujący wyjaśnił, że termin „nielicencjonowane w technologii radiowej” obejmuje powszechnie używane pasma, które mogą być używane w wielu krajach bez konieczności posiadania licencji częstotliwości. Częstotliwości nielicencjonowane mają tę zaletę, że nie wymagają koncesji (zazwyczaj licencje są objęte roczną opłatą i są wydawane przez krajowy organ regulacyjny lub państwowego operatora telekomunikacyjnego). Jednak nielicencjonowane łącza mogą być zakłócone przez innych użytkowników, co może spowodować zmniejszenie przepustowości lub całkowite wyłączenie łącza. Istotnym jest przy

tym, że takie zakłócenia są, co do zasady, silniejsze na obszarach i miastach o dużej gęstości zaludnienia, gdzie setki czy tysiące radiotelefonów może konkurować o to samo widmo w danym regionie, a w takim właśnie obszarze działa zamawiający. Z kolei licencjonowana eksploatacja oznacza, że użytkownik sprzętu musi uzyskać rezerwację częstotliwości przed użyciem pasma. Może to być dostępne na zasadzie per-link, w którym to przypadku regulator przydziela określone częstotliwości dla konkretnego łącza, posiadając centralną bazę danych wszystkich łączy lub w przypadku sieci operatorów komórkowych, licencję ogólnokrajową, w ramach której operator samokoordynuje przydział częstotliwości i zasięg. Brak przewidywalności w nielicencjonowanych pasmach jest głównym powodem, dla którego operatorzy preferują licencjonowane pasma do działania. Równie istotne są także aspekty dotyczące bezpieczeństwa informacji i stabilności transmisji.

Nie sposób przy tym uznać, że sformułowanie „pasma licencjonowane” i „pasma nielicencjonowane” są niedostatecznie dokładne czy niezrozumiałe w sytuacji, gdy sam odwołujący w treści odwołania używa ich w sposób świadomy i zgodny z powszechnym ich rozumieniem, wskazując m.in. na kwestię rezerwacji częstotliwości oraz częstotliwości otwarte. Nie powinno tym samym budzić wątpliwości, że określenie to jest jednoznaczne, w pełni zrozumiałe i jako takie nie wymaga definicji ustawowej czy doprecyzowania w dokumentach zamówienia. Odwołujący w sposób dorozumiany przyznał zatem, że zdefiniowanie danego pojęcia w ustawie pozostaje irrelewantne z perspektywy prawidłowego opisu przedmiotu zamówienia i tego rodzaju argumentacja nie pozwala na uznanie postawionego zarzutu za uzasadniony.

Postawionego zarzutu nie uzasadnia także odwołanie się do projektu wdrożonego na zlecenie innego zamawiającego. Zastosowanie technologii LoRaWAN przez innego zamawiającego nie dowodzi, że potrzeby zamawiającego w tym postępowaniu również uzasadniałyby takie rozwiązanie. Każdego zamawiającego cechują inne potrzeby i uwarunkowania. Decyzje zakupowe jednego podmiotu, nie są wiążące dla innego podmiotu. Wobec tego dowód taki jest nieprzydatny dla rozstrzygnięcia.

Ad. zarzut naruszenia art. 99 ust. 1, 2 oraz 4 ustawy i art. 16 ust. 1 oraz ust. 3 ustawy w zw. z art. 353(1) w zw. z art. 58 § 1 i 2 Kodeksu cywilnego

Zakwestionowania wymaga, aby uwzględnienie w opisie przedmiotu zamówienia wymogu oparcia systemu na technologii transmisji danych w wydzielonej podsieci APN dedykowanej zamawiającemu i w co najmniej 90% wykorzystującej własną infrastrukturę telekomunikacyjną Wykonawcy prowadziło do uprzywilejowania konkretnych wykonawców, czy też pozwalało na stwierdzenie, że opis przedmiotu zamówienia jest niejednoznaczny, niewyczerpujący lub nieproporcjonalny. Opis przedmiotu zamówienia został tak sformułowany, aby odzwierciedlał potrzeby zamawiającego i umożliwiał ich spełnienie z odwołaniem się do pojęć powszechnie stosowanych na rynku przez operatorów. Natomiast analiza treści wniesionego odwołania prowadzi do wniosku, że intencją odwołującego jest ukształtowanie wymagań zamówienia w oderwaniu od tych potrzeb, tak aby dostosowano je do produktu dystrybuowanego przez odwołującego. Oczekiwanie takie nie znajduje umocowania w przepisach, w tym w objętych zarzutami art. 99 ust. 1, 2 i 4 PZP i art. 16 ust. 1 i 3 ustawy. Zgodnie z ugruntowanym stanowiskiem Krajowej Izby Odwoławczej, wyrażonym m.in. w wyroku z dnia 28 marca 2023 r., sygn. akt: KIO 703/23 i w wyroku z dnia 22 września 2023 r. KIO 2516/24, zamawiający ma prawo określić warunki udziału w postępowaniu odnoszące się do przedmiotu zamówienia w sposób, który uwzględni obiektywne potrzeby zamawiającego, pomimo, że wyklucza on możliwość dopuszczenia do realizacji zamówienia wszystkich wykonawców działających na rynku.

Prawem zamawiającego jest takie opisanie warunków udziału w postępowaniu, które zaspokoi potrzeby i oczekiwania zamawiającego w ramach realizacji danego przedmiotu zamówienia.

Zaprzeczenia wymaga, by system oparty wyłącznie na pasmach nielicencjonowanych wykazywał się tożsamą funkcjonalnością i niezawodnością jak system oparty na pasmach licencjonowanych.

Odwołujący nie wykazał, aby możliwa do zaoferowana przez niego technologia była równoważna do tej wymaganej przez zamawiającego. Odwołujący ograniczył się do hasłowego przytoczenia cech i funkcjonalności, bez przedstawienia szerszej analizy i dowodów, które uzasadniałyby stwierdzenie o równoważności rozwiązań. Tożsamości rozwiązań przeczy przy tym załączone do niniejszego pisma i omówione powyżej opracowanie „Sieci rozległe o niskim poborze mocy: Porównanie wydajności LoRaWAN i NB-IoT”. Oczywistym jest przy tym, że każde z rozwiązań cechują określone wady i zalety, racjonalnym jest jednak założenie, że zamawiający w sposób świadomy wybrał oczekiwany sposób realizacji zamówienia jako najlepiej przystający do jego potrzeb. Twierdzenie to jest tym bardziej uzasadnione w świetle faktu, że wybór systemu odczytowego był poprzedzony pilotażem przeprowadzonym przez zamawiającego.

Analiza wniesionego odwołania skłania do wniosku, że odwołujący utożsamiana uczciwą konkurencję z konkurencją absolutną. Nie jest przy tym prawdą, że możliwość udziału w postępowaniu, wobec wymagań sformułowanych przez zamawiającego, ograniczona jest do 1-2 konkretnych podmiotów. Nie jest także prawdą, że wyłącznie Orange Polska S.A. posiada własną infrastrukturę telekomunikacyjną mobilną na obszarze aglomeracji Katowickiej. W rzeczywistości własną infrastrukturę telekomunikacyjną w aglomeracji Katowickiej posiadają również inni operatorzy telekomunikacyjni. Szerszy niż określony w odwołaniu krąg Wykonawców zdolnych do realizacji zamówienia potwierdza chociażby

przystąpienie innych podmiotów do postępowania odwoławczego po stronie zamawiającego. W konsekwencji stwierdził, że przyjęta przez zamawiającego technologia powoduje, że zamawiający nie będzie uzależniony od jednego operatora komórkowego.

Przystępujący zauważył, że sama redakcja uzasadnienia zarzutu wzajemnie się wyklucza. Z jednej bowiem strony odwołujący stoi na stanowisku, że opis przedmiotu zamówienia jest niejednoznaczny i niewyczerpujący, a z drugiej strony stoi na stanowisku, że wskazuje on na usługi dostarczane przez konkretnych wykonawców (co świadczyłoby o jego jednoznacznym brzmieniu).

Niewyjaśnionym ponadto pozostaje, w jaki sposób redakcja opisu przedmiotu zamówienia narusza art. 353(1) w zw. z art. 58 § 1 i 2 Kodeksu cywilnego, bowiem nie zostało to w żadnej mierze poruszone w odwołaniu. Późniejsze rozszerzenie podstawy faktycznej zarzutu będzie przy tym niedopuszczalne.

Przystępujący stwierdził, że nawet w przypadku, gdy odwołujący widział konieczność doprecyzowania brzmienia OPZ (niezależnie od oceny zasadności takiej konieczności), to miał on też możliwość zwrócenia się do zamawiającego o wyjaśnienie treści SWZ, a następnie złożenia oferty z uwzględnieniem tych wyjaśnień.

Ad. zarzut naruszenia art. 112 ust. 1 ustawy

Stanowisko przedstawione w odniesieniu od innych zarzutów odwołania zachowuje aktualność również w odniesieniu do zarzutu naruszenia art. 112 ust. 1 ustawy. Przystępujący zauważył, że uzasadnienie faktyczne tego zarzutu opiera się na nadinterpretacji wymogu posiadania w co najmniej 90% własnej infrastruktury telekomunikacyjnej. Zamawiający, w przeciwieństwie do odwołującego, nie posługuje się bowiem pojęciem „własności fizycznej infrastruktury”. Prowadzi to do sytuacji, w której odwołujący w praktyce nie kwestionuje brzmienia OPZ, ale przyjętą przez siebie interpretację OPZ. Działanie takie nie zasługuje na akceptację, podobnie jak dążenie do ukształtowania opisu przedmiotu zamówienia w sposób zapewniający możliwość złożenia oferty konkretnemu wykonawcy tj. odwołującemu z pominięciem potrzeb zamówienia, parametrów technicznych i specyfiki środowiska, w którym będzie ono realizowane.

Odnosząc się do oczekiwanych przez odwołującego zmian brzmienia OPZ przystępujący stanął na stanowisku, że wprowadzenie tych zmian doprowadziłoby do niejednoznaczności i utrudnienia uczciwej konkurencji z uwagi na zastąpienie precyzyjnie określonego sposobu wykonania zamówienia ogólnikowymi sformułowaniami. Odwołujący oczekuje bowiem m.in., aby jednoznaczne określenie stosowanej technologii zastąpić ogólnym określeniem mówiącym o technologii zapewniającej stabilność, bezpieczeństwo i ciągłość komunikacji. Dopuszczenie takiej zmiany brzmienia OPZ z jednej strony stawiałoby zamawiającego w stanie niepewności, co do tego jaka technologia zostanie wdrożona, a przy tym skutkowałoby nieporównywalnością ofert. Każdy wykonawca może bowiem w inny sposób rozumieć wyczerpanie wymagania zapewnienia stabilności, bezpieczeństwa i ciągłości komunikacji. W praktyce wprowadzałoby to pełną dowolność w zakresie sposobu realizacji zamówienia i pozbawienie zamawiającego jego podstawowego uprawnienia, jakim jest określenie opisu przedmiotu zamówienia, w tym standardów jakościowych i technicznych, zgodnie z jego potrzebami.

Na rozprawie odwołujący przedstawił dodatkowe pisemne stanowisko w sprawie:

I/ Brak uzasadnienia dla proporcji 90/10

W całym piśmie procesowym zamawiającego brak jest jakichkolwiek dowodów i wyliczeń, które uzasadniałyby konieczność ustalenia wymogu, aby 900/0 transmisji realizowanych było w oparciu o pasma licencjonowane (technologie komórkowe), a jedynie 10% w innych technologiach.

Zamawiający w istocie ograniczył się do ogólnego wskazania, że pasma licencjonowane zapewniają większą stabilność, bezpieczeństwo i przewidywalność transmisji niż pasma nielicencjonowane (takie jak LORa). Argumentacja ta, choć może wskazywać na preferencję dla technologii komórkowej, nie wykazuje jednak w żaden sposób, że akurat 900/0 transmisji musi być realizowane w oparciu o sieci komórkowe, aby spełnić wymagania przedmiotu zamówienia.

W szczególności:

a/ Brak powiązania wymogu 90/10 z poziomami SLA — zamawiający sam przyznał, że zarówno transmisja w paśmie licencjonowanym, jak i nielicencjonowanym może zapewnić wymagane parametry SLA (m.in. odczyt z co najmniej 900/0 urządzeń raz dziennie, z 95% raz w tygodniu, i z 980/0 raz w miesiącu). Skoro zatem poziom SLA może być zachowany niezależnie od technologii transmisji, to nie sposób przyjąć, że ustanowienie proporcji 90/10 znajduje obiektywne uzasadnienie.

b/ Brak danych z pilotażu

Zamawiający powołał się na przeprowadzony pilotaż, jednak nie przedstawił żadnych wyników ilościowych, które dowodziłyby, że w realnych warunkach Katowic konieczne było wykorzystanie akurat 90% technologii komórkowej.. Gdyby nawet uznać, że pilotaż wykazał ograniczenia pasm nielicencjonowanych w pewnych lokalizacjach, to nie przesądza to o konieczności utrzymania aż 90% transmisji w technologii komórkowej — równie dobrze proporcja 600/0 czy 700/0 mogłaby zapewniać identyczny efekt funkcjonalny. Jednocześnie Zamawiający przedstawił wybiórczo informację z prowadzonych testów nie przedstawił bowiem informacji o teście realizowanym wspólnie z odwołującym, w

którym łączność w technologii LoRaWAN osiągnęła poziom 100 0/0 zakładanego w postępowaniu SLA o czym w dalszej części pisma.

c/ Brak analizy ryzyka — zamawiający powołuje się na przepisy NIS2, Krajowego Systemu Cyberbezpieczeństwa oraz RODO, podkreślając wagę bezpieczeństwa danych i ochrony infrastruktury krytycznej. Jednak w całym piśmie brak jest analizy ryzyka lub ekspertyzy, z której wynikałoby, że dopiero przy poziomie 90% dla telefonii komórkowej zagrożenia cyberbezpieczeństwa są wykluczone w sposób właściwy. Takie arbitralne przyjęcie wskaźnika procentowego nie spełnia wymogu proporcjonalności.

d/ Skutek rynkowy — ustanowienie wymogu 90/10 prowadzi w praktyce do zawężenia kręgu potencjalnych wykonawców wyłącznie do podmiotów powiązanych z operatorami komórkowymi, co zostało dostrzeżone również w treści odwołania. Tymczasem art. 99 ust. 4 ustawy stanowi, że opis przedmiotu zamówienia nie może prowadzić do nieuzasadnionego ograniczenia konkurencji. Zamawiający nie wykazał, aby eliminacja integratorów, operatorów hurtowych czy podmiotów korzystających z modeli dzierżawczych była konieczna dla realizacji zamówienia.

Odwołujący wskazał, że zamawiający nie wykazał, aby ustalenie proporcji 90/10 było uzasadnione jego rzeczywistymi potrzebami. Wymóg ten jest arbitralny, nie znajduje oparcia w wynikach pilotażu ani w przepisach prawa, a jego skutkiem jest nieproporcjonalne ograniczenie konkurencji poprzez uprzywilejowanie operatorów komórkowych i ich partnerów.

## 2/ Obowiązek uzasadnienia wymogów — orzecznictwo KIO i TSUE

Zamawiający w swojej odpowiedzi na odwołanie ograniczył się jedynie do ogólnych stwierdzeń o wyższości pasm licencjonowanych nad nielicencjonowanymi, nie udowadniając, a nawet nie wykazując w żaden sposób, dlaczego wymóg realizacji 90%) transmisji w technologii komórkowej miałby być uzasadniony rzeczywistymi potrzebami zamawiającego.

Brak jakiegokolwiek analizy danych z pilotażu, brak wskazania związku z parametrami SLA oraz brak dowodów technicznych sprawia, że przyjęcie wskaźnika 90/10 ma charakter arbitralny.

Ten wniosek znajduje pełne potwierdzenie w orzecznictwie Krajowej Izby Odwoławczej i Trybunału Sprawiedliwości UE, które jednoznacznie wskazują, że ciężar wykazania obiektywnych potrzeb i proporcjonalności wymagań spoczywa na zamawiającym. Sama deklaracja, że pasmo licencjonowane jest „bezpieczniejsze”, nie spełnia tego wymogu.

W szczególności powołał wyrok z dnia 6 września 2024 r., sygn. KIO 2918/24 wyrok z dnia 24 lipca 2023 r., sygn. KIO 959/23. Podobnie TSUE w sprawie C-368/10 stwierdził, że wszelkie ograniczenia konkurencji muszą być uzasadnione rzeczywistymi potrzebami i proporcjonalne.

## 3/ Systemowe ograniczanie konkurencji

W ocenie odwołującego, analizowany wymóg (90% pasmo komórkowe 10% pasmo inne) nie stanowi jednostkowego przypadku, lecz wpisuje się w szerszy, systemowy trend ograniczania konkurencji w zamówieniach publicznych w sektorze wodociągowym.

Podobne postanowienia były bowiem formułowane już w innych dużych postępowaniach przetargowych — m.in. w Krakowie oraz w Bydgoszczy — gdzie zamawiający również ustanawiali wymogi de facto eliminujące z rynku technologie alternatywne wobec technologii komórkowych (w szczególności LoRaWAN, Sigfox czy inne rozwiązania LPWAN).

Wymóg korzystania w co najmniej 90% z pasma na które dany przedsiębiorca uzyskał rezerwację częstotliwości (NB-IoT, LTE-M) prowadzi do sytuacji, w której konkurencja technologiczna zostaje sztucznie ograniczona do wybranej grupy dostawców — operatorów komórkowych oraz ich partnerów handlowych, co nie ma odzwierciedlenia w rzeczywistych potrzebach zamawiającego. Integratorzy, operatorzy MVNO czy podmioty budujące własną infrastrukturę IoT zostają z góry wykluczeni, pomimo że technicznie są zdolni zapewnić parametry SLA, bezpieczeństwo transmisji i zgodność z wymogami prawa.

Tego rodzaju praktyka stanowi w istocie tworzenie barier wejścia na rynek przez opis przedmiotu zamówienia w sposób faworyzujący jedną rodzinę technologii. W konsekwencji następuje nieuzasadnione ograniczenie konkurencji, które stoi w sprzeczności z art. 99 ust. 4 ustawy oraz zasadami uczciwej konkurencji wynikającymi z art. 16 ust. 1 i 3 ustawy.

Co istotne, systemowe powtarzanie identycznych wymogów w kolejnych postępowaniach (Kraków, Bydgoszcz, obecnie Katowice) dowodzi, że mamy do czynienia z praktyką rynkową eliminującą w sposób sztuczny inne rozwiązania technologiczne niż operatorów komórkowych. Oznacza to, że ograniczenie konkurencji nie jest wynikiem specyficznych potrzeb Katowic, lecz wynika z przyjętego wzorca opisu przedmiotu zamówienia.

Podkreślił, że takie działanie jest szczególnie niebezpieczne z punktu widzenia systemu zamówień publicznych, gdyż prowadzi do de facto zamknięcia rynku przed innowacyjnymi rozwiązaniami IoT, które są w stanie spełnić wymagania jakościowe i bezpieczeństwa przy niższych kosztach dla zamawiających. Skoro bowiem w kilku dużych miastach zastosowano niemal identyczne ograniczenia, mamy do czynienia z praktyką, która w sposób powtarzalny i systemowy eliminuje technologie inne niż komórkowe. W konsekwencji należy uznać, że wymóg 90% pasma komórkowego w Katowicach nie wynika z obiektywnych potrzeb tego zamawiającego, lecz jest elementem szerszego schematu

ograniczania konkurencji technologicznej w postępowaniach Tego rodzaju praktyka narusza fundamentalne zasady ustawy oraz zasady prawa unijnego w zakresie równego traktowania wykonawców i proporcjonalności wymogów.

#### 4/ Uwagi szczegółowe

Odpowiedź na zarzut pierwszy — brak podstaw prawnych i niejasność pojęcia „pasmo nielicencjonowane” Odnosząc się do argumentacji zamawiającego dotyczącej wymogu korzystania w co najmniej 90% z pasma licencjonowanego, odwołujący podkreślił, że zamawiający w swojej odpowiedzi szeroko powołuje przepisy prawa telekomunikacyjnego (w tym nieobowiązującej ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne oraz ustawy z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej — Dz.U. z 2024 r. poz. 1221 dalej również „PKE”).

Jednakże w żadnym z tych aktów prawnych nie występuje pojęcie „pasmo nielicencjonowanego”, którym posługuje się zamawiający. Faktycznie w PKE funkcjonuje kategoria „rezerwacji częstotliwości” (art. 2 pkt 50 PKE), czyli prawo do korzystania z określonego zakresu częstotliwości w oparciu o decyzję Prezesa UKE. Nie oznacza to jednak, że pozostałe częstotliwości stanowią „pasmo nielicencjonowane” w rozumieniu przyjętym przez zamawiającego.

W świetle obowiązujących przepisów Prawa komunikacji elektronicznej można mówić jedynie o: a/ częstotliwościach wymagających rezerwacji (tzw. pasma objęte rezerwacją), oraz b/ częstotliwościach ogólnodostępnych (np. pasma ISM), które mogą być wykorzystywane na warunkach określonych w przepisach szczególnych, bez konieczności uzyskania indywidualnej rezerwacji.

W żadnym jednak miejscu przepisy PKE nie posługują się pojęciem „pasmo nielicencjonowanego”. Jest to wyłączenie sformułowanie użyte przez zamawiającego, niemające definicyjnego zakotwiczenia w obowiązującym prawie.

Należy podkreślić, że zgodnie z art. 99 ust. 1 i 2 ustawy opis przedmiotu zamówienia musi być dokonany w sposób jednoznaczny, wyczerpujący, a zarazem zrozumiały dla wykonawców. Posługiwanie się w dokumentacji przetargowej i w odpowiedzi na odwołanie pojęciem, które nie występuje w żadnym obowiązującym akcie prawnym, stoi w oczywistej sprzeczności z tym wymogiem.

Skoro zamawiający przyznał, że jedynym ustawowym pojęciem jest „rezerwacja częstotliwości”, to użycie kategorii „pasmo nielicencjonowanego” — bez definicji legalnej i bez odniesienia do konkretnego przepisu — prowadzi do niejasności co do zakresu wymagań i sposobu ich oceny.

Zamawiający nie wykazał, aby pojęcie „pasmo nielicencjonowane” miało charakter jednoznaczny i zrozumiały. Wymóg oparty na tym pojęciu jest wadliwy, gdyż: a/ nie znajduje oparcia w obowiązujących przepisach prawa, b/ jest nieprecyzyjny i niedookreślony, c/ powoduje niepewność wykonawców co do sposobu spełnienia warunków zamówienia. Tym samym wymóg ten narusza art. 99 ust. 1—2 ustawy oraz art. 16 ust. 1 i 3 ustawy, gdyż wprowadza opis przedmiotu zamówienia w sposób niejednoznaczny, utrudniający uczciwą konkurencję i równe traktowanie wykonawców.

W świetle powyższego bez odwołania się do rezerwacji częstotliwości jako dokumentu indywidualnego wydanego przez organ regulacyjny może być twierdzenie, że licencja to uprawnienie wynikające z przepisów prawa, które określają zasady korzystania z określonych zakresów częstotliwości bez konieczności uzyskania indywidualnej rezerwacji. Warunkiem korzystania z tego uprawnienia jest spełnienie wymagań technicznych określonych w normach ETSI (np. EN 300 220). W tym sensie:

czy „licencją” jest samo ustawowe uprawnienie, a zgodność urządzenia z ETSI EN 300 220 jest warunkiem materialnym, który sprawia, że dane urządzenie mieści się w ramach prawnych i faktycznie może korzystać z tego uprawnienia.

W świetle prawa komunikacji elektronicznej „licencją” jest również ustawowe uprawnienie do korzystania z określonych pasm radiowych na zasadach ogólnych, o ile wykorzystywane urządzenia spełniają wymagania techniczne wynikające z norm ETSI (np. EN 300 220).

Odpowiedź na zarzut pierwszy — Brak dowodów na zajętość pasma — arbitralne twierdzenia zamawiającego

Odwołujący przyjął i posługuje się na potrzeby tego pisma nomenklaturą stosowaną przez zamawiającego, zgodnie z treścią OPZ, tj. określaniem uprawnienia do pracy urządzenia w danym paśmie mianem 'licencji'. Zamawiający twierdzi, że pasmo otwarte (nielicencjonowane, publiczne) posiada z natury słabszą ochronę, jest podatne na zakłócenia i utratę danych oraz — jak wskazano — „traci zasięg w funkcji zajętości tych pasm, co przekłada się na utratę transmisji danych w zwartych, gęstych lokalizacjach, jak ma to miejsce na obszarze gminy Katowice”.

Stanowisko to nie znajduje żadnego oparcia w materiale dowodowym. Należy bowiem podkreślić, że: a/ brak badań ze strony zamawiającego — zamawiający w żadnym miejscu nie wykazał, że przeprowadził jakiegokolwiek pomiary pasma ISM (w Tm LoRaWAN 868 MHz) na obszarze Katowic. Nie wskazano żadnych wyników, raportów, czy analiz widma radiowego, które dokumentowałyby „zajętość pasma” w Katowicach. Tym samym twierdzenia zamawiającego mają wyłącznie charakter spekulacyjny, nieoparty żadnym dowodem.

b/ Brak wskazania źródła danych — zamawiający nie podał, na czym opiera twierdzenie o zajętości pasma w Katowicach. Z treści odpowiedzi wynika jednoznacznie, że są to czysto hipotetyczne stwierdzenia, nieoparte żadnym

obiektywnym materiałem.

c/ Wątpliwości budzi także wiarygodność i moc „dowodu” złożonego przez zamawiającego w postaci notatki z dnia 5 grudnia 2024 r. na okoliczność wyboru technologii stacjonarnego odczytu wodomierzy. Jak wynika bowiem z art. 233 par. 1 kpc, sąd ocenia wiarygodność i moc dowodów według własnego przekonania, na podstawie wszechstronnego rozważenia zebranego materiału. Tymczasem przedłożona notatka zawiera ogólne oświadczenia o weryfikacji przez podpisanych skuteczności działania systemów odczytowych i technologii wskazanych w notatce podmiotów oraz wynikach przeprowadzonych testów. W notatce brak jest podstawowych informacji takich jak sposób przeprowadzenia testów oraz dokładnej lokalizacji, gdzie te testy przeprowadzono. Ponadto, do notatki nie załączono np. dokumentacji zdjęciowej czy też video, mającej potwierdzić wyniki testów.

Zastanawiające jest też to, że pomimo, że zgodnie z treścią notatki w spotkaniu dotyczącym wyboru technologii stacjonarnego odczytu wodomierzy wzięły udział 4 osoby, to notatkę podpisały jedynie 3 z nich. Osobą, która nie podpisała notatki, jest osoba zajmująca stanowisko merytoryczne, p. Barbara Gazda — Kierownik Działu Wodomierzy.

d/ Dowód przeciwny przedstawiony przez odwołującego — w odpowiedzi na stanowisko zamawiającego odwołujący przedstawił wyniki własnego badania zajętości pasma LoRaWAN (868 MHz) na terenie Katowic. Badanie to jednoznacznie wskazuje, że pasmo jest wolne i dostępne w zakresie pozwalającym na stabilną transmisję danych. Oznacza to, że zarzut „funkcji zajętości pasma” jest bezpodstawny, skoro w badaniu empirycznym nie potwierdzono jego występowania.

Konsekwencje procesowe — zgodnie z art. 534 ust. 1 ustawy to strona, która wywodzi skutki prawne z określonych twierdzeń, zobowiązana jest do ich udowodnienia. Skoro zamawiający twierdzi, że pasmo LoRaWAN w Katowicach jest „zajęte” i „traci zasięg”, to powinien przedstawić twarde dane pomiarowe. Brak takich dowodów oznacza, że jego stanowisko należy uznać za gołosłowne.

e/ Brak proporcjonalności — jeżeli faktycznie zamawiający chciał oprzeć opis przedmiotu zamówienia na obiektywnych uwarunkowaniach radiowych, powinien przeprowadzić badania widma (tj. realizacji czynności pomiaru i analizy zajętości określonego pasma częstotliwości w celu oceny jego przydatności do transmisji danych w sieciach radiowych) i dopiero na tej podstawie określić dopuszczalny udział technologii LoRa. Tymczasem ograniczenie ich do 10% oparto wyłącznie na założeniu teoretycznym, że „pasmo może być zajęte”. To nie spełnia wymogu proporcjonalności do wartości i celów przedmiotu zamówienia, o której mowa w art. 99 ust. 2 ustawy.

Wniosek dowodowy nr 1.

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu — raportu z pomiarów pasma LoRaWAN 868 MHz, przeprowadzonych na terenie miasta Katowice, który stanowi załącznik nr I do pisma.

Raport ten jednoznacznie potwierdza, że pasmo 868 MHz pozostaje wolne od zakłóceń w zakresie istotnym dla prawidłowej pracy systemu oraz może być w pełni wykorzystane do realizacji transmisji danych w ramach systemu zdalnego odczytu wodomierzy.

Dowód ten ma na celu wykazanie, że twierdzenia zamawiającego o rzekomej niedostępności i zakłócalności pasma nielicencjonowanego nic znajdują oparcia w stanie faktycznym.

Raport stanowi załącznik nr 1 do pisma.

Jednocześnie wniósł o zastrzeżenie materiału dowodowego jako tajemnicy przedsiębiorstwa

Wniosek o utajnienie

Na podstawie art. 545 ust. 3 ustawy wniósł o utajnienie dowodu („Załącznik I Raport z pomiarów”) przed innymi uczestnikami postępowania odwoławczego, z wyjątkiem zamawiającego oraz Krajowej Izby Odwoławczej z uwagi na okoliczność, że informacje w ww. dokumencie stanowią tajemnicę przedsiębiorstwa Emitel w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji.

Dokument zawiera bowiem szczegółowe dane techniczne oraz technologiczne przedsiębiorstwa, a ich ujawnienie mogłoby narazić Emitel na szkodę. Oświadczył, że informacje te, zarówno jako całość, jak i w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji oraz nie są łatwo dostępne dla takich osób.

Zamawiający w swojej argumentacji posługuje się uproszczonym i nielogicznym twierdzeniem dotyczącym rzekomej „zajętości pasma” lub „zakłóceń” w technologii LoRaWAN. Twierdzenie to oparte jest na założeniu, że samo wystąpienie kilku transmisji prowadzi do utraty danych, co ma rzekomo odróżniać LoRaWAN od technologii komórkowych. Jest to jednak rozumowanie całkowicie chybione, ponieważ mechanizm współdzielenia pasma jest immanentną cechą każdej technologii radiowej, także GSM, LTE, NB-IoT czy LTE-M.

Twierdzenie zamawiającego, że w przypadku kilku transmisji w paśmie LoRaWAN dojdzie do zajętości i utraty danych, jest argumentem całkowicie chybionym i wewnętrznie sprzecznym.

Każda technologia radiowa — w tym GSM, LTE, NB-IoT czy LTE-M — zakłada współdzielenie zasobów częstotliwościowych przez wielu użytkowników. Jeżeli kilku abonentów telefonii komórkowej równocześnie prowadzi

rozmowy czy transmisję danych, również dochodzi do zajętości pasma. Nie oznacza to jednak, że technologia komórkowa jest niefunkcjonalna — przeciwnie, technologia została zaprojektowana do obsługi wielu jednoczesnych transmisji, podobnie jak LoRaWAN.

Po drugie, LoRaWAN dysponuje własnymi mechanizmami zarządzania kolizjami i retransmisją (ALOHA, adaptacyjne dobieranie SF — spreading factor, ADR — Adaptive Data Rate), które umożliwiają efektywną pracę przy dużej liczbie urządzeń. W praktyce testy pokazują, że sieć LoRaWAN bez problemu obsługuje dziesiątki tysięcy modułów przy zachowaniu SLA, a jedna stacja bazowa jest w stanie obsłużyć do kilkudziesięciu tysięcy urządzeń.

Po trzecie, gdyby konsekwentnie stosować logikę zamawiającego, to należałoby uznać, że również GSM, NB-IoT czy LTE-M nie nadają się do użycia, bo tam też występują sytuacje przeciążenia, np. w godzinach szczytu w centrach miast. W rzeczywistości żadna sieć radiowa nie gwarantuje absolutnej odporności na kolizje transmisji — każda technologia rozwiązuje ten problem na swój sposób, zapewniając minimalny poziom jakości transmisji.

Wniosek dowodowy nr 2

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentów karty katalogowej stacji bazowej LoRaWAN firmy Kerlink Wirnet iStation, oraz prezentacji sprzedażowej polskiego dystrybutora urządzeń Kerlink spółki JM elektronik Sp z o.o. który to dokumenty potwierdza, że stacje bazowe LoRaWAN są przystosowane do obsługi wysokich wolumenów urządzeń końcowych oraz milionów dwukierunkowych wiadomości każdego dnia.

Zgodnie z dokumentacją producenta, brama iStation jest w stanie przetworzyć ponad 700 000 wiadomości dziennie, co w przypadku scenariusza jednego komunikatu na dzień z urządzenia końcowego oznacza teoretyczną zdolność obsługi 700 000 urządzeń

Dane te jednoznacznie obalają twierdzenia zamawiającego, jakoby technologia LoRaWAN była niezdolna do zapewnienia masowej transmisji danych lub nie gwarantowała skalowalności wymaganej dla systemów zdalnego odczytu.

Celem przeprowadzenia dowodu jest wykazanie, że LoRaWAN zapewnia skalowalność znacznie przewyższającą potrzeby zamawiającego (24 000 modułów), a jej ograniczanie do 10% lokalizacji nie znajduje żadnego racjonalnego ani technicznego uzasadnienia.

Emitel w projekcie przyjmuje, że 1 stacja bazowa LoRaWAN obsłuży 20000 urządzeń co przy założeniu projektu 60 stacji bazowych daje teoretyczną możliwość obsługi 1.2 mil. urządzeń nakładek.

Karta katalogowa, z prezentacji dystrybutora spółki JM elektronik Sp z o.o. stanowi załącznik nr 2 do pisma. Dokument złożono wraz z tłumaczeniem na język polski. Elementy prezentacji ang. Features — pol. Funkcje / cechy. > 700 K msg/day (ang.) — 700 tys wiadomości dziennie (pol)

Wniosek dowodowy nr 3

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu — Decyzji Wykonawczej Komisji (UE) 2019/1345 z dnia 2 sierpnia 2019 r. zmieniającej decyzję 2006/771/WE w sprawie aktualizacji zharmonizowanych warunków technicznych w zakresie wykorzystania widma radiowego na potrzeby urządzeń bliskiego zasięgu (notyfikowana jako dokument nr C(2019) 5660, Tekst mający znaczenie dla EOG).

Dowód ten ma wykazać, że:

Mechanizm współdzielenia pasma jest immanentną cechą każdej technologii radiowej — dotyczy to zarówno pasm tzw. „nielicencjonowanych” (np. 868 MHz), jak i pasm licencjonowanych (np. GSM, NB-IoT).

Decyzja Komisji jednoznacznie przewiduje, że urządzenia radiowe w pasmach ISM mogą działać bez indywidualnych rezerwacji częstotliwości, jednak pod ścisłymi warunkami technicznymi (m.in. moc nadawcza, cykl pracy, kompatybilność elektromagnetyczna).

Zasada ta dowodzi, że współdzielenie pasma nie jest wadą technologii LoRaWAN, lecz elementem powszechnie przyjętego systemu regulacyjnego UE. Podobny mechanizm współdzielenia stosowany jest w GSM, LTE czy NB-IoT, gdzie wielu użytkowników korzysta z jednego pasma. Dokument stanowi załącznik nr 3 do pisma.

Każda technologia radiowa — niezależnie od tego, czy działa w paśmie licencjonowanym (np. GSM, LTE, NB-IoT), czy nielicencjonowanym (np. LoRaWAN) — opiera się na współdzieleniu pasma częstotliwościowego przez wielu użytkowników. Różnią się jedynie stosowane mechanizmy kontroli dostępu, zarządzania kolizjami i retransmisji.

Poniższa tabela przedstawia zestawienie kluczowych rozwiązań:

Technologia	Mechanizm współdzielenia pasma	Opis działania
GSM (2G)	TDMA + FDMA	Pasmo dzielone na kanały częstotliwościowe (FDMA), a każdy kanał dodatkowo na szczeliny czasowe (TDMA). W danej chwili użytkownik korzysta z przypisanego timeslotu.
LTE (4G)	OFDMA + dynamic scheduling	Pasmo dzielone na bloki zasobów (resource blocks). eNodeB przydziela je użytkownikom co 1 ms, uwzględniając obciążenie i jakość sygnału. Mechanizmy HARQ zapewniają retransmisję w razie błędów.
NB-IoT LTE-M	Resource Units repetitions + QoS	Zasoby przydzielane dynamicznie przez stację

bazową. Możliwe wielokrotne powtórzenia ramek dla poprawy zasięgu. QoS pozwala ustalać priorytety transmisji.

LoRaWAN (868 MHz) ALOHA + ADR(Adaptive Data Rate) +

SF (Spreading Factor) Urządzenia wysyłają dane zgodnie z protokołem ALOHA. Sieć automatycznie dostosowuje prędkość transmisji (ADR) i spreading factor. Bramy obsługują setki tysięcy pakietów dziennie.

Z powyższego porównania jasno wynika, że współdzielenie pasma jest immanentną cechą każdej technologii radiowej. GSM, LTE, NB-IoT i LoRaWAN różnią się jedynie narzędziami stosowanymi do organizacji tego współdzielenia, ale zasada jest identyczna: wielu użytkowników jednocześnie korzysta z ograniczonych zasobów widma.

Wniosek dowodowy nr 4

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu publikacji naukowej N.A. „The ALOHA System — Another alternative for computer communications” (University of Hawaii, 1970).

Dowód ten ma wykazać, że:

Protokół ALOHA, stanowiący podstawę funkcjonowania technologii LoRaWAN, został opracowany i udokumentowany jako skuteczny mechanizm dostępu do współdzielonego pasma radiowego. Już w pierwotnych badaniach wykazano, że system ALOHA umożliwia obsługę wielu niezależnych transmisji radiowych przy zapewnieniu stabilności całej sieci, co zostało następnie rozwinięte i wdrożone w nowoczesnych technologiach LPWAN.

Argument zamawiającego, jakoby współdzielenie pasma LoRaWAN uniemożliwiało zachowanie parametrów SLA, jest bezpodstawny — ponieważ współdzielenie pasma jest rozwiązane w warstwie protokołu, a jego skuteczność została potwierdzona zarówno w literaturze naukowej, jak i w praktycznych wdrożeniach sieci.

Dokument z tłumaczeniem stanowi załącznik nr 4 do pisma.

Technologia LoRaWAN, oprócz prostego i skutecznego mechanizmu współdzielenia pasma opartego na protokole ALOHA, posiada także dodatkowe mechanizmy po które można sięgnąć zwiększające stabilność i niezawodność transmisji:

1/ Rozpraszanie sygnału (Chirp Spread Spectrum)

LoRaWAN wykorzystuje modulację CSS (chirp spread spectrum), która znacząco zwiększa odporność na zakłócenia i interferencje, także w warunkach dużego nasycenia sygnałami pochodzącymi od innych systemów.

2/ Skakanie po częstotliwościach (frequency hopping)

Urządzenia przy każdej transmisji losowo wybierają kanał, stosując mechanizm frequency hopping. Rozwiązanie to dodatkowo redukuje prawdopodobieństwo kolizji oraz równomiernie rozkłada obciążenie ruchu w paśmie.

3/ Dodatkowe mechanizmy redukcji kolizji

-ADR (Adaptive Data Rate) sieć automatycznie dostosowuje parametry transmisji (moc nadajnika, współczynnik rozpraszania SF) dla każdego urządzenia, minimalizując czas trwania transmisji i ryzyko zakłóceń.

-Backoff— w przypadku nieudanej transmisji urządzenie odczeka losowy czas przed ponowną próbą wysyłki, co znacząco ogranicza ryzyko kolejnych kolizji i stabilizuje ruch w sieci.

Co istotne, raport z badania pasma ISM 868 MHz przeprowadzony przez odwołującego w Katowicach jednoznacznie wykazał dostępność wolnych częstotliwości, które mogą zostać bezpiecznie wykorzystane na potrzeby transmisji danych z wodomierzy. Oznacza to, że argumentacja zamawiającego, jakoby pasmo nielicencjonowane było przeciążone lub niewystarczającej jakości, jest całkowicie gołosłowna i nie znajduje potwierdzenia w żadnych rzetelnych badaniach.

Brak gwarancji trwałości rezerwacji częstotliwości oraz niepewność technologii komórkowych zamawiający powołuje się na przewagę pasm „licencjonowanych”, wskazując, że zapewniają one „stabilną i przewidywalną transmisję” dzięki decyzjom rezerwacyjnym Prezesa UKE. Argument ten nie wytrzymuje jednak krytyki w świetle realiów rynku polskiego oraz faktycznych danych wynikających z wykazu rezerwacji ogólnopolskich.

a/ Krótki horyzont czasowy rezerwacji częstotliwości — większość obowiązujących decyzji rezerwacyjnych, na które powołuje się zamawiający, ma okres ważności krótszy niż 10 lat, czyli mniej niż planowany okres realizacji zamówienia przez Wodociągi Katowickie (2026—2036). W aktualnym rejestrze Prezesa UKE (stan na 01.08.2025 r.) żaden z operatorów komórkowych przystępujących (F-Mobile Polska, Orange Polska, Polkomtel) nic posiada rezerwacji w pasmach 700, 800 ani 900 MHz — tj. pasmach wykorzystywanych do świadczenia usług NB-IoT i LTE-M — ważnej do 2036 roku. Najdłuższe dostępne rezerwacje sięgają roku 2030—2032, a więc kończą się w trakcie obowiązywania umowy. Stabilność pasm licencjonowanych jest więc pozorna, a ryzyko regulacyjne realne.

b/ Ewolucja technologiczna — NB-IoT i LTE-M działają w standardzie 4G. Tymczasem zarówno w Polsce, jak i w UE, trwa intensywne migracja do 5G. Operatorzy posiadają już długoterminowe rezerwacje pasma 700 MHz (Band n28) ważne do 2040 r. — jedyne wśród pasm 700/800/900 MHz z takim horyzontem czasowym. Jednak rezerwacje te są wykorzystywane wyłącznie do uruchamiania usług 5G NR, co potwierdzają m.in. Orange i T-Mobile w Polsce. W efekcie NB-IoT i LTE-M, które mogą być wykorzystane jako technologie dla Wodociągów Katowickich, nadal działają w pasmach 800 MHz i 900 MHz, których rezerwacje wygasają około 2030—2032 — czyli

przed zakończeniem okresu obowiązywania umowy (2026—2036). W tych samych latach technologie 4G mogą być dodatkowo stopniowo marginalizowane, co podważa długoterminową wydajność i niezawodność usług NB-IoT/LTE-M w całym horyzoncie kontraktu.

c/ Brak unikatowej gwarancji wyższości — technologie komórkowe nie zapewniają niezawodności przez cały okres 10-letniego kontraktu. W trakcie jego trwania mogą pojawić się zmiany w polityce widma, w decyzjach Prezesa UKE, a także w strategiach biznesowych operatorów. Co więcej, nabycie nakładek na wodomierze w technologii NB-IoT (T-Mobile/Polkomtel) albo LTE-M (Orange) uniemożliwia późniejszą zmianę operatora — jeżeli T-Mobile utraci rezerwację, a Orange uruchomi na tym paśmie wyłącznie LTEM (CAT-M), konieczna będzie wymiana urządzeń końcowych. Analogiczna sytuacja wystąpi w odwrotnym przypadku.

d/ Ryzyko zamawiającego — ograniczenie się wyłącznie do technologii komórkowych przesuwa na zamawiającego pełne ryzyko regulacyjne i technologiczne, zarówno związane z wygaśnięciem decyzji rezerwacyjnych w trakcie trwania kontraktu, jak i z wygaszaniem technologii 4G. Różnicowanie technologiczne (np. dopuszczenie LoRaWAN), a nie jego sztuczne ograniczanie.

e/ Brak ryzyka w przypadku LoRaWAN — w przeciwieństwie do NB-IoT i LTE-M, technologia LoRaWAN działa w nielicencjonowanych pasmach ISM (np. 868 MHz), które nie są objęte krótkoterminowymi decyzjami rezerwacyjnymi Prezesa UKE. Dostęp do tych częstotliwości nie zależy od wyników przetargów ani od strategii operatorów komórkowych, a więc nie występuje ryzyko utraty usług wskutek wygaśnięcia rezerwacji lub zmian regulacyjnych. LoRaWAN eliminuje zatem ryzyko, które w przypadku technologii komórkowych obciąża zamawiającego i podważa stabilność kontraktu w perspektywie 10 lat.

Wniosek dowodowy nr 5

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu w postaci wykazu rezerwacji ogólnopolskich Prezesa UKE (plik „2025-08-01\_rezerwacje\_cala\_pl.xlsx”, stan na OI .08.2025 r.) a także na okoliczność:

1/ że żaden z operatorów komórkowych (T-Mobile Polska, Orange Polska, Polkomtel) nie dysponuje rezerwacją w pasmach 800 MHz lub 900 MHz ważną do stycznia 2036 r., co potwierdza brak stabilności tych pasm.

2/ że pasma 800 MHz i 900 MHz wygasną przed końcem planowanego okresu obowiązywania umowy Wodociągów Katowickich (2026—2036).

3/ że w związku z tym rezerwacje w pasmach 800/900 MHz nie gwarantują ciągłości i niezawodności Świadczenia usług przez cały czas trwania kontraktu.

4/ że technologia LoRaWAN, działająca w paśmie nielicencjonowanym (ISM, np. 868 MHz), nie podlega ograniczeniom wynikającym z decyzji rezerwacyjnych Prezesa UKE i nie generuje ryzyka utraty rezerwacji, w przeciwieństwie do technologii komórkowych. Wykaz stanowi załącznik nr 5 do pisma.

W Polsce wszyscy główni operatorzy (Orange, T-Mobile, Polkomtel) posiadają obecnie rezerwacje w paśmie 700 MHz, ważne do 2040 r. — są to jedyne rezerwacje w pasmach 700/800/900 MHz o tak długim horyzoncie czasowym. Jednakże z dokumentów UKE oraz publikacji operatorów wynika jednoznacznie, że pasmo 700 MHz zostało przeznaczone na budowę sieci 5G (Band n28), a nie na świadczenie usług IoT w standardzie NB-IoT czy LTE-M.

Orange oraz T-Mobile już uruchomiły na nim komercyjne usługi 5G, co potwierdzają komunikaty prasowe, natomiast Polkomtel posiada blok 718—723 / 773—778 MHz zarezerwowany w ramach aukcji UKE na potrzeby 5G. NB-IoT i LTE-M nadal działają wyłącznie w pasmach 800 MHz i 900 MHz, których rezerwacje wygasają w latach 2030—2032, czyli przed końcem umowy Wodociągów Katowickich (2026—2036). Oznacza to, że pasmo 700 MHz nie stanowi podstawy dla usług NB-IoT/LTE-M i nie zapewnia ich stabilności w perspektywie kontraktu.

Wniosek dowodowy nr 6

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentów w postaci wydruków ze stron internetowych oraz materiałów Urzędu Komunikacji Elektronicznej:

„Pierwsi klienci Orange mogą już korzystać z 5G w paśmie 700 MHz” — opublikowanej w serwisie Orange Polska (biuroprasowe.orange.pl),

„T-Mobile 5G w paśmie 700 MHz” — opublikowanej w serwisie Benchmark.pl (benchmark.pl),

Prezentacji Urzędu Komunikacji Elektronicznej pt. „Aukcja pasm 700 i 800 MHz” (plik PDF opublikowany na stronice UKE załączony do akt sprawy),

Prezentacji UKE pt. „Aukcja pasm 700 i 800 MHz” (plik PDF opublikowany na stronice UKF., załączony do akt sprawy),

Na okoliczność:

Że operatorzy komórkowi Orange Polska i T-Mobile Polska uruchomili usługi wyłącznie w technologii 5G NR (Band n28) w paśmie 700 MHz,

a/ że Polkomtel sp. z o.o. również posiada długoterminową rezerwację pasma 700 MHz do 2040 r., lecz brak jest dowodów na to, aby rezerwacja ta była wykorzystywana do usług NB-IoT czy LTE-M rezerwacja została przyznana w ramach aukcji przewidzianej dla budowy sieci 5G,

b/ że pasmo 700 MHz, mimo długiego horyzontu obowiązywania rezerwacji, jest przeznaczone do Świadczenia usług 5G, a nie do NB-IoT ani LTE-M (CAT-M),

c/ że technologie NB-IoT i LTE-M w Polsce funkcjonują wyłącznie w pasmach 800 MHz i 900 MHz, których rezerwacje wygasają w latach 2030—2032, a więc przed końcem okresu obowiązywania umowy Wodociągów Katowickich (2026—2036),

d/ że powyższe potwierdza, iż nawet w przypadku operatora Polkomtel (Plus), który posiada rezerwację 700 MHz, pasmo to nie zapewnia możliwości uruchamiania usług NB-IoT/LTE-M, a wyłącznie budowę sieci 5G NR.

Dokumenty te stanowią odpowiednio załącznik 6a-c do pisma.

Brak konsekwencji zamawiającego w ocenie technologii — asymetryczne podejście

Sam zamawiający wprost przyznaje, że technologia komórkowa nie jest w stanie w 10% pokryć potrzeb zamówienia, skoro zakłada możliwość zastosowania w 10% lokalizacji innych technologii transmisji danych (np. LoRaWAN). Innymi słowy, zamawiający jest świadomy, że technologia komórkowa również ulega zakłóceniom i nie gwarantuje stuprocentowej skuteczności. Mając tego świadomość, zamawiający tworzy jednak asymetryczne rozwiązanie:

a/ dopuszcza 10%) transmisji w innych technologiach niż telefonia komórkowa,

b/ lecz zupełnie odmawia przyjęcia rozwiązania odwrotnego, tj. aby zasadnicza część transmisji (np. 90%) odbywała się w sieciach telekomunikacyjnych innych aniżeli telefonii komórkowej np. sieci telekomunikacyjnej odwołującego a tylko 10% w telefonii komórkowej.

Taka konstrukcja jest wewnętrznie sprzeczna i arbitralna. Skoro bowiem sam zamawiający uznaje, że telefonia komórkowa nie zapewnia pełnej szczelności systemu i w części lokalizacji konieczne jest zastosowanie alternatywy, to nie istnieją żadne obiektywne podstawy, aby odrzucać proporcję odwrotną — w szczególności, że technologia LoRaWAN w realnych warunkach Katowic (co potwierdza dowód przedstawiony przez Odwołującego w postaci pomiarów zajętości pasma) Jest w pełni zdolna zapewnić wymogi SLA.

Co istotne — odwołujący nie kwestionuje w ogóle zasadności wykorzystania technologii komórkowej w realizacji zamówienia. Wręcz przeciwnie — w swoim modelu również przewiduje jej wykorzystanie, jednak w sposób proporcjonalny i racjonalny. Przedmiotem zarzutu nie jest więc wyłączenie lub całkowite zastąpienie telefonii komórkowej, lecz arbitralnie narzucone proporcje 90% telefonia komórkowa i 10% LoRaWAN.

Odwołujący podkreślił, że:

a/ Nierówne traktowanie technologii — zamawiający przyznaje telefonii komórkowej prymat absolutny, mimo że technologia ta także wymaga wsparcia innymi rozwiązaniami. To dowodzi, że preferencja telefonii komórkowej ma charakter sztuczny i nic jest oparta na obiektywnych potrzebach.

b/ Brak dowodów na zasadność ustalonych proporcji — zamawiający nie wykazał w żadnym miejscu, dlaczego aż 90% udziału w systemie ma przypadać na telefonię komórkową, a jedynie 100/0 na technologię LoRaWAN. Nie przedstawiono żadnej analizy technicznej które mogłyby uzasadniać takie proporcje.

Tymczasem to przedsiębiorca telekomunikacyjny, jako podmiot wyspecjalizowany i posiadający stosowne kompetencje techniczne, jest profesjonalistą w zakresie budowy i eksploatacji sieci telekomunikacyjnych. To on, na podstawie wiedzy eksperckiej i doświadczenia, mając na względzie cel zamówienia, powinien określać optymalny model architektury sieci i proporcje wykorzystania poszczególnych technologii transmisyjnych.

Przyjęcie ogólnych proporcji przez zamawiającego, bez jakiegokolwiek uzasadnienia technicznego, stanowi nie tylko działanie arbitralne, ale również prowadzi do naruszenia zasady racjonalności i proporcjonalności. W efekcie takie arbitralne narzucenie proporcji ogranicza konkurencję i uniemożliwia urzeczywistnienie innych, nowych sieci telekomunikacyjnych, aniżeli już istniejące. Tym samym rynek zostaje zamknięty na innowacyjne rozwiązania, które jedynie profesjonalny operator telekomunikacyjny — jako podmiot wyspecjalizowany i dysponujący odpowiednią wiedzą — jest w stanie obiektywnie ocenić i zrealizować.

Ograniczenie konkurencji — narzucenie proporcji 90/10 faworyzuje wykonawców powiązanych z operatorami komórkowymi, eliminując z rynku integratorów i operatorów systemów LoRaWAN, którzy mogliby w większości spełnić wymagania SLA, a sieć komórkową stosować jedynie pomocniczo. To stanowi naruszenie art. 99 ust. 4 ustawy i art. 16 ust. 1 i 3 ustawy.

Skoro zamawiający sam przyznaje, że sieć komórkowa nie spełnia w pełni wymogów zamówienia i dopuszcza w 10% przypadków wsparcie inną technologią (np. LoRaWAN), to nie ma podstaw, by odmawiać wykonawcy możliwości odwrotnego rozwiązania — 90% LoRaWAN i 10% sieci komórkowej — o ile spełnione zostaną wymagania SLA.

Odwołujący nie kwestionuje w ogóle możliwości wykorzystania technologii sieci komórkowej, lecz sprzeciwia się arbitralnemu i niezasadnionemu narzuceniu proporcji 90/10. Wymóg ten jest wewnętrznie niespójny, nieproporcjonalny i prowadzi do nieuzasadnionego ograniczenia konkurencji.

„Dorobiona” ex post argumentacja zamawiającego, nieznajdująca oparcia w OPZ i SWZ - Odniesienie do tabeli porównawczej zamawiającego zamieszczonej w Odpowiedzi na odwołanie

Zamawiający nic może tworzyć sztucznych i arbitralnych argumentów na etapie odpowiedzi na odwołanie, które nic wynikają z treści dokumentacji postępowania (OPZ ani SWZ). Wymagania dotyczące jakości transmisji, parametrów SLA, bezpieczeństwa i niezawodności zostały bowiem wprost określone w OPZ i są technologicznie neutralne — odnoszą się do rezultatu, jaki ma zostać a nie do konkretnej technologii (czy to telefonii komórkowej CAT-M/NB-IoT, czy LoRaWAN).

Odwołujący zauważył, że wymagania dotyczące technologii komórkowej oraz LoRaWAN w dokumentacji postępowania są tożsame — każda z nich musi zapewnić odczyt z minimum 90%) urządzeń dziennie, 95% tygodniowo i 98% miesięcznie, przy zachowaniu bezpieczeństwa danych i odporności systemu. Dokumentacja nie rozróżnia tych wymogów w zależności od technologii.

Dopiero na etapie odpowiedzi na odwołanie zamawiający zaprezentował tabelę porównawczą, w której przedstawił LoRaWAN w negatywnym świetle, przypisując jej wady, a technologiom komórkowymi wyłącznie zalety. Odwołujący wskazał, że tabela ta jest arbitralnym i jednostronnym wymysłem zamawiającego i stanowi próbę dorobienia ex post argumentacji, aby uzasadnić ograniczenie konkurencji. Etap postępowania odwoławczego nie jest etapem, na którym zamawiający powinien szukać argumentów mających rzekomo potwierdzić wcześniejsze ograniczenie konkurencji w prowadzonym przez niego postępowaniu. To przed wszczęciem postępowania zamawiający powinien dokonać analizy swoich uzasadnionych potrzeb i na ich podstawie tak przygotować dokumentację postępowania, by wykonawcy mogli zaoferować rozwiązania, które te potrzeby zaspokoją.

Skoro bowiem wymagania kontraktowe są jednakowe dla każdej technologii, to ocena technologii powinna odbywać się wyłącznie pryzmat tego, czy dany wykonawca jest w stanie te wymagania spełnić. W rzeczywistości jest to zatem sztuczna konstrukcja, która ma uzasadnić wcześniej arbitralnie narzuconą proporcję 90% komórkowa / 10% inne technologie. W ten sposób zamawiający zamiast bazować na obiektywnie sformułowanych wymaganiach OPZ dotyczących jakości transmisji, parametrów SLA, bezpieczeństwa i niezawodności, tworzy narrację podporządkowaną faworyzowaniu jednej technologii. Co więcej, składając odpowiedź na odwołanie zamawiający pominął fakt, że w porozumieniu z Emitel S.A. przeprowadził pilotażowe wdrożenie sieci LoRaWAN w aglomeracji katowickiej, w lokalizacjach wyznaczonych przez samego zamawiającego jako trudne pod względem odczytu wodomierzy a miesięczna skuteczność takiego odczytu była wyższa aniżeli przyjęta w SLA opisanym w obecnie prowadzonym przez zamawiającego postępowaniu.

W ramach tego pilotażu, po zainstalowaniu zakładanych trzech stacji bazowych LoRaWAN oraz 50 nakładek przeprowadzono testy, synchronizacje w bazach danych. Test był prowadzony w cyklu 28-dniowym (miesięcznym) i wykazał, że wszystkie zainstalowane nakładki dokonały co najmniej jednego skutecznego odczytu w okresie miesięcznym.

Zgodnie z postanowieniami OPZ (Załącznik nr 1), SLA miesięczne uznaje się za spełnione, jeżeli każda nakładka zgłosi się przynajmniej jeden raz w danym miesiącu rozliczeniowym. Wobec powyższego, w badanym okresie poziom SLA miesięcznego wyniósł 100%, gdyż wszystkie nakładki spełniły wymagane kryterium. Wynik ten jest lepszy niż wymagany w OPZ poziom SLA — 98% w skali miesiąca.

Fakt przeprowadzenia i wyniki tego pilotażu zostały udokumentowane w prezentacji przedstawionej na spotkaniu z kierownictwem Katowickich Wodociągów (wyciąg z prezentacji ze zrzutami z systemu odczytowego załącznik 7 do pisma). Brak jakiegokolwiek wzmianki o tym projekcie w odpowiedzi na odwołanie oraz w notatce służbowej zamawiającego należy uznać za działanie celowe — prowadzi ono do zniekształcenia rzeczywistego obrazu technologii LoRaWAN.

Wyniki testów jasno pokazują, że technologia LoRaWAN jest w stanie zapewnić, a wręcz przewyższyć wymagania określone przez samego zamawiającego w OPZ. Ukrycie tych informacji w odpowiedzi na odwołanie świadczy o jednostronnym podejściu Zamawiającego, który przedstawiając LoRaWAN w negatywnym Świetle, pomija dostępne dane wskazujące na wysoką skuteczność i niezawodność tego rozwiązania.

Wniosek dowodowy nr 7

Wniosek o dopuszczenie i przeprowadzenie dowodu z dokumentu w postaci „Zał. 7 — z systemu z opisem skuteczności 50 nakładek w trybie 28 dni”, obejmującego slajd zatytułowany „Skuteczność odczytów”, sporządzonego po zakończeniu pilotażowego wdrożenia technologii LoRaWAN przez Emitel S.A. w aglomeracji katowickiej w 2023 roku, na okoliczność:

1/ że pilotaż został przeprowadzony w aglomeracji katowickiej, w lokalizacjach wyznaczonych przez Katowickie Wodociągi S.A.,

2/ że w ramach pilotażu zainstalowano przewidziane stacje bazowe LoRaWAN oraz 50 nakładek,

3/ że testy prowadzone w trybie 28-dniowym (miesięcznym) wykazały skuteczność odczytów na poziomie 100% przyjmując kwalifikację SLA z OPZ dla odczytu miesięcznego, ,

4/ że uzyskane rezultaty są lepsze niż wymagane w OPZ poziomu SLA (98% miesięcznic),

5/ że dowód wprost potwierdza, iż technologia LoRaWAN zapewnia wymaganą niezawodność, a nawet przewyższa

wymagania zamawiającego,

Wniosek o utajnienie

Na podstawie art. 545 ust. 3 ustawy wniósł o utajnienie dowodu („Zał. 7 — Wyciąg z systemu.słajd Skuteczność odczytów) przed innymi uczestnikami postępowania odwoławczego, z wyjątkiem zamawiającego oraz Krajowej Izby Odwoławczej z uwagi na okoliczność, że informacje w ww. dokumencie stanowią tajemnicę przedsiębiorstwa Emitel w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Dokument zawiera bowiem szczegółowe dane techniczne oraz technologiczne naszego przedsiębiorstwa, a ich ujawnienie mogłoby narazić Emitel na szkodę. Oświadczył, że informacje te, zarówno jako całość, jak i w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji oraz nie są łatwo dostępne dla takich osób.

Arbitralne zestawienie technologii komórkowej i technologii LoRaWAN

Zamawiający przedstawił w uzasadnieniu tabelę zestawiającą rzekome cechy technologii opartych o pasmo licencjonowane (CAT-M/NB-IoT) i nielicencjonowane (LoRaWAN 868 MHz). Prezentacja ta jest jednak jednostronna i tendencyjna, a przede wszystkim nieoparta żadnym materiałem dowodowym.

a/ Regulacja prawna i zarządzanie dostępem — zamawiający twierdzi, że LoRaWAN 868 nie podlega regulacjom i jest narażona na zakłócenia. Jest to nieprawda: pasmo 868 MHz jest uregulowane w prawie UE (decyzje CEPT/ETSI), a w Polsce w komunikatach Prezesa UKE. Urządzenia korzystające z LoRaWAN muszą spełniać normy ETSI EN 300 220 w tym dotyczące mocy, modulacji i czasu pracy. Wbrew twierdzeniom zamawiającego, nie jest to „dziki” obszar bez regulacji, lecz pasmo z precyzyjnymi zasadami użytkowania. W przypadku stwierdzenia, że urządzenie w rozumieniu przepisów ustawy z dnia 13 kwietnia 2007 r. o kompatybilności elektromagnetycznej, wytwarzające pole elektromagnetyczne powoduje szkodliwe zakłócenie pracy innego urządzenia spełniającego zasadnicze wymagania w rozumieniu przepisów tej ustawy, na podstawie art. 436 ustawy PKE, Prezes Urzędu Komunikacji Elektronicznej w drodze decyzji administracyjnej jest uprawniony do wydania decyzji w zakresie zastosowania środków technicznych prowadzących do usunięcia przyczyny zakłóceń.

b/ Odporność na zakłócenie i niezawodność — protokół LoRaWAN wykorzystuje technikę rozproszonego widma (spread spectrum), co zwiększa odporność na interferencje. Posiada też mechanizmy retransmisji i adaptacji przepływności. Doświadczenia praktyczne z wdrożeń w miastach europejskich dowodzą, że sieci LoRaWAN z powodzeniem obsługują setki tysięcy urządzeń w gęstej zabudowie, bez utraty jakości transmisji.

c/ Zasięg — zamawiający wskazał, że LoRaWAN ma „ograniczony zasięg”. W praktyce zasięg pojedynczej stacji LoRaWAN wynosi od kilku do kilkunastu kilometrów w środowisku miejskim i nawet do 30—40 km w otwartym terenie (zob. wniosek dowodowy Sieć LoRaWAN: modele propagacji radiowej i ocena wydajności w różnych środowiskach w Libanie Rida El Chall, Samer Lahoud, and Melhem El Helou, Senior Member, IEEE ). W efekcie do pokrycia obszarów Katowic wymaga się znacząco mniejszej liczby stacji LoRa niż w przypadku stacji bazowych komórkowych, co stanowi istotną przewagę kosztową i operacyjną.

d/ Bezpieczeństwo transmisji — LoRaWAN implementuje szyfrowanie end-to-end (AES-128), co zapewnia integralność i poufność danych. Twierdzenie zamawiającego, że brak jest bezpieczeństwa, jest nieprawdziwe i sprzeczne z faktyczną specyfikacją protokołu. Co więcej, LoRaWAN daje pełną kontrolę nad danymi po stronie właściciela sieci, w przeciwieństwie do technologii komórkowej oraz sieci dosyłowe różnych dostawców usług telekomunikacyjnych.

e/ Zależność od sieci — LoRaWAN pozwala zamawiającemu na budowę i kontrolę własnej sieci (onpremise). W przypadku telefonii komórkowej zamawiający całkowicie uzależnia się od infrastruktury operatora komórkowego, co stanowi ryzyko vendor lock-in. Z punktu widzenia bezpieczeństwa i niezależności infrastruktury krytycznej, LoRaWAN daje większą kontrolę niż technologie komórkowe.

f/ Koszty początkowe i utrzymanie — zamawiający wskazał na rzekomo wyższe koszty utrzymania LoRaWAN. W rzeczywistości wdrożenia LoRaWAN charakteryzują się niższym CAPEX i OPEX, gdyż stacje bazowe są tańsze, a urządzenia końcowe mają żywotność baterii do 10 lat. Utrzymanie własnej sieci LoRaWAN nie generuje opłat abonamentowych dla operatora, co oznacza niższe koszty całkowite w okresie życia projektu.

Wniosek dowodowy nr 8

Wniósł o dopuszczenie i przeprowadzenie dowodu z

1/ stron z Suplementu do Dziennika Urzędowego Unii Europejskiej — Tenders Electronic Daily UED), przedstawiających aktywne ogłoszenia o zamówieniach publicznych w technologii LoRaWAN, pobranych w dniu 27 sierpnia 2025 r., oznaczonych jako Załącznik nr 8 — Wydruki ogłoszeń TED (LoRaWAN) a także z umów realizowanych przez Emitel usług telekomunikacyjnych przesyłu sygnału z wodomierzy w technologii LoRaWAN.

2/ informacji o wyborze oferty najkorzystniejszej Zakładu Wodociągów i Kanalizacji Sp. z o.o. Grodzisk Mazowiecki z dnia 12.02.2025 rok sygn. ZWIK/MG/DOO.540.000417.2025.1/0559

3/ Informacji z otwarcia oferty Wójt Gminy Lubianka sygn. SZP/271.13.2025 z dnia 22.08.2025 r, 4/ Informacji z otwarcia

oferty z dnia 23.02.2024r sygn.. IRO.271.2.1.2024.EW, Informacji o wyborze oferty najkorzystniejszej z dnia 03.04.2024 r sygn. IRO.271.2.1.2024.EW oraz z Specyfikacji Warunków Zamówienia postępowania Modernizacja infrastruktury wodno-kanalizacyjnej na terenie gminy Piekoszków.'

5/ Informacji z otwarcia oferty z dnia 23.06.2023 roku w postępowaniu na dostawę nakładek i systemu do stacjonarnych odczytów wodomierzy na terenie Chorzowa i Świętochłowic nr postępowania PZP/MD/2020.

6/ Wyciągu ze specyfikacji zamówienia na system zdalnego odczytu wodomierzy organizowanego przez PK Wronki sygn. ZP/14/2020

7/ Informacji z otwarcia oferty z dnia 07.07.2025 roku w postępowaniu przetargowym na Usługę wdrożenia i utrzymania systemu sterowania i zarządzania oświetleniem na terenie mst. Warszawy nr post. ZDM/UM/DZP/37/PN/15/25 oraz Opisu Przedmiotu Zamówienia pkt. 3.5.2 zgodnie z którym zamawiający dopuścił następujące rozwiązania sieciowe: mesh, mesh/hybrida lub jednolitą sieć na pasmach komercyjnych

Na okoliczność wykazania, że technologia LoRaWAN:

1/ jest powszechnie stosowana w zamówieniach publicznych w Unii Europejskiej,

2/ stanowi rozwiązanie dojrzałe rynkowo — zamawiane są zarówno urządzenia końcowe, jak i bramki, licencje serwerów sieci, usługi budowy i utrzymania sieci oraz łączności IoT,

3/ spełnia typowe wymogi określone w specyfikacjach OPZ w projektach smart mctering/IoT (transmisja w paśmie EU868, bezpieczeństwo, energooszczędność, skalowalność),

4/ a zatem obalą twierdzenia zamawiającego o rzekomej „niszowości” i braku przydatności LoRaWAN do realizacji zamówienia.

Dla ilustracji wskazuję przykładowo ogłoszenia ujęte w TED (numery ogłoszeń i państwa):

351995-2025 (IT) — dostawa statycznych wodomierzy z łącznością LoRaWAN (Włochy),

360920-2025 (ES) — dostawa i instalacja rozwiązania łączności IoT/LoRaWAN (Hiszpania),

245986-2025 (ES) — dostawa wodomierzy oraz modułów zdalnego odczytu LoRaWAN (Hiszpania),

319047-2025 (AT) — dostawa bramek LoRaWAN i akcesoriów (Austria),

457046-2025 (ES) — system LoRaWAN dla potrzeb zarządzania hodowlą (Hiszpania),

310114-2025 (FR) — wymaganie dostępności urządzeń z komunikacją w protokole Radio LoRaWAN (Francja),

227911-2025 (HR) - licencja na sieć LoRaWAN (Chorwacja),

288622-2025 (DE) — zamówienie obejmujące m.in. OMS/LoRaWAN, bramki i dostawę danych pomiarowych (Niemcy).

Dowód pochodzi z oficjalnego źródła — Suplementu do Dziennika Urzędowego Unii Europejskiej (TED), w którym publikowane są ogłoszenia o zamówieniach publicznych obowiązkowo przekazywane przez instytucje i podmioty zamawiające w całej UE.

Wskazane ogłoszenia pokazują, że LoRaWAN jest standardowo wymagane lub dopuszczane w zamówieniach publicznych w wielu państwach członkowskich UE, w różnych sektorach (gospodarka wodna, energetyka, administracja, smart City, rolnictwo).

Materiał ten w sposób obiektywny i urzędowy potwierdza, że LoRaWAN jest rozwiązaniem stosowanym w praktyce zamówień publicznych w Unii i może w pełni odpowiadać uzasadnionym potrzebom zamawiającego, w tym spełniać wymogi OPZ analogiczne do tych określonych przez zamawiającego (tj. dotyczące jakości transmisji, parametrów SLA, bezpieczeństwa i niezawodności).

Pełny materiał dowodowy stanowi zestawienie numerów Suplementu do Dziennika Urzędowego Unii Europejskiej — Tenders Electronic Daily UED)

Informacje o wyborze ofert najkorzystniejszych (pkt 2, 4) — dokumentują kryteria oceny, sposób rozstrzygnięcia postępowań w szczególności dopuszczenie rozwiązań opartych nie na sieciach operatorów komórkowych. W zakresie zdalnego odczytu wodomierzy czy systemów sterowania oświetleniem) były dopuszczane i faktycznie oferowane w postępowaniach.

Wyciągi z Specyfikacji Warunków Zamówienia i OPZ (pkt 4, 6, 7) — wykazują, jakie wymagania techniczne i funkcjonalne zamawiający stawiali w porównywalnych postępowaniach. Jest to kluczowe, aby wykazać, że rozwiązania dopuszczane przez zamawiających w innych postępowaniach obejmowały różne technologie (np. sieci mesh, hybrydowe lub komercyjne), co ma znaczenie dla oceny zgodności oferty w niniejszym postępowaniu z zasadami uczciwej konkurencji oraz równego traktowania wykonawców. Przykładowo, w postępowaniu organizowanym przez Zarząd Dróg Miejskich w Warszawie (sygn. ZDM/UM/DZP/37/PN/15/25), dotyczącym usługi wdrożenia i utrzymania systemu sterowania i zarządzania oświetleniem na terenie m.st. Warszawy, zamawiający wprost dopuścił w opisie przedmiotu zamówienia (pkt 3.5.2) różne rozwiązania sieciowe, tj. mesh, mcsh/hybrida, jak również jednolitą sieć na pasmach komercyjnych.

Postępowania dotyczące systemów wodociągowych, wodomierzy oraz infrastruktury komunalnej (pkt 2—6) są zbliżone przedmiotowo i dowodzą, że rynek dopuszcza różne rozwiązania technologiczne oraz że wybór zamawiających w

przeszłości nie ograniczał konkurencji do jednego typu rozwiązań.

Postępowanie dotyczące oświetlenia w m.st. Warszawa (pkt 7) — potwierdza, że nawet przy innej branży zamawiający dopuszczają alternatywne rozwiązania sieciowe, co świadczy o powszechnym standardzie formułowania wymagań w sposób otwarty i konkurencyjny.

Znaczenie postępowania warszawskiego. Jest to postępowanie szczególnie istotne, ponieważ dotyczyło ono infrastruktury krytycznej — systemu oświetlenia publicznego w stolicy państwa. Oświetlenie uliczne i miejskie stanowi element podstawowego bezpieczeństwa publicznego, mającego bezpośredni wpływ na funkcjonowanie przestrzeni miejskiej, bezpieczeństwo ruchu drogowego oraz porządek publiczny. Jeżeli w tak newralgicznym obszarze zamawiający dopuścił stosowanie technologii opartych na pasmach nielicencjonowanych, to trudno uznać, aby w postępowaniach mniejszej skali, dotyczących infrastruktury wodno-kanalizacyjnej lub lokalnych systemów telemetrycznych, istniały podstawy do kwestionowania takich rozwiązań jako rzekomo niewystarczających czy nieodpowiednich.

Konkurencja i ceny ofert. Warto podkreślić, że w tym postępowaniu oferty złożyli znaczący uczestnicy rynku: Orange Polska S.A., która zaoferowała wykonanie zamówienia za kwotę 173 404 455,36 zł, oraz Emitel S.A., która złożyła ofertę na kwotę 105 104 721,96 zł. Dane te wskazują, że przedmiot zamówienia został potraktowany przez rynek z najwyższą powagą i że nawet największe podmioty telekomunikacyjne, posiadające dostęp do pełnego spektrum technologii, uznały dopuszczone przez zamawiającego rozwiązania, w tym oparte o pasma nielicencjonowane, za w pełni adekwatne i zgodne z wymogami bezpieczeństwa oraz niezawodności.

Praktyka rynkowa i zasady konkurencji. Przywołane postępowanie warszawskie jednoznacznie pokazuje, że na rynku zamówień publicznych przyjęty jest standard dopuszczania różnych technologii komunikacyjnych, w tym sieci działających w pasmach nielicencjonowanych. Dopuszczenie konkurencyjnych technologii pozwala wykonawcom na przedstawienie ofert zróżnicowanych cenowo i funkcjonalnie, co prowadzi do wyboru rozwiązania najbardziej optymalnego z punktu widzenia interesu publicznego.

W odniesieniu do argumentacji zamawiającego zawartej w tabeli zamieszczonej na str. 11 odpowiedzi na odwołanie, mającej rzekomo stanowić porównanie technologii w pasmach licencjonowanych i nielicencjonowanych, odwołujący wskazał, że prezentacja ta ma charakter jednostronny, tendencyjny i nie została poparta żadnym materiałem dowodowym. W szczególności zarzut dotyczący rzekomego braku bezpieczeństwa LoRaWAN jest nieprawdziwy i sprzeczny z dokumentami źródłowymi, w tym publikacjami LoRa Alliance — organizacji rozwijającej i certyfikującej tę technologię. W celu wykazania, że LoRaWAN jest protokołem bezpiecznym, spełniającym najwyższe standardy kryptograficzne oraz regulacyjne, składam następujący wniosek dowodowy:

Wniosek dowodowy nr 9

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu w postaci artykułu „LoRaWAN@ jest bezpieczny (ale implementacja ma znaczenie)” (oryg. „LoRaWAN@ Is Secure (but Implementation Matters)”), opublikowanego przez LoRa Alliance i dostępnego pod adresem: <https://resources.loraalliance.org/security/lorawan-is-secure-but-implementation-matters>, wraz z tłumaczeniem na język polski, na okoliczność:

1/ że protokół LoRaWAN od samego początku został zaprojektowany z bezpieczeństwem jako elementem kluczowym, z obowiązkowym uwierzytelnianiem i szyfrowaniem,

2/ że LoRaWAN implementuje szyfrowanie end-to-end (AES-128), zapewniając integralność i poufność danych w całym łańcuchu komunikacji,

3/ że specyfikacja LoRaWAN definiuje dwie warstwy kryptografii: unikalny 128-bitowy klucz sesji sieciowej oraz unikalny 128-bitowy klucz sesji aplikacyjnej, współdzielone odpowiednio z serwerem sieciowym i aplikacyjnym,

4/ że dzięki dwupoziomowym zabezpieczeniom możliwe jest bezpieczne wdrażanie współdzielonych sieci „multitenant”, w których operator nie ma dostępu do danych użytkowników,

5/ że LoRaWAN dopuszcza różne mechanizmy aktywacji urządzeń, w tym OTAA (Over-The-Air Activation), które pozwala na ponowne ustanawianie sesji kryptograficznych (rekeying),

6/ że LoRa Alliance opracowała dodatkowe mechanizmy zwiększające bezpieczeństwo, takie jak interfejsy backend do izolacji przechowywania kluczy głównych w serwerze join oraz sprzętowo moduły typu secure element,

7/ że bezpieczeństwo LoRaWAN jest stale rozwijane — LoRa Alliance monitoruje zagrożenia, publikuje dokumenty „Recommended Practices” oraz aktualizuje wytyczne, aby technologia pozostawała odporna na zmieniający się krajobraz cyberzagrożeń,

8/ że powyższe jednoznacznie dowodzi, iż LoRaWAN jest technologią bezpieczną, spełniającą wymagania regulacyjne i branżowe, a twierdzenia zamawiającego o „braku bezpieczeństwa” tej technologii są nieprawdziwe i nie znajdują potwierdzenia w dokumentach źródłowych.

Dokument ten stanowi wraz z tłumaczeniem załącznik nr 9 do pisma.

Zamawiający twierdzi, że technologia LoRaWAN jest niebezpieczna, jednocześnie wskazując jako alternatywę

technologie komórkowe NarrowBand IoT (NB-IoT) oraz LTE Cat-M (Cat-M). Odwołujący podkreślił, że każda sieć radiowa — niezależnie od tego, czy działa w paśmie licencjonowanym, czy nielicencjonowanym — zmagają się z podobnymi wyzwaniem i zagrożeniami bezpieczeństwa. NB-IoT i CatM, mimo że są promowane przez zamawiającego jako „bezpieczne” rozwiązania, posiadają udokumentowane podatności tożsame z innymi technologiami radiowymi. Potwierdzają to liczne publikacje naukowe i branżowe, wskazujące na zagrożenia takie jak: - ataki na warstwę danych (data-plane signaling),

-zakłócanie transmisji (jamming), manipulacje bitowe (bit-flipping), - SIM-swapping,

-ataki na urządzenia końcowe IoT (np. smart home, drony), - ogólne podatności typowe dla sieci LPWAN.

Wniosek dowodowy nr 10

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentów w postaci artykułów naukowych opublikowanych na platformie ResearchGate, które wskazują na podatności technologii komórkowych NarrowBand IoT (NB-IoT) oraz LTE Cat-M, na okoliczność wykazania, że:

1/ NB-IoT i LTE Cat-M, podobnie jak LoRaWAN, są narażone na ataki i nie gwarantują pełnego bezpieczeństwa transmisji,

2/ każda technologia radiowa wymaga właściwej implementacji i stosowania mechanizmów ochronnych,

3/ twierdzenia strony przeciwnej, jakoby NB-IoT i Cat-M były wolne od zagrożeń, są nieprawdziwe i nie znajdują potwierdzenia w literaturze.

4/ że technologie NB-IoT oraz CAT-M są wykorzystywane jedynie w 52% aplikacji IoT, Dowody:

„Security threats of NB-IoT and countermeasures” (2020) — artykuł przedstawia główne zagrożenia w NB-IoT i omawia środki zaradcze.

Autorzy: Adam U. Mentsiev oraz Tamirlan R. Magomaev.

[https://www.rcsarcchgate.net/publication/341711539\\_Security\\_threats\\_of\\_NBIoT\\_and\\_countcrmcasurcs\\_Data-plane\\_signaling\\_in\\_cellular\\_IoT:\\_attacks\\_and\\_defense](https://www.rcsarcchgate.net/publication/341711539_Security_threats_of_NBIoT_and_countcrmcasurcs_Data-plane_signaling_in_cellular_IoT:_attacks_and_defense) (2025) — publikacja analizuje ataki na warstwę danych w NB-IoT i Cat-M, wskazując realne scenariusze naruszeń bezpieczeństwa.

Autorzy: Z.T., B.D., J.Z., Y.G. i pozostali (łącznie pięciu autorów).

[https://www.researchgatc.nct/publication/355673884\\_Dataplane\\_signaling\\_in\\_ccllular\\_IoT\\_attacks\\_and\\_defense](https://www.researchgatc.nct/publication/355673884_Dataplane_signaling_in_ccllular_IoT_attacks_and_defense)

Dokumenty te wraz z tłumaczeniami stanowią załącznik nr 10 do pisma.

Wskazane publikacje potwierdzają, że technologie NB-IoT i LTE Cat-M również niosą ze sobą realne zagrożenia bezpieczeństwa, a więc argumentacja strony przeciwnej, jakoby tylko LoRaWAN była narażona na takie zagrożenia, jest nieprawdziwa.

Zamawiający pomija kluczową okoliczność: ekonomika utrzymania systemu opartego na publicznej łączności komórkowej (CAT-M/NB-IoT) w praktyce prowadzi do znacznego wzrostu kosztów operacyjnych, które stają się barierą dla długofalowej eksploatacji systemów zdalnego odczytu.

W przeciwieństwie do technologii LoRaWAN, w której przedsiębiorca komunalny lub telekomunikacyjny może samodzielnie uruchomić i utrzymywać własną, prywatną sieć, w przypadku technologii komórkowych (CAT-M/NB-IoT) nie istnieje realna alternatywa konkurencyjna.

W Polsce jedynym operatorem świadczącym usługę CAT-M jest Orange Polska, co w praktyce oznacza pełne uzależnienie od jednego dostawcy i brak możliwości migracji do innej sieci w razie niezadowolenia z jakości usług czy poziomu opłat.

W przypadku NoB-IoT również dostępność jest ograniczona — poza Polkomtel usługi świadczy T-Mobile, jednak skala i warunki komercyjne nie zapewniają realnej alternatywy konkurencyjnej. Jest to klasyczny przypadek vendor lock-in.

Doświadczenia zagraniczne dowodzą, że przedsiębiorcy komunalni, konfrontowani z zawyżonymi opłatami za transmisję danych w publicznych sieciach komórkowych, podejmują decyzje o migracji do modelu LoRaWAN. Dobitym przykładem jest belgijska spółka CILE (Compagnie Intercommunale Liegeoise des Eaux), która pierwotnie korzystała z usług zdalnego odczytu opartego na publicznej łączności komórkowej. Jednak szacowane koszty na poziomie ponad 3,5 mln EUR rocznie przy ok. 300 000 liczników uczyniły projekt nieopłacalnym. W konsekwencji spółka zbudowała i uruchomiła własną sieć LoRaWAN — obejmującą 24 gminy, ok. 3500 km sieci wodociągowej i opartą na 48 antenach (dowody:

CILE/1-CILE/5).

Model LORaWAN wykazuje przewagę w dwóch wymiarach:

Ekonomicznym — brak opłat abonamentowych dla operatora komórkowego, niższy CAPEX i OPEX oraz długowieczność urządzeń końcowych (bateria nawet do 10 lat).

Organizacyjnym — możliwość pełnej kontroli nad własną siecią, bez ryzyka monopolu jednego dostawcy i bez uzależnienia od komercyjnych warunków operatora.

Co więcej, jeżeli zamawiający spotkałby się z zawyżoną ofertą na usługi LoRaWAN, w każdej chwili mógłby uruchomić i

utrzymywać własną sieć LoRaWAN. Natomiast w przypadku technologii CAT-M lub NB-IoT, w których operatorami są wyłącznie komercyjni dostawcy (w Polsce m.in. Orange/T-Mobile), zamawiający nie ma takiej możliwości — sieci tych nie może samodzielnie zbudować ani eksploatować.

Wniosek dowodowy nr 11

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu w postaci studium przypadku Cisco CILE (Załącznik nr 11), dostępnego również na oficjalnej stronie Cisco pod adresem: <https://www.cisco.com/Site/us/en/about/case-studies-customer-stories/cilc.html>, na okoliczność wykazania, że:

1/ utrzymywanie systemów zdalnego odczytu w modelu publicznej łączności komórkowej (CAT-M/NB-IoT) prowadzi do znacznego wzrostu kosztów operacyjnych, co potwierdza przykład belgijskiej spółki CILE, gdzie koszty transmisji danych w sieci publicznej szacowano na ponad 3,5 mln EUR rocznie przy ok. 300 000 liczników,

2/ przedsiębiorcy komunalni, konfrontowani z zawyżonymi opłatami za transmisję danych, podejmują decyzje o migracji do własnych sieci LoRaWAN, które mogą samodzielnie uruchomić i utrzymywać — CILE wdrożyła własną sieć LoRaWAN opartą o 48 anten, obejmującą 24 gminy i 3500 km sieci wodociągowej,

3/ w odróżnieniu od LoRaWAN, w przypadku technologii komórkowych (CAT-M/NB-IoT) brak jest realnej możliwości migracji do innego operatora w Polsce — usługi CAT-M świadczy wyłącznie Orange Polska, co prowadzi do uzależnienia od jednego dostawcy (vendor lock-in) i braku alternatywy konkurencyjnej,

4/ jeżeli zamawiający spotkałby się z zawyżonymi opłatami w modelu LoRaWAN, mógłby uruchomić i utrzymywać własną sieć, natomiast w modelu CAT-M/NB-IoT nie ma takiej możliwości, gdyż sieci tego rodzaju nie mogą być samodzielnie budowane przez przedsiębiorców komunalnych.

Uzasadnienie - kwestia infrastruktury krytycznej i charakteru zamówienia

Zamawiający, uzasadniając swoje wymagania, powołuje się na szczególny charakter prowadzonej działalności wskazując, że dysponuje infrastrukturą krytyczną, co ma uzasadniać stosowanie wyłącznie technologii komórkowych (NB-IoT/CAT-M). Argumentacja ta jest jednak pozbawiona podstaw prawnych i faktycznych, a ponadto abstrahuje od przedmiotu zamówienia oraz obowiązujących regulacji dotyczących infrastruktury krytycznej.

1. Charakter zamówienia

Po pierwsze, należy jednoznacznie wskazać, że przedmiotem postępowania nie są usługi związane z dostawą wody, ani eksploatacja sieci wodociągowej, lecz usługi i urządzenia telekomunikacyjne, co wynika wprost z klasyfikacji kodów CPV określonych w dokumentacji: 48614000-5 — system pozyskiwania danych,

32260000-3 — urządzenia do przesyłu danych,

51612000-5 — usługi instalowania urządzeń do przetwarzania informacji, 48920000-3 — pakiety oprogramowania do automatyzacji prac biurowych, 80510000-2 — usługi szkolenia specjalistycznego.

Wykonawca ma dostarczyć system telekomunikacyjny wraz z urządzeniami komunikacyjnymi, które służyć będą zdalnym odczytom wodomierzy. Nakładki na wodomierze, wbrew sugestiom zamawiającego, nie stanowią elementu infrastruktury wodociągowej, lecz są urządzeniami telekomunikacyjnymi — elementami systemu transmisji danych, które z punktu widzenia prawa komunikacji elektronicznej należy traktować jako część sieci łączności, a nie jako część sieci wodociągowej są tzw. urządzeniami końcowymi.

2. Infrastruktura krytyczna — definicje i zakres

Po drugie, w świetle art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2020 r. poz. 1856), infrastrukturą krytyczną są „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje i usługi kluczowe dla bezpieczeństwa państwa i jego obywateli (... ) obejmujące m.in. systemy łączności”. Z powyższego jasno wynika, że:

a/ infrastrukturą krytyczną mogą być co do zasady systemy łączności, a więc sieci telekomunikacyjne;

b/ nie sposób uznać, że pojedyncze wodomierze i transmisja danych z nich spełniają ustawowe kryteria infrastruktury krytycznej.

Gdyby przyjąć logikę zamawiającego, zgodnie z którą każdy wodomierz i każda transmisja danych stanowi element infrastruktury krytycznej, wówczas:

a/ całe postępowanie przetargowe musiałoby toczyć się w trybie niejawnym,

b/ dokumentacja powinna być objęta klauzulami bezpieczeństwa,

c/ każdy wodomierz musiałby być fizycznie chroniony jak element strategiczny.

Taka interpretacja prowadzi do oczywistego absurdu, sprzecznego z racjonalnym rozumieniem pojęcia infrastruktury krytycznej.

3. Status odwołującego — Emitel

Po trzecie, należy podkreślić, że to właśnie odwołujący (Emitel S.A.), a nie zamawiający, posiada formalnie faktyczne podstawy do zarządzania i ochrony infrastruktury krytycznej:

1/ Emitel dysponuje infrastrukturą krytyczną w rozumieniu ustawy o zarządzaniu kryzysowym, obejmującą m.in. systemy

łączności zob. Narodowy Program Ochrony Infrastruktury Krytycznej (str. 29) dostępny na [www. Rządowego Centrum Bezpieczeństwa](http://www.RzadowegoCentrumBezpieczenstwa.gov.pl/wpcontent/uploads.pdf) [https://archiwum.rcb.gov.pl/wpcontent/uploads .pdf](https://archiwum.rcb.gov.pl/wpcontent/uploads.pdf) a także

2/ Emitel posiada status podmiotu o szczególnym znaczeniu gospodarczo—obronnym, przyznany na podstawie ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (t.j. Dz.U. z 2020 r. poz. 1669).

3/ Emitel został formalnie wpisany do wykazu podmiotów objętych ochroną na mocy Rozporządzenia Rady Ministrów z dnia 27 grudnia 2023 r., obowiązującego od 1 stycznia 2024 r., które objęło szczególną ochroną m.in. spółki telekomunikacyjne, energetyczne, surowcowe i infrastrukturalne.

Emitel posiada procedury ochrony informacji, systemy rezerwowe oraz wieloletnie doświadczenie w zakresie utrzymania ciągłości działania sieci, co potwierdza jego zdolność do ochrony elementów infrastruktury krytycznej zgodnie z wymaganiami ustawowymi.

W konsekwencji, jeżeli jakkolwiek element sieci telekomunikacyjnej wykorzystywanej w niniejszym zamówieniu miałby zostać zakwalifikowany przez ABW lub BBN do infrastruktury krytycznej, to dysponentem i odpowiedzialnym za ochronę byłby odwołujący — a nie zamawiający.

Wniosek dowodowy nr 12

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu:

1/ opublikowanego na oficjalnej stronie Rzeczypospolitej Polskiej — Ministerstwo Spraw Wewnętrznych i Administracji ([gov.pl](http://gov.pl)) pt.

„Modernizujemy system alarmowy — ponad 4 tys. lokalizacji z nowoczesnymi syrenami”

(<https://www.gov.pl/wcb/obrona-cywilna/modernizujemy-syrenami>)

2/z decyzji Prezesa UKE z dnia 8 lipca 2019 roku potwierdzającego że Emitel jest dysponentem infrastruktury krytycznej i ta jest wyłączona obowiązków zapewnienia dostępu telekomunikacyjnego str. 6 decyzji.

Na okoliczność wykazania, że:

1/ Łączność LoRaWAN została wskazana do wykorzystania w systemie obrony cywilnej Rzeczypospolitej Polskiej, w ramach modernizacji krajowego systemu alarmowego, obejmującego ponad 4 tys. lokalizacji z syrenami alarmowymi, co stanowi infrastrukturę bezpośrednio związaną z bezpieczeństwem i obronnością państwa.

2/ Stanowisko MSWiA potwierdza, że technologia LoRaWAN spełnia wymagania dotyczące niezawodności, bezpieczeństwa i zasięgu, wskazując, że sieć LoRaWAN umożliwia komunikację na dystansie do kilkudziesięciu kilometrów, co gwarantuje skuteczne działanie systemów alarmowych nawet w trudnych warunkach topograficznych.

3/ Skoro LoRaWAN może zostać uznana przez państwo polskie za technologię odpowiednią do zastosowań w obronie cywilnej i ochronie ludności, a więc w obszarze infrastruktury krytycznej o fundamentalnym znaczeniu dla bezpieczeństwa państwa, to tym bardziej może służyć do celów znacznie mniej wymagających, takich jak transmisja danych z wodomierzy tj. podanie ramki z informacją o stanie wodomierza.

4/ Argumentacja zamawiającego, jakoby tylko technologie komórkowe (NB-IoT, CAT-M) gwarantowały odpowiedni poziom bezpieczeństwa i niezawodności, jest sprzeczna ze stanowiskiem polskich władz publicznych (MSWiA), które wprost wdrożyły LoRaWAN w obszarze obronności.

Wydruk z informacji MSWiA stanowi załącznik 11 do pisma.

c/ Brak związku między infrastrukturą krytyczną a proporcją technologii

Podnoszony argument nie wykazuje, że transmisja w technologii komórkowej zapewnia wyższy poziom bezpieczeństwa niż LoRaWAN. Odwołujący, jako operator infrastruktury krytycznej i podmiot o szczególnym znaczeniu gospodarczo-obronnym, ma doświadczenie w zapewnianiu bezpieczeństwa transmisji danych oraz jest w stanie spełnić wymagania SLA oraz wymogi prawne w zakresie cyberbezpieczeństwa niezależnie od tego, czy transmisja będzie realizowana w pasmach licencjonowanych, czy nielicencjonowanych.

Odniesienie do zarzutów w zakresie dyrektywy NIS2 i KSC

Zamawiający powołuje się na przepisy dyrektywy NIS2 oraz Krajowego Systemu Cyberbezpieczeństwa, wskazując, że jako przedsiębiorstwo wodociągowo—kanalizacyjne podlega tym regulacjom, a więc ma prawo wymagać stosowania technologii „przewidywalnej w strukturze zaufania i architekturze zgodnej z NIS”, co — zdaniem zamawiającego — ma uzasadniać wymóg transmisji w technologii komórkowej z dedykowanym APN i tunelem VPN.

Stanowisko to jest błędne i nie znajduje oparcia w treści dyrektywy ani w przepisach krajowych.

A/ Zgodność z NIS2 i KSC — Twierdzenie zamawiającego, że tylko telefonia komórkowa zapewnia zgodność z NIS2 i RSC, jest pozbawione podstaw prawnych i wymuszałoby korzystanie z usług telekomunikacyjnych jedynie przystępujących.

Dodać również należy, że dyrektywa NIS2, nie została jeszcze implementowana do polskiego systemu prawnego. W Polsce proces ten ma nastąpić w drodze nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (RSC). Projekt

ustawy nowelizującej znajduje się w toku prac legislacyjnych, ale do chwili obecnej nie został uchwalony, a tym samym nie obowiązuje.

Z tego względu, w świetle zasady legalizmu (art. 7 Konstytucji RP), organy państwa mogą działać wyłącznie na podstawie i w granicach prawa, zaś na przedsiębiorców mogą być nakładane jedynie te obowiązki, które wynikają wprost z przepisów obowiązującego prawa krajowego. Samo istnienie dyrektywy unijnej, dopóki nie zostanie implementowana, nic rodzi bezpośrednich obowiązków wobec podmiotów prywatnych (z wyjątkiem sytuacji, gdy przepisy dyrektywy byłyby bezwarunkowe i wystarczająco precyzyjne, co w przypadku NIS2 nie zachodzi).

Co więcej, na gruncie aktualnie obowiązującej ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r., przedsiębiorcy telekomunikacyjni zostali *expressis verbis* wyłączeni z katalogu podmiotów objętych RSC. Oznacza to, że w obecnym stanie prawnym przedsiębiorcy telekomunikacyjni nie podlegają reżimowi obowiązków przewidzianych ustawą RSC, w tym w szczególności: obowiązkowi raportowania incydentów, wdrażania systemów zarządzania bezpieczeństwem czy poddawania się audytom. Dopiero planowana nowelizacja ustawy RSC, mająca na celu wdrożenie dyrektywy NIS2, przewiduje włączenie przedsiębiorców telekomunikacyjnych do kręgu podmiotów kluczowych lub ważnych, a tym samym objęcie ich nowymi, szerokimi obowiązkami w zakresie cyberbezpieczeństwa. Do czasu wejścia w życie tych przepisów, przedsiębiorcy telekomunikacyjni w Polsce pozostają poza zakresem obowiązywania RSC.

b/ NIS2 nic narzuca technologii — Dyrektywa (UE) 2022/2555 (NIS2) wskazuje jedynie, że podmioty kluczowe i ważne mają wdrażać odpowiednie i proporcjonalne środki techniczne i organizacyjne, dostosowane do oszacowanego ryzyka. Nigdzie w dyrektywie nie ma mowy o obowiązku stosowania technologii komórkowych, pasm licencjonowanych czy dedykowanego APN. Dyrektywa określa cele (poufność, integralność, dostępność, autentyczność, ciągłość), ale pozostawia wykonawcom dobór środków — właśnie po to, by zapewnić otwartość technologiczną i elastyczność.

c/ Środki organizacyjne narzucenie jednej technologii — obowiązki wskazane przez zamawiającego (monitorowanie, ochrona przed modyfikacją, aktualizacja oprogramowania, reagowanie na incydenty) odnoszą się do zarządzania systemem informacyjnym jako całości, a nie do wyboru pasma radiowego. To oznacza, że zarówno system oparty na technologii komórkowej, jak i system oparty na LoRaWAN może spełniać wymagania NIS2, o ile operator wdroży właściwe procedury i zabezpieczenia. d/ Bezpieczeństwo LoRaWAN — technologia LoRaWAN zapewnia szyfrowanie end-to-end (AES-128), uwierzytelnianie dwustronne i integralność komunikatów, co oznacza, że spełnia podstawowe wymogi poufności, integralności i autentyczności danych. Co więcej, dzięki architekturze prywatnej sieci, zamawiający ma pełną kontrolę nad systemem i jego bezpieczeństwem, w przeciwieństwie do modelu komórkowego, gdzie część bezpieczeństwa zależy od operatora komórkowego.

e/ APN/VPN to tylko jedna z możliwości — zamawiający wskazuje, że dedykowany APN i tunel VPN zapewnia zgodność z NIS. Odwołujący podkreślił, że podobny poziom ochrony można uzyskać w LoRaWAN poprzez szyfrowanie end-to-end, prywatną bramę i dedykowany serwer aplikacyjny w infrastrukturze zamawiającego. NIS2 nie preferuje jednej technologii, lecz wymaga efektu bezpieczeństwa — a efekt ten można osiągnąć zarówno w technologii komórkowej, jak i w LoRaWAN.

f/ Proporcjonalność wymogów — skoro obowiązki NIS2 odnoszą się do efektu (bezpieczna usługa), a nie do sposobu technicznego jego osiągnięcia, to narzucenie jednej konkretnej technologii transmisji jest nieproporcjonalne i sprzeczne z art. 99 ust. 4 ustawy. W szczególności nic wykazano, aby LoRaWAN nie mogła spełnić wymogów NIS2 — przeciwnie, praktyczne wdrożenia w innych krajach UE (np. Francja, Holandia, Hiszpania) dowodzą, że systemy LoRaWAN są stosowane w infrastrukturze krytycznej w zgodzie z wymogami cyberbezpieczeństwa.

g/ Po trzecie, kluczowe znaczenie ma operator sieci.

To właśnie operator, a nie sama technologia radiowa, odpowiada za zapewnienie zgodności z wymaganiami KSC i NIS2. W szczególności do jego obowiązków należy: - wdrożenie redundancji i mechanizmów zapewniających ciągłość działania,

- uruchomienie procedur monitorowania i reagowania na incydenty,

- opracowanie polityk bezpieczeństwa i raportowania, - organizacja procesów zgodnych z KSC i NIS2.

Innymi słowy — to nie pasmo częstotliwości (licencjonowane czy nielicencjonowane) determinuje zgodność z KSC i NIS2, lecz sposób implementacji środków bezpieczeństwa oraz organizacja pracy po stronie operatora sieci.

Takie podejście jest spójne z logiką ustawodawcy unijnego i krajowego, który nakłada obowiązki wprost na operatorów usług kluczowych i operatorów sieci, a nie na producentów sprzętu czy na samą technologię transmisji. W konsekwencji LoRaWAN może być w pełni zgodna z KSC i NIS2 na równi z technologiami komórkowymi.

Odwołujący wskazał, że organizacja LoRa Alliance wprowadziła formalny proces certyfikacji urządzeń końcowych w ramach specyfikacji LoRaWAN 1.0.4. Certyfikacja ta obejmuje szereg testów bezpieczeństwa, w tym obowiązkowe szyfrowanie transmisji algorytmem AES-128, weryfikację integralności komunikacji przy użyciu kodu MIC (AES-CMAC), mechanizmy ochrony przed atakami powtórzeniowymi, kontrolę liczników ramek, testy poprawności procedur aktywacji

OTAA/ABP oraz weryfikację zgodności z regulacjami dotyczącymi ograniczeń emisji radiowej i cyklu pracy.

Dokument „End Device Certification Requirements for LoRaWAN 1.0.4” wraz z tłumaczeniem kluczowych fragmentów dotyczącym bezpieczeństwa stanowi załącznik do niniejszego wniosku i jednoznacznie potwierdza, że urządzenia certyfikowane zgodnie z LoRaWAN 1.0.4 spełniają wyśrubowane kryteria bezpieczeństwa i są uznawane za rozwiązania o bardzo wysokim poziomie ochrony.”

Wniosek dowodowy nr 13

Wnoszę o dopuszczenie i przeprowadzenie dowodu z dokumentu „End Device Certification Requirements for LoRaWAN 1.0.4” wydanego przez organizację LoRa Alliance, wraz z tłumaczeniem na język polski kluczowych fragmentów dotyczących bezpieczeństwa, na okoliczność wykazania, że urządzenia końcowe certyfikowane według tej specyfikacji spełniają najwyższe wymagania bezpieczeństwa w sieciach IoT i są uznawane za urządzenia o bardzo wysokim poziomie zabezpieczeń.

Jako uzasadnienie wniosku wskazał, że proces certyfikacji LoRaWAN 1.0.4 jest wieloetapowy i obejmuje testy weryfikujące poprawność implementacji protokołu, jego odporność na manipulacje oraz zgodność z wymaganiami prawnymi dotyczącymi pracy radiowej. Certyfikacja nie jest formalnością— to zestaw rygorystycznych testów, które mają zapewnić odporność urządzeń końcowych na najczęściej spotykane zagrożenia w systemach IoT, takie jak podsłuch, fałszowanie danych, ataki powtórzeniowe, przeciążenia czy błędy konfiguracyjne. Najważniejsze wymagania bezpieczeństwa:

Poufność i integralność danych

- 1.Obowiązkowe szyfrowanie wszystkich danych aplikacyjnych algorytmem AES-128.
- 2.Oddzielne klucze AppSKey (dla danych aplikacyjnych) i NwkSKey (dla poleceń MAC).
- 3.Każda ramka zawiera kod integralności MIC (AES-CMAC), który chroni przed podsłuchiwaniem, manipulacją i atakami replay.
- 4.Ramki z niepoprawnym MIC są automatycznie odrzucane przez urządzenie. Bezpieczna aktywacja urządzeń
  1. W trybie OTAA testowane są: unikalność parametrów sesji (JoinNonce), poprawna interpretacja ustawień DLSettings, RXDelay i CFList, co eliminuje ryzyko nieautoryzowanego dołączenia do sieci.
  - 2.W trybie ABP wymuszone jest prowadzenie liczników ramek, co chroni przed ponownym użyciem starych pakietów (atak replay).
  - 3.W obu trybach wszystkie ramki muszą być szyfrowane i weryfikowane pod kątem integralności. Bezpieczne zarządzanie parametrami urządzenia (MAC Commands)
    1. DevStatusReq — urządzenie raportuje stan baterii i jakość sygnału w sposób ograniczony i zgodny ze standardem, nie ujawniając dodatkowych informacji mogących zostać wykorzystanych przez atakującego.
    - 2.LinkADRReq — urządzenie musi odróżniać poprawne i niepoprawne żądania zmiany parametrów transmisji (mocy, DataRate, maski kanałów). Żądania wykraczające poza możliwości urządzenia muszą być odrzucane lub obsługiwane w sposób bezpieczny.
    - 3.DutyCycleReq — urządzenie musi stosować ograniczenia cyklu pracy, co zabezpiecza sieć przed przeciążeniem i zapewnia zgodność z przepisami radiowymi.
    - 4.DeviceTimeReq — urządzenie synchronizuje czas z siecią, co eliminuje błędy w oknach odbiorczych i chroni przed manipulacjami czasowymi.

Synchronizacja i niezawodność

1. Urządzenia muszą precyzyjnie otwierać swoje okna odbiorcze RX1 i RX2 w właściwym momencie i na prawidłowych parametrach.
- 2.Testy potwierdzają, że urządzenie potrafi odbierać wiadomości nawet przy zmienionych ustawieniach opóźnień i przepływności.
- 3.To gwarantuje odporność na zakłócenia i manipulacje, które mogłyby odciąć urządzenie od sieci. Ochrona przed przeciążeniem i awariami
  1. Urządzenia muszą odrzucać ramki o zbyt dużym rozmiarze (Oversized Payload), co chroni przed atakami typu buffer overflow i Denial of Service.
  2. Jednocześnie muszą poprawnie obsługiwać ramki o maksymalnym dozwolonym rozmiarze, co potwierdza ich stabilność w warunkach granicznych.

Z powyższej analizy wynika jednoznacznie, że urządzenia certyfikowane zgodnie ze specyfikacją LoRaWAN 1.0.4:

- a) spełniają najwyższe międzynarodowe standardy bezpieczeństwa dla urządzeń IoT, b) gwarantują poufność, integralność i autentyczność transmisji danych,
- c)są odporne na kluczowe zagrożenia cyberbezpieczeństwa: podsłuch, manipulację, ataki powtórzeniowe, błędne konfiguracje oraz przeciążenia,
- d)zapewniają zgodność z regulacjami prawnymi w zakresie pracy radiowej i ochrony pasma,

e) dzięki wbudowanym mechanizmom bezpieczeństwa są uznawane za urządzenia bardzo bezpieczne i godne zaufania w zastosowaniach krytycznych (m.in. w inteligentnych sieciach energetycznych, systemach monitoringu, automatyce przemysłowej).

Wskazany dokument źródłowy wraz z przygotowanym tłumaczeniem fragmentów dotyczących bezpieczeństwa stanowi załącznik nr 16 do pisma stanowi dowód, że proces certyfikacji LoRaWAN jest procedurą restrykcyjną, obejmującą wielopoziomowe testy, które skutecznie eliminują urządzenia niespełniające wymogów bezpieczeństwa.

Dowód ten ma istotne znaczenie dla postępowania, ponieważ obala twierdzenia o braku bezpieczeństwa technologii LoRaWAN i wskazuje, że certyfikacja prowadzona przez LoRa Alliance stanowi realny mechanizm weryfikacji jakości i zgodności urządzeń. Urządzenia te mogą być stosowane w różnorodnych obszarach Internetu Rzeczy, takich jak systemy środowiskowe, gospodarka wodna, logistyka, rolnictwo czy inteligentne miasta, wszędzie tam, gdzie niezbędne są niezawodne i bezpieczne rozwiązania komunikacyjne.

Choć odwołujący domaga się możliwości posłużenia się siecią LoRaWAN w szerszym zakresie, niż dopuścił to zamawiający, to odwołujący nie kwestionuje postanowień wzoru umowy domagając się ich złagodzenia. Gdyby odwołujący obawiał się o np. bezpieczeństwo czy też niezawodność rozwiązania zakładającego zwiększenie udziału technologii LoRaWAN, to składając odwołanie, domagałby się m.in. usunięcia (lub złagodzenia) postanowień dotyczących kar umownych z tytułu odstąpienia od umowy (S8 ust. 1 pkt 1) czy też za brak dostępu do platformy do zdalnego odczytu (S8 ust. 1 pkt 1 I). Brak postawienia takiego zarzutu w odwołaniu dowodzi, że Odwołujący jest pewien, że posłużenie się technologią LoRaWAN w większym niż obecnie przewidzianym zakresie nic narazi odwołującego na sankcje z tytułu kar umownych, odstąpienia, a w dalszej perspektywie — do wykluczenia z innych postępowań.

Niewielki odsetek lokalizacji trudnych — brak uzasadnienia dla wymogu 90% technologii komórkowej zamawiający w uzasadnieniu odpowiedzi na odwołanie posługuje się mapami i tabelami, wskazując na występowanie tzw. „lokalizacji trudnych”, w których transmisja danych miałaby być utrudniona.

Jednocześnie wskazał, że łączna liczba tych lokalizacji wynosi 2 171, podczas gdy przedmiotem zamówienia jest 24 000 nakładek. Oznacza to, że lokalizacje trudne stanowią jedynie ok. 9% całości zamówienia.

Tym samym, nawet przyjmując twierdzenia zamawiającego, że w lokalizacjach trudnych konieczne jest zastosowanie transmisji w technologii komórkowej, to wynika z tego wprost, że:

1/ w 9% lokalizacji można zastosować technologię komórkową,

2/ w pozostałych 91% nie ma przeszkód, aby zastosować transmisję LoRaWAN.

Zestawienie to w oczywisty sposób podważa zasadność wymogu, aby 90%) wszystkich transmisji realizowanych było w technologii komórkowej. Sam Zamawiający przyznaje bowiem, że problem występuje jedynie w ograniczonej liczbie lokalizacji, a więc proporcja powinna być odwrotna do przyjętej w SWZ - komórkowa w 9%, LoRaWAN w 91%.

Przyjęty przez zamawiającego wymóg 90/10 nie ma żadnego związku z faktycznymi potrzebami, które wynikają z przedstawionych danych liczbowych. Jest to konstrukcja całkowicie arbitralna, nieproporcjonalna i sprzeczna z art. 99 ust. 4 PZP, gdyż wprowadza ograniczenie konkurencji na podstawie kryteriów, które nic odpowiadają realnemu rozkładowi lokalizacji trudnych.

Brak wyjątkowości warunków zabudowy w Katowicach — doświadczenia Wrocławia

Zamawiający wskazuje na charakterystykę urbanistyczną Katowic, powołując się na występowanie XIX- i XX-wiecznych kamienic, bloków powojennych, osiedli robotniczych, wysokich bloków z wielkiej płyty, a także nowoczesnych osiedli i zabudowy jednorodzinnej. Na tej podstawie stara się wykazać konieczność zastosowania technologii komórkowej do transmisji danych.

Argumentacja ta jest chybiona, ponieważ taka struktura zabudowy nie jest w żaden sposób unikatowa dla Katowic. Analogiczne warunki urbanistyczne występują we Wrocławiu, gdzie Odwołujący z powodzeniem zrealizował wdrożenie systemu LoRaWAN, które działa stabilnie i spełnia wymagania SLA.

Śródmieście Wrocławia (Stare Miasto, Nadodrze, Ołbin) — gęsta zabudowa kamieniczna z XIX i XX w., o grubych murach i wysokich kondygnacjach, porównywalna do katowickiego Śródmieścia, Koszutki czy Załęża.

Nowy Dwór, Gądów Mały — wysokie bloki mieszkalne z lat 80. i 90., analogiczne do bloków wielopłytowych w dzielnicach Katowic takich jak Giszowiec czy Ligota.

Krzyki, Ołtaszyn, Psie Pole — mieszana zabudowa jednorodzinna i nowe osiedla apartamentowe, odpowiadające charakterem takim dzielnicom Katowic jak Kostuchna, Podlesie czy Piotrowice. Muchobór Wielki, Zerniki, Brochów, Klecina — rozległe tereny przemysłowe i logistyczne, z halami stalowymi i dużymi obiektami magazynowymi, które stanowią odpowiednik katowickich obszarów przemysłowych w Załężu, Szopienicach-Burowcu czy Dąbrówce Małej.

We wszystkich tych obszarach, mimo zróżnicowanych i często trudnych warunków transmisyjnych, system LoRaWAN wdrożony przez odwołującego działa prawidłowo i zapewnia wymagany poziom SLA.

Zamawiający wskazuje na specyfikę urbanistyczną Katowic — obecność zabudowy kamienicznej, bloków wielopłytowych, osiedli robotniczych i nowych inwestycji — jako argument na rzecz stosowania wyłącznie technologii

komórkowej do transmisji danych.

Argument ten jest chybiony, gdyż analogiczne, a nawet trudniejsze warunki transmisyjne występują we Wrocławiu, gdzie odwołujący z powodzeniem wdrożył system LoRaWAN, który działa stabilnie i spełnia wymagania SLA.

Skala zabudowy: Wrocław ma ponad dwukrotnie większą populację od Katowic (672 882 wobec 278 885 mieszkańców) i wyższą gęstość zaludnienia (2 298 os./km<sup>2</sup> wobec 1 693 os./km<sup>2</sup> — GUS 2024). To oznacza większą liczbę budynków, większe zagęszczenie konstrukcji i potencjalnie trudniejsze warunki propagacji radiowej.

Zabudowa śródmiejska: We Wrocławiu występuje rozległe Śródmieście (Stare Miasto, Nadodrze, Olbin) z gęstą zabudową kamieniczną o grubych murach i wysokich kondygnacjach — porównywalną, a miejscami bardziej zwartą niż w Katowicach (Śródmieście, Koszutka, Załęże).

Zabudowa wielokondygnacyjna: Wrocław posiada liczne osiedla wysokich bloków (Nowy Dwór, Gądów Mały), odpowiadające katowickim Giszowcowi czy Ligocie, ale w większej skali.

Zabudowa mieszkaniowa i przemysłowa: Mieszana struktura jednorodzinnych domów, nowych apartamentowców i hal przemysłowo-logistycznych występuje zarówno w Katowicach, jak i we Wrocławiu. Jednak rozległość terenów przemysłowych i gęstość zabudowy logistycznej we Wrocławiu (Muchobór Wielki, Brochów, Klecina) jest większa niż w Katowicach.

W praktyce oznacza to, że to właśnie Wrocław stanowi bardziej wymagające środowisko radiowe — ze względu na większą liczbę budynków, wyższą gęstość zabudowy i większą populację.

Mimo tych trudniejszych warunków odwołujący z sukcesem zrealizował tam wdrożenie LoRaWAN, które działa stabilnie i zapewnia wymagany poziom SLA. W konsekwencji, jeżeli sieć LoRaWAN sprawdza się w gęstszym i trudniejszym środowisku Wrocławia, to tym bardziej może zostać skutecznie wdrożona w Katowicach.

Wniosek dowodowy nr 14

Wniósł o dopuszczenie i przeprowadzenie dowodu z

1/ dokumentu pt. Dane Głównego Urzędu Statystycznego (GUS) za 2024 r., Załącznik „Powierzchnia i ludność w przekroju terytorialnym w 2024 roku — tablice”, arkusz Tabl. 2. Powierzchnia, ludność oraz lokaty według powiatów i miast na prawach powiatu.

3.zdjęć zalanych studni wykonanych na terenie miasta Wrocławia

Na okoliczność że

1/ Wrocław: powierzchnia 293 km<sup>2</sup>, ludność 673 743 mieszkańców, gęstość zaludnienia 2 301 os./km<sup>2</sup>

2/ Katowice: powierzchnia 165 km<sup>2</sup>, ludność 279 190 mieszkańców, gęstość zaludnienia 1 695 os./km<sup>2</sup>. Powołany wniosek wskazuje wyraźnie że warunki urbanistyczne i transmisyjne we Wrocławiu są istotnie trudniejsze niż w Katowicach z uwagi na: 1 / ponad dwukrotnie większą populację,

2/ wyższą gęstość zaludnienia,

3/ większą powierzchnię i większą liczbę budynków.

Jednocześnie prezentowane zdjęcia zalanych studni wodociągowych na terenie Wrocławia wskazują:

1/ że w praktyce eksploatacyjnej studnie wodociągowe często ulegają okresowemu zalewaniu wodą, 2/ że w takich sytuacjach stosuje się standardowe rozwiązania techniczne polegające na montażu anten w sposób uwzględniający ryzyko zalewania (np. anteny wyniesione, anteny zewnętrzne, specjalne mocowania) ,

3/ a tym samym, że istnienie zjawiska zalewania studni nie stanowi przeszkody w skutecznym funkcjonowaniu systemów odczytowych opartych na technologii LoRaWAN, co znajduje potwierdzenie w praktyce inżynierskiej i wdrożeniach w innych dużych miastach.

Odwołujący z powodzeniem zrealizował we Wrocławiu wdrożenie systemu LoRaWAN, który działa stabilnie i spełnia wymagania SLA. Oznacza to, że tym bardziej możliwe i zasadne jest jego skuteczne wdrożenie w Katowicach, gdzie warunki urbanistyczne są mniej wymagające.

Dowód w postaci zdjęć zalanych studni z Wrocławia obrazuje realne i typowe warunki eksploatacyjne dla infrastruktury wodociągowej w dużych miastach. Zjawisko okresowego zalewania studni wodociągowych nie jest szczególną cechą Katowic, lecz powszechną sytuacją spotykaną w wielu aglomeracjach, w tym we Wrocławiu. W branży wodociągowej wypracowane są standardowe i sprawdzone praktyki instalacyjne, które w pełni neutralizują skutki tego zjawiska — w szczególności poprzez odpowiedni montaż anten i elementów transmisyjnych w lokalizacjach narażonych na wodę.

Materiał fotograficzny potwierdza, że ryzyko zalewania jest normalnym czynnikiem środowiskowym, który nie dyskwalifikuje zastosowania technologii radiowych (np. LoRaWAN) w systemach odczytowych. Przeciwnie — pokazuje, że w takich przypadkach stosuje się rozwiązania techniczne, które zapewniają zachowanie wymaganych parametrów SLA. Dowód ten obala twierdzenia Zamawiającego, jakoby sam fakt zalewania studni stanowił przeszkodę dla niezawodnej transmisji danych.

Odpowiedź na argument o topografii i zabudowie Katowic

Zamawiający w uzasadnieniu powołuje się na szczególne uwarunkowania Katowic — zróżnicowaną topografię (różnice

wysokości 100—120 m, doliny Rawy i Kłodnicy, wzniesienia leśne), zwartą zabudowę historyczną (kamienice, familoki) czy bloki wielkopłytowe. Wskazuje, że te warunki ograniczają propagację fal radiowych i uzasadniają ograniczenie technologii LoRaWAN do maksymalnie 10%) lokalizacji.

Ta argumentacja nie jest przekonująca z następujących powodów: a/ Problemy propagacyjne dotyczą każdej technologii. Sam zamawiający przyznał, że nawet NB-IoT i LTE-M (technologie komórkowe w paśmie licencjonowanym) mogą napotykać problemy z zasięgiem w dolinach, piwnicach czy przy grubych murach. Oznacza to, że żadna technologia nie eliminuje trudnych lokalizacji. Rozwiązaniem jest właściwy projekt sieci — dobór odpowiednich punktów bazowych, anten zewnętrznych, retransmiterów — a nie arbitralne narzucenie proporcji 90/10.

b/ Uwarunkowania Katowic nie są wyjątkowe

Zróżnicowana zabudowa historyczna i przemysłowa, bloki wielkopłytowe czy tereny obniżeń występują w każdym dużym mieście w Polsce — np. we Wrocławiu, Krakowie, Łodzi. Odwołujący wykazał, że w takich samych warunkach (Śródmieście i Nadodrze we Wrocławiu — gęsta zabudowa kamieniczna, Muchobór Wielki i Brochów — tereny przemysłowe) system LoRaWAN działa skutecznie i spełnia wymagania SLA. Katowice nie stanowią tu żadnego wyjątku.

c/ Projekt sieci = gwarancja działania

To nie wybór pasma, lecz poprawny projekt sieci decyduje o niezawodności. W lokalizacjach trudnych stosuje się anteny zewnętrzne, repeatery, odpowiednią gęstość bram LoRaWAN czy konfigurację ADR. Podobnie operatorzy komórkowi budują dodatkowe stacje bazowe tam, gdzie sygnał jest słaby. Wniosek jest oczywisty: prawidłowo zaprojektowana sieć gwarantuje pokrycie, niezależnie od wybranej technologii.

d/ Dane Zamawiającego wskazują na coś odwrotnego

Sam zamawiający podał, że tzw. trudne lokalizacje stanowią 2171 z 24 000 punktów, czyli ok. 9% całości. Skoro więc trudne przypadki to realnie tylko 9%, logiczne i proporcjonalne byłoby przyjęcie odwrotnej proporcji — technologii komórkowej w trudnych 9% lokalizacji, LoRaWAN w pozostałych 91%. Narzucona proporcja 90/10 jest sprzeczna z danymi, które zamawiający sam przedstawił.

c/ Brak dowodu na poparcie twierdzeń

Zamawiający ograniczył się do ogólnego opisu terenu i zabudowy. Nie przedstawił żadnych pomiarów propagacyjnych, analiz radiowych ani badań wykazujących, że LoRaWAN nie zapewnia wymaganego SLA w Katowicach. Tymczasem odwołujący przeprowadził badania zajętości pasma i wykazał, że LoRaWAN działa w Katowicach stabilnie. Brak dowodów po stronie zamawiającego oznacza, że jego stanowisko ma charakter czysto teoretyczny. Odwołujący natomiast wykonał profesjonalny projekt techniczny sieci telekomunikacyjnej w specjalistycznym oprogramowaniu komputerowym.

Wniosek dowodowy nr 15 — Profesjonalny projekt sieci LoRaWAN

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentu w

1/ postaci „Projekt techniczny sieci telekomunikacyjnej LoRaWAN opracowany przez odwołującego, wykonany w profesjonalnym oprogramowaniu do planowania radiowego przez specjalistów z zakresu telekomunikacji.

2/ artykułu naukowego pt. „LoRaWAN Network: Radio Propagation Models and Performance Evaluation in Various Environments in Lebanon” (IEEE Internet of Things Journal, DOI:

10.1109/JIOT.2019.2906838) — wraz z tłumaczeniem na język polski.

Treść dowodu:

Odwołujący przygotował szczegółowy projekt sieci LoRaWAN dla obszaru Katowic.

W analizach propagacyjnych uwzględniono:

— numeryczny model terenu (DTM) zawierający informację o ukształtowaniu terenu np. dolinach, wzniesieniach, cyfrowy model zabudowy (dane o wysokości i typach zabudowy np. zabudowa przemysłowa, wieżowce, gęsta zabudowa miejska, tereny podmiejskie, obszary wiejskie, lasy),

-model propagacji fal radiowych Volcano opracowany i rekomendowany dla łączności IoT przez producenta oprogramowania firmę SIRADEL bazujący na modelu Śledzenia promieni „3D Ray-Tracing” oraz z wykorzystaniem innych modeli propagacyjnych COST-231, ITU-R P. 1812),

— symulacje propagacji w środowisku zurbanizowanym,

-czułość odbiorników do -120 dBm, margines tłumienia 10 dB,

— parametry pracy LoRaWAN (SF7—SF12, BW 125).

Planowanie infrastruktury: lokalizacje bram (gateway), optymalizacja wysokości i kierunków anten,

— redundancja pokrycia w „trudnych” lokalizacjach.

Konfiguracja i pojemność sieci:

— mechanizm ADR (Adaptive Data Rate), analiza obciążenia kanałów i rozkładu urządzeń, zapewnienie rezerwy >300/0 pojemności.

Testy i optymalizacja:

— kampanie pomiarowe drive-test/walk-test (RSSI, SNR, PER), testy w piwnicach i obszarach dolinnych, korekta map pokrycia i parametrów radiowych.

Środki dla lokalizacji trudnych:

- stosowanie anten zewnętrznych,
- możliwość zagęszczenia bram
- indywidualne profilowanie urządzeń w trudniejszych punktach.

Utrzymanie i monitoring:

- bieżący monitoring SLA (PER, DEL, dostępność),
- cykliczne analizy zajętości pasma, procedury optymalizacji i reagowania na zdarzenia sieciowe.

Przedstawiony projekt dowodzi, że odwołujący nie ogranicza się do teoretycznych deklaracji, lecz stosuje pełną metodykę inżynierską, identyczną jak w planowaniu profesjonalnych sieci komórkowych. Oznacza to, że system LoRaWAN w Katowicach został zaprojektowany tak, aby spełnić wymagania SLA w każdych warunkach terenowych i urbanistycznych.

Wniosek o utajnienie

Na podstawie art. 545 ust. 3 ustawy wniósł o utajnienie niniejszego dowodu („Załącznik 15 Projekt techniczny sieci telekomunikacyjnej LoRaWAN) przed innymi uczestnikami postępowania odwoławczego, z wyjątkiem zamawiającego oraz Krajowej Izby Odwoławczej z uwagi na okoliczność, że informacje w ww. dokumencie stanowią tajemnicę przedsiębiorstwa Emitel w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Dokument zawiera bowiem szczegółowe dane techniczne oraz technologiczne naszego przedsiębiorstwa, a ich ujawnienie mogłoby narazić Emitel na szkodę. Oświadczył, że Informacje, zarówno jako całość, jak i w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji oraz nie są łatwo dostępne dla takich osób

Wniosek dowodowy nr 16 — Profesjonalny projekt sieci LoRaWAN

Wnoszę o dopuszczenie i przeprowadzenie dowodu z dokumentu w artykule naukowego pt. „LoRaWAN Network: Radio Propagation Models and Performance Evaluation in Various Environments in Lebanon” (IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2019.2906838) — wraz z tłumaczeniem na język polski.

Jednocześnie przedstawiany artykuł wskazuje, że:

1/ Technologia LoRaWAN zapewnia stabilną i niezawodną transmisję danych w różnych środowiskach (miejskich, podmiejskich, wiejskich i wewnętrznych),.

2/ LoRaWAN spełnia wymagania jakościowe i wydajnościowe dla systemów IoT, w tym w zakresie niezawodności transmisji, co podważa twierdzenia Zamawiającego o jej rzekomej niestabilności i braku skalowalności.

3/ Wyniki badań naukowych wprost potwierdzają, że LoRaWAN jest technologią powszechnie stosowaną w projektach typu smart City i smart metering, co czyni ją pełnoprawną alternatywą dla technologii komórkowych.

Dokument ten z tłumaczeniem stanowi załącznik nr 16 do pisma.

Brak rzetelnej analizy zasięgu sieci komórkowej po stronie zamawiającego

Co więcej, gdyby zamawiający faktycznie przeprowadził rzetelną analizę warunków propagacyjnych i jakości transmisji w Katowicach, to powinien był wprost wskazać, gdzie jego zdaniem występuje brak zasięgu sieci komórkowych.

Tymczasem w dokumentacji postępowania nie ma żadnej informacji ani mapy zasięgu, która wskazywałaby, w jakich dzielnicach lub lokalizacjach występują problemy z dostępnością sieci komórkowej. W praktyce wiedzę o realnych niedostatkach w zasięgu sieci komórkowej mają jedynie sami operatorzy komórkowi, co powoduje, że to oni — a nie pozostali wykonawcy — są w stanie lepiej zaplanować sieć i uwzględnić słabsze punkty infrastruktury.

W konsekwencji rodzi się pytanie: jak zamawiający zamierza planować to zamówienie, skoro sam nic dysponuje ani nie przedstawił żadnych danych o faktycznych brakach zasięgu technologii komórkowej? Skoro takie informacje posiadają wyłącznie operatorzy komórkowi, to narzucona proporcja 90/10 prowadzi do sytuacji, w której podmioty powiązane z tymi operatorami uzyskują nieuzasadnioną przewagę informacyjną, przekładającą się na przewagę konkurencyjną nad pozostałymi uczestnikami postępowania.

Taka przewaga może być zniwelowana jedynie poprzez usunięcie sztucznych wymogów 90/10.

Takie działanie prowadzi do faktycznego uprzywilejowania określonej grupy wykonawców i ograniczenia konkurencji, co jest sprzeczne z art. 16 ust. 1 i 3 oraz art. 99 ust. 4 ustawy.

Odpowiedź na argument o „racjonalnym środku proporcjonalnym do celu”

Zamawiający twierdzi, że narzucenie proporcji 90% sieci komórkowej / 10% LoRaWAN nic jest kaprysem ani preferowaniem określonych wykonawców, lecz „racjonalnym środkiem proporcjonalnym do założonych celów”.

Twierdzenie to nie znajduje jednak potwierdzenia w faktach:

a/ Brak proporcjonalności

Proporcjonalność oznacza dostosowanie wymogów do faktycznych potrzeb. Dane samego zamawiającego wskazują, że tzw. lokalizacje trudne to 2 171 z 24 000 punktów, czyli ok. 9% całości. Skoro więc jedynie lokalizacji wymagało by teoretycznie instalacji komórkowych, to arbitralne narzucenie 900/0 sieci komórkowe i tylko 10% LoRaWAN nie jest proporcjonalne — lecz odwrotne do rzeczywistych potrzeb.

b/ Rynek nie jest równy dla wszystkich

Zamawiający powołuje się na fakt, że kilku operatorów (F-Mobile, Orange, Plus) oferuje NB-IoT i LTE-M, a moduły produkuje wielu producentów. Jednak w praktyce tylko operatorzy komórkowi posiadają wiedzę o rzeczywistych brakach zasięgu i możliwość elastycznego planowania sieci. Integratorzy i inni wykonawcy pozbawieni są dostępu do tych danych, co w oczywisty sposób faworyzuje podmioty powiązane z operatorami komórkowymi. To zaś prowadzi do ograniczenia konkurencji. Integratorzy też nie mają instrumentów by zmusić operatora komórkowego do udostępnienia mu pewnych konfiguracji sieci komórkowych a które są wymagane w postępowaniu i które są kwestionowane jak dedykowana podsieć APN wydzielona logicznie od publicznego Internetu. Możliwości wykorzystania technologii komórkowej dla odwołującego zawężają się do możliwości zakupu karty sim od operatora komórkowego przez skorzystanie z jego ogólnodostępnej oferty.

c/ Alternatywne technologie są stabilne i efektywne

Zamawiający deprecjonuje alternatywne technologie jako „pozornie tańsze”. Tymczasem doświadczenia z wdrożeń LoRaWAN we Wrocławiu i innych miastach pokazują, że systemy te działają stabilnie i spełniają wymagania SLA. Co więcej, dzięki niższym kosztom eksploatacji, braku opłat abonamentowych i dłuższej żywotności baterii, całkowity koszt UCO) takich systemów jest niższy niż w przypadku sieci komórkowej.

d/ Wymogi OPZ są „technologicznie neutralne”?

OPZ i SWZ określają wymagania SLA (np. 90% dziennie, 95 % tygodniowo, 98% miesięcznie), które odnoszą się do efektu, a nie do sposobu technicznego jego zrealizowania

Skoro odwołujący wykazał, że LoRaWAN spełnia te wymagania, to zamawiający nie może arbitralnie narzucać preferencji dla sieci komórkowej, zwłaszcza bez przedstawienia rzetelnych dowodów.

Odpowiedź na argument o „braku ograniczenia konkurencji”

Zamawiający podnosi, że nic narzuca konkretnej marki ani producenta, lecz jedynie wymóg skuteczności i niezawodności, które — w jego ocenie — mogą być zapewnione przede wszystkim przez systemy działające w paśmie licencjonowanym. Wskazuje również, że na rynku działa kilku operatorów komórkowych, a więc nic może być mowy o ograniczeniu konkurencji, gdyż odwołujący mógłby zawrzeć z nimi umowę i uzyskać dostęp do częstotliwości.

Ta argumentacja jest jednak błędna z następujących powodów:

I/ De facto narzucenie infrastruktury

Choć zamawiający twierdzi, że nie narzuca producenta ani marki, to w rzeczywistości narzuca wykonawcom konieczność korzystania z infrastruktury operatorów komórkowych. Tylko oni posiadają rezerwacje częstotliwości, kontrolują dostęp do pasma i mają wiedzę o realnym zasięgu swoich sieci oraz mogą udostępnić pewne konfiguracje sieci postawione w wymaganiach. Oznacza to, że inni wykonawcy, którzy nie są operatorami komórkowymi, muszą działać w zależności od nich, a więc tracą niezależność i stają się faktycznie podwykonawcami.

2/ Nierówne traktowanie wykonawców

Operatorzy komórkowi są w uprzywilejowanej pozycji — dysponują własną siecią, znają jej niedostatki, mogą tym samym efektywniej planować wdrożenie. Wykonawcy niezależni takich danych nie mają i musieliby je nabywać od operatorów na nieznanych i jednostronnie narzuconych warunkach. To nie jest równe traktowanie podmiotów — przeciwnie, to systemowe ograniczenie konkurencji, bo wyklucza integratorów i podmioty posiadające własne rozwiązania alternatywne (np. LoRaWAN).

3/ Teoretyczność powołania się na art. 96 PKE

Zamawiający powołuje się na art. 96 ustawy Prawo komunikacji elektronicznej, wskazując, że operator może „wydzierżawić częstotliwość” innemu podmiotowi. W praktyce jednak takie sytuacje są skrajnie rzadkie i dotyczą współpracy strategicznej między operatorami, spółkami operatorskimi w ramach jednej grupy kapitałowej a nie udostępniania częstotliwości podmiotom zewnętrznym, które miałyby z nimi konkurować. Nie istnieje żaden przykład, by operator komórkowy wydzierżawił rezerwację częstotliwości integratorowi systemu odczytowego celem oferowania usług spółce wodociągowej — jest to czysto teoretyczna możliwość, która nie ma żadnego przełożenia na praktykę rynkową. 4/ Rynek nie jest otwarty

Twierdzenie, że rynek nie jest zamknięty, ponieważ działa na nim czterech operatorów komórkowych, jest niepełne i wprowadzające w błąd. Rynek jest w rzeczywistości zamknięty właśnie dlatego, że jedynie ci operatorzy mają bezpośredni i wyłączny dostęp do pasma radiowego oraz realną możliwość swobodnego dysponowania nim. Oznacza to, że wszyscy pozostali wykonawcy — integratorzy, producenci urządzeń, dostawcy alternatywnych rozwiązań — są z tego rynku wykluczeni lub skazani na pośrednie działanie w oparciu o zależność od operatora komórkowego. Taka

konstrukcja wymagań prowadzi do powstania asymetrii informacyjnej i przewagi konkurencyjnej operatorów, którzy jako jedyni dysponują wiedzą o rzeczywistym pokryciu zasięgiem i mogą elastycznie kształtować konfigurację własnych sieci. Tymczasem odwołujący podkreślił, że istnieją inni przedsiębiorcy, którzy mogliby dostarczyć zamawiającemu usługę na wymaganym poziomie jakości (SLA), wykorzystując technologie alternatywne wobec komórkowych, takie jak LoRaWAN czy inne rozwiązania LPWAN. Wdrożenia zrealizowane w innych dużych miastach (m.in. Wrocław) potwierdzają, że przy prawidłowo zaprojektowanej sieci możliwe jest osiągnięcie tego samego poziomu niezawodności i dostępności usługi, jakiego oczekuje zamawiający.

W świetle art. 99 ust. 4 ustawy zamawiający nie może formułować wymagań w sposób, który de facto ogranicza rynek do wąskiej grupy podmiotów. Wymóg oparty wyłącznie o technologie kontrolowane przez czterech operatorów komórkowych prowadzi do sytuacji, w której konkurencja zostaje sztucznie ograniczona, a inni wykonawcy, mimo posiadania kompetencji i technologii zdolnych zapewnić wymagane SLA, zostają z udziału w postępowaniu wykluczeni.

W efekcie powstaje ryzyko naruszenia podstawowych zasad prawa zamówień publicznych — w szczególności zasady uczciwej konkurencji, równego traktowania wykonawców oraz proporcjonalności — co wprost podważa legalność postępowania w obecnym kształcie.

Odpowiedź na argument o SLA i przewadze technologii komórkowej

Zamawiający wskazał, że choć OPZ określa jednolite progi SLA (90% dziennie, 95% tygodniowo, 98% miesięcznie), to w jego ocenie tylko technologie komórkowe (NB-IoT, LTE-M) realnie umożliwiają ich osiągnięcie. Jako uzasadnienie podaje ograniczenia LoRaWAN w paśmie nielicencjonowanym (duty-cycle, brak QoS, ryzyko interferencji).

Stanowisko to jest błędne z kilku powodów:

a/ Neutralność OPZ

OPZ sformułował wymagania jakości w sposób technologicznie neutralny — wykonawca ma zapewnić określone progi SLA, bez wskazania, że mogą one być zrealizowane tylko przez jedną technologię. Skoro tak, to każdy wykonawca, niezależnie od technologii, musi udowodnić, że jest w stanie spełnić SLA. Twierdzenie zamawiającego, że tylko operator komórkowy jest w stanie je zrealizować, to próba dorobienia uzasadnienia ex post, które nic znajduje oparcia w dokumentacji przetargowej. b/ LoRaWAN spełnia wymagania SLA

LoRaWAN zapewnia spełnienie progów SLA dzięki:

- mechanizmom retransmisji i adaptacji przepływności (ADR),
- rozproszonemu widmu (spread spectrum) zwiększającemu odporność na zakłócenia,
- szyfrowaniu AES-128 end-to-end zapewniającemu bezpieczeństwo transmisji,
- redundancji ramek — pojedyncza wiadomość może być odebrana przez kilka stacji bazowych, co zwiększa niezawodność,
- dłuższej żywotności baterii — co minimalizuje awaryjność urządzeń i konieczność interwencji serwisowych.

Praktyka dowodzi, że sieci LoRaWAN z powodzeniem działają w wielu miastach europejskich

(Amsterdam, Paryż, Barcelona) i w Polsce (Wrocław), spełniając SLA w środowiskach równie trudnych jak Katowice.

c/ Argumenty o „ograniczeniach LoRaWAN” są przesadne

-Duty-cycle 1/0/0 — to ograniczenie dotyczy pojedynczego urządzenia, które i tak wysyła bardzo niewielką ilość danych (kilka kilobajtów dziennie). odczytach wodomierzy nie stanowi to żadnego ograniczenia.

-Brak QoS — LoRaWAN nie potrzebuje QoS w rozumieniu GSM, bo protokół jest zoptymalizowany do transmisji krótkich, sporadycznych danych (typowych dla odczytów liczników).

Zakłócenia i interferencja — LoRaWAN dzięki mechanizmowi „diversity reception” (odbiór tej samej ramki przez wiele ramek) i retransmisjom zapewnia stabilność transmisji nawet w gęstych środowiskach miejskich.

-NB-IoT lub CAT-M także nie jest wolny od problemów

Zamawiający pomija, że również technologie komórkowe napotykają ograniczenia: brak zasięgu w piwnicach i dolinach, uzależnienie od operatora i jego inwestycji, ograniczenia czasowe rezerwacji częstotliwości. NB-IoT lub CAT-M nie daje absolutnej gwarancji spełnienia SLA — wymaga rozbudowy infrastruktury i działa w określonym horyzoncie czasowym (do wygaśnięcia rezerwacji). Sam zamawiający przewidział że 10% nakładek w technologii komórkowej nie będzie pracować.

Argument o art. 96 PKE — czysto teoretyczny, nigdy niewykorzystany

Zamawiający powołuje się na art. 96 ustawy Prawo komunikacji elektronicznej, zgodnie z którym podmiot dysponujący rezerwacją częstotliwości może wydzierżawić lub przekazać do użytkowania częstotliwości objęte rezerwacją innemu podmiotowi. Na tej podstawie twierdzi, że Odwołujący mógłby uzyskać dostęp do pasma licencjonowanego poprzez zawarcie umowy cywilnoprawnej z operatorem komórkowym. Argument ten jest jednak całkowicie pozorny i nie znajduje odzwierciedlenia w praktyce:

a/ Brak przykładów w praktyce zamówień publicznych

Zamawiający nie wskazał ani jednego przypadku w historii zamówień publicznych w Polsce, w którym którykolwiek z

operatorów komórkowych wydzierżawiłby częstotliwości innemu podmiotowi na potrzeby realizacji zdalnego odczytu wodomierzy (ani żadnego innego systemu IoT dla infrastruktury komunalnej). Takie przypadki nigdy nie występowały, co podważa realność powoływania się na art. 96 PKE w tym kontekście.

b/ Częstotliwości to dobro rzadkie i kosztowne

Częstotliwości radiowe są dobrem rzadkim, rozdysponowanym w drodze aukcji, w których operatorzy komórkowi płacą setki milionów złotych za uzyskanie rezerwacji. Z ekonomicznego punktu widzenia operatorzy nie mają interesu w tym, by odpłatnie lub nieodpłatnie udostępniać swoje częstotliwości konkurentom, skoro stanowią one strategiczne źródło przewagi rynkowej. c/ Możliwość prawna realna dostępność rynkowa

Fakt, że przepisy prawa dopuszczają dzierżawę częstotliwości, nie oznacza, że taka praktyka istnieje na rynku. Zamawiający powinien wykazać, że dostęp do częstotliwości licencjonowanych jest realny i powszechnie dostępny dla wszystkich wykonawców. Skoro tego nie zrobił, a praktyka pokazuje, że operatorzy nigdy nie dzierżawią częstotliwości w takich przypadkach, to argument należy uznać za czysto teoretyczny.

d/ Paradoks wymagań OPZ

Paradoks wymagań określonych w OPZ polega na tym, że zamawiający domaga się, aby transmisje z urządzeń końcowych (nakładek) do stacji bazowych odbywały się wyłącznie w pasmach licencjonowanych, podczas gdy w praktyce rynkowej znaczna część transmisji pomiędzy samymi stacjami bazowymi operatorów komórkowych realizowana jest w pasmach nielicencjonowanych. Operatorzy powszechnie korzystają z technologii radiolinii, systemów dosyłowych czy backhaufu w paśmie nielicencjonowanym (np. 5 GHz, 17 GHz, 60 GHz) jako ekonomicznego i szybkiego rozwiązania dla własnych sieci.

Co więcej, odwołujący od wielu lat świadczy usługi bezpośrednio na rzecz operatorów komórkowych w zakresie budowy i utrzymania takich systemów dosyłowych w pasmach nielicencjonowanych, zapewniając im stabilne i niezawodne funkcjonowanie infrastruktury przesyłowej. Oznacza to, że ci sami operatorzy, na których powołuje się zamawiający, w swojej działalności korzystają na szeroką skalę z pasm nielicencjonowanych i powierzają odwołującemu utrzymanie tych krytycznych elementów swojej sieci. W tym Świśle żądanie, aby komunikacja urządzeń końcowych z bramkami była ograniczona wyłącznie do pasm licencjonowanych, jawi się jako niespójne i arbitralne. Skoro bowiem operatorzy komórkowi sami uznają pasma nielicencjonowane za wystarczająco niezawodne, aby obsługiwać ruch dosyłowy pomiędzy stacjami bazowymi (co stanowi element krytyczny dla funkcjonowania ich sieci), to tym bardziej brak jest podstaw, aby odrzucać możliwość realizacji transmisji z urządzeń IoT w tych samych pasmach, zwłaszcza że Odwołujący wykazał zdolność Świadczenia takich usług z zachowaniem wymaganego poziomu SLA.

Wniosek dowodowy nr 17 — Tajemnica przedsiębiorstwa Emitel

Wniósł o dopuszczenie i przeprowadzenie dowodu z dokumentów umów (zamówień) usług dzierżawy łącz radiowych podpisanych pomiędzy Emitel S.A. a T-Mobile Polska S.A., dokumentujących świadczenie usług transmisji danych w paśmie nielicencjonowanym, z gwarantowanym SLA.

Z dokumentów wynika jednoznacznie, że Emitel Świadczy na rzecz T-Mobile Polska usługi transmisji danych realizowane w paśmie nielicencjonowanym.

Teza dowodowa:

Dowód ten potwierdza, że operatorzy komórkowi — w tym T-Mobile — sami w swojej działalności sieciowej korzystają z łącz dosyłowych w paśmie nielicencjonowanym i powierzają Emitel realizację usług o krytycznym znaczeniu dla funkcjonowania ich stacji bazowych. Paradoks wymogów OPZ polega więc na tym, że zamawiający wymaga, aby transmisje z nakładek do stacji bazowych odbywały się wyłącznie w paśmie licencjonowanym, podczas gdy w praktyce transmisje między stacjami bazowymi operatorów komórkowych często realizowane są właśnie w pasmach nielicencjonowanych.

Wniosek o utajnienie

Na podstawie art. 545 ust. 3 ustawy wniósł o utajnienie niniejszego dowodu („Zał. 17 Zamówienie na zestawienie łącz”) przed innymi uczestnikami postępowania odwoławczego, z wyjątkiem zamawiającego, Krajowej Izby Odwoławczej oraz przystępującego T-Mobile z uwagi na okoliczność, że informacje zawarte w ww. dokumentach stanowią tajemnicę przedsiębiorstwa Emitel w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Dokumenty te zawierają bowiem szczegółowe dane techniczne, organizacyjne oraz handlowe Emitel, a ich ujawnienie mogłoby narazić przedsiębiorcę na szkodę. Oświadczył, że informacje te, zarówno jako całość, jak i w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji oraz nie są łatwo dostępne dla takich osób.

Odpowiedź na argument o APN i własnej infrastrukturze

Zamawiający wskazał, że wymóg korzystania z dedykowanej podsieci APN i w 900/0 z własnej infrastruktury jest podyktowany względami bezpieczeństwa (infrastruktura krytyczna, wytyczne MC, art. 21 NIS2), a dostęp do jego realizacji mają wszyscy operatorzy komórkowi (Orange, Polkomtel, T-Mobile, P4). Stanowisko to jest niezasadne:

a/ APN nie jest jedynym sposobem na zapewnienie bezpieczeństwa

Dyrektywa NIS2 wskazuje na konieczność „segmentacji i kontroli komunikacji”, ale nie przesądza, że segmentacja ta musi zostać wykonana w oparciu o APN operatora komórkowego. Ten sam efekt można osiągnąć w systemach LoRaWAN czy separacji logicznej ruchu, szyfrowania AES-128 end-to-end i dedykowanych serwerów aplikacyjnych. OPZ zawiera wymagania szyfrowania TLS 1.3 i AES-128, które są standardowo realizowane również w sieciach nieopartych na APN GSM.

b/ Wymóg 90% „własnej infrastruktury” jest nieracjonalny

Zamawiający twierdzi, że dostęp do tego wymogu mają wszyscy operatorzy GSM, ale pomija fakt, że nawet oni nie korzystają wyłącznie z własnej infrastruktury — stosują powszechnie modele współdzielenia (np. NctWorks! — wspólna infrastruktura T-Mobile i Orange, czy współdzielenie sieci Polkomtela i P4). Skoro nawet operatorzy nie spełniają warunku literalnie, to wymóg staje się czysto iluzoryczny i de facto preferuje największych operatorów infrastrukturalnych, eliminując mniejszych graczy i integratorów.

c/ Faktyczne uprzywilejowanie Orange

Na obszarze aglomeracji katowickiej największą, najgęstszą i najlepiej rozwiniętą infrastrukturą komórkową dysponuje Orange Polska S.A. Wymóg 90% własnej infrastruktury w praktyce premiuje właśnie tego operatora, ponieważ mniejsi operatorzy korzystają z modeli dzierżawy lub współdzielenia sieci. Twierdzenie zamawiającego, że wymóg nie preferuje Orange, jest głosłowne — w praktyce takie ukształtowanie kryterium oznacza przewagę podmiotu dominującego na rynku. d/ Eliminacja konkurencji poza MNO MVNO, integratorzy czy operatorzy hurtowi, którzy mają techniczne i organizacyjne kompetencje do realizacji zamówienia, zostają z góry wykluczeni. To ogranicza konkurencję i sprowadza rynek do 3—4 operatorów komórkowych, podczas gdy dostępne są inne technologie i modele biznesowe, które mogłyby zagwarantować równie wysoki poziom SLA i bezpieczeństwa.

Odpowiedź na argument o „pełnej kontroli nad infrastrukturą”

W odpowiedzi na odwołanie zamawiający wyjaśnił, że wymóg „własnej infrastruktury” należy rozumieć nie jako własność fizyczną masztów czy światłowodów, lecz jako posiadanie pełnej kontroli operacyjnej nad infrastrukturą w co najmniej 90% przypadków. Wskazał, że celem jest ograniczenie ryzyka podwykonawstwa kaskadowego oraz zapewnienie gwarancji SLA i integralności danych.

Stanowisko to nie wytrzymuje krytyki z kilku powodów:

a/ Niejasność definicji

Pojęcie „pełna kontrola operacyjna” jest nieostre i może być interpretowane w różny sposób. Nic wiadomo, czy oznacza to posiadanie wyłącznych uprawnień konfiguracyjnych, pełnej widoczności ruchu IP, czy także prawo do zarządzania pasmem radiowym. W praktyce żaden wykonawca nie jest w stanie udowodnić tak rozumianej „pełnej kontroli”, bo zawsze istnieją elementy infrastruktury pozostające poza jego zarządem (np. urządzenia węzłowe operatora). Wymóg ten jest więc nieprecyzyjny, a przez to niezgodny z art. 99 ust. 1 ustawy.

b/ Nierealność spełnienia wymogu w praktyce

Nawet operatorzy infrastrukturalni nie spełniają literalnie wymogu 90% własnej infrastruktury z pełną kontrolą operacyjną — korzystają z modeli współdzielenia (np. NetWorks! — Orange i T-Mobile wspólnie zarządzają siecią radiową, Polkomtel i P4 współdzielą elementy sieci). Skoro nawet najwięksi gracze nie mają wyłącznej kontroli nad całością infrastruktury, to wymaganie staje się nierealne i iluzoryczne.

c/ SLA i bezpieczeństwo można zagwarantować inaczej

Cele wskazane przez zamawiającego (monitoring ruchu, integralność danych, szyfrowanie, redundancja, SLA) mogą być w pełni osiągnięte również w modelach współdzielonych lub integratorskich. Od tego właśnie służą umowy SLA — które mogą precyzyjnie regulować odpowiedzialność operatora za dostępność, czas reakcji i bezpieczeństwo transmisji. Stosowanie VPN, tuneli IPsec czy szyfrowania AES128 zapewnia taki sam poziom poufności i integralności danych jak dedykowany APN. d/ De facto ograniczenie konkurencji

Wymóg „pełnej kontroli” preferuje jedynie największych operatorów infrastrukturalnych i eliminuje z rynku integratorów, MVNO i operatorów hurtowych, którzy mogliby zaproponować konkurencyjne cenowo i technologicznie rozwiązania, spełniające te same cele. Tymczasem celem art. 99 ust. 4 ustawy jest zapewnienie proporcjonalności wymagań i otwartości konkurencji — a nie tworzenie definicji, które w praktyce wykluczają większość rynku.

Zamawiający twierdzi, że tylko dedykowany APN w technologii komórkowej jest w stanie zapewnić wymagany poziom bezpieczeństwa, integralności i niezawodności transmisji danych. Jest to założenie nieuprawnione, ponieważ funkcje, które przypisuje się dedykowanemu APN, mogą być w pełni i skutecznie zrealizowane również w technologii LoRaWAN przy użyciu innych środków technicznych.

Poniższa tabela przedstawia zestawienie argumentów zamawiającego dotyczących APN oraz odpowiadających im rozwiązań w LoRaWAN, które pozwalają osiągnąć identyczne cele w zakresie segmentacji ruchu, szyfrowania, kontroli i raportowania SLA.

Funkcja / Cel APN wg Zamawiającego Rozwiązanie w  
 APN GSM Odpowiednik w LoRaWAN  
 (alternatywa) Uwagi

Segmentacja ruchu, izolacja od Internetu publicznego Dedykowana podsieć APN wydzielona logicznie od publicznego Internetu Prywatna sieć LoRaWAN z własnymi bramkami dedykowany serwer Network Server; ruch tunelowany przez VPN/1Psec do systemu

Zamawiającego LoRaWAN działa w modelu prywatnej sieci — pełna separacja ruchu możliwa już na poziomie architektury

Kontrola komunikacji i priorytetyzacja GSM Perator zarządza QoS w sieci mobilnej Kontrola ADR (Adaptive Data Rate) + konfiguracja kanałów i moc nadawcza w LoRaWAN; dodatkowo możliwy priorytet w warstwie aplikacyjnej W systemach pomiarowych transmisje są sporadyczne i krótkie Qos GSM nie daje istotnej przewagi

Szyfrowanie i integralność danych TLS 1.3, szyfrowanie transmisji w APN AES-128 end-to-end (standard LoRaWAN) + TLS

1.3 pomiędzy Network Server a systemem Zamawiającego W LoRaWAN szyfrowanie jest natywne i działa od urządzenia do serwera aplikacyjnego

Możliwość monitorowania ruchu i raportowania SLA Operator GSM zapewnia logi i monitoring ruchu IP Własny Network Server LoRaWAN generuje raporty transmisji, poziom RSSI/SNR Odwołujący jako operator sieci ma pełną

Funkcja / Cel APN wg Zamawiającego Rozwiązanie w  
 APN GSM Odpowiednik w LoRaWAN (alternatywa) Uwagi

statystyki pakietów, monitoring bram kontrolę nad całości ruchu i raportami

Redundancja, niezawodność Operator zapewnia redundancję tras i stacji bazowych Redundantne bramy LoRaWAN - jeden pakiet może być odebrany przez wiele bram; serwer wybiera najlepszy W LoRaWAN redundancja jest natywna wzmacnia SLA

Bezpieczeństwo i niezależność od podwykonawców APN kontrolowany przez operatora GSM Sieć LoRaWAN budowana i kontrolowana przez wykonawcę; pełna własność bram, serwerów i konfiguracji LoRaWAN wykonawca

Zamawiającymają bezpośrednią kontrolę nad infrastrukturą

Dodatkowo odwołujący podkreślił, że ruch sieci LoRaWAN nie odbywa się w publicznym Internecie, lecz w prywatnej sieci LoRaWAN zbudowanej i utrzymywanej przez Odwołującego. Oznacza to, że Odwołujący — a nie operator zewnętrzny — ma pełną kontrolę nad ruchem, konfiguracją i bezpieczeństwem transmisji. Tym samym LoRaWAN zapewnia zamawiającemu niezależność i transparentność, której nie daje APN kontrolowany przez operatora GSM. Oznacza to, że wymóg stosowania APN GSM nie jest ani konieczny, ani proporcjonalny do zakładanych celów, a jego utrzymanie prowadzi do nieuzasadnionego ograniczenia konkurencji. Skoro bowiem oba rozwiązania pozwalają na osiągnięcie tych samych efektów, Zamawiający powinien dopuścić alternatywne technologie, w szczególności LoRaWAN, które dają zamawiającemu dodatkowo większą niezależność i pełną kontrolę nad infrastrukturą. Co więcej, odwołujący jest operatorem telekomunikacyjnym w rozumieniu ustawy Prawo komunikacji elektronicznej, a z tego tytułu podlega rygorom prawnym w zakresie zapewnienia bezpieczeństwa sieci i usług. W szczególności:

a/ art. 4 pkt 16 PKE — definiuje przedsiębiorcę telekomunikacyjnego jako podmiot świadczący publicznie dostępne usługi łączności elektronicznej, co obejmuje odwołującego;

b/ art. 40 ust. 1—2 PKE — nakłada na przedsiębiorców telekomunikacyjnych obowiązek zapewnienia integralności i bezpieczeństwa sieci oraz usług, w tym poprzez stosowanie odpowiednich środków technicznych i organizacyjnych;

c/ art. 41 ust. 1—3 PKE — nakłada obowiązek zgłaszania poważnych incydentów bezpieczeństwa Prezesowi UKE oraz CSIRT NASK i podejmowania działań naprawczych; d/ art. 42 ust. 1—2 PKE — wprowadza obowiązek współpracy z krajowym systemem cyberbezpieczeństwa, w tym wdrażania środków ochrony zgodnych z wymogami NIS2;

e/ art. 441)KE — nakłada obowiązek przechowywania danych o incydentach i prowadzenia dokumentacji w zakresie środków bezpieczeństwa.

W konsekwencji odwołujący — podobnie jak operatorzy GSM — podlega tym samym obowiązkom prawnym w zakresie cyberbezpieczeństwa, integralności i poufności danych. Nic ma więc żadnych podstaw, aby twierdzić, że wyłącznie operatorzy GSM zapewniają bezpieczeństwo wymagane w OPZ. Przeciwnie — model prywatnej sieci LoRaWAN budowanej i zarządzanej przez odwołującego daje zamawiającemu dodatkową gwarancję, że transmisja danych nie przechodzi przez infrastrukturę kontrolowaną przez zewnętrzny podmiot, lecz pozostaje pod pełną kontrolą wykonawcy, który podlega ustawowym obowiązkom bezpieczeństwa. W przypadku modelu sieci komórkowej odwołujący również realizuje ruch na zlecenie operatorów sieci komórkowej pomiędzy stacjami bazowymi.

LoRaWAN jako rozwiązanie niewymagające „budowy ad hoc” obalenie argumentu zamawiającego

Odwołujący podkreślił, że twierdzenie zamawiającego, że tylko wykorzystanie istniejącej infrastruktury GSM w pasmach licencjonowanych pozwala uniknąć budowy „ad hoc” i związanych z tym problemów, jest nieuprawnione i nie znajduje oparcia ani w stanie faktycznym, ani w prawie.

a/ LoRaWAN również opiera się na istniejącej infrastrukturze

Budowa sieci LoRaWAN nie oznacza konieczności stawiania masztów, ingerencji w przestrzeń publiczną czy szeroko zakrojonych prac terenowych. Bramy LoRaWAN instaluje się na istniejących obiektach (np. dachach budynków, masztach telekomunikacyjnych, obiektach użyteczności publicznej) bez konieczności przeprowadzania inwestycji infrastrukturalnych na dużą skalę. Nie jest to więc „budowa infrastruktury telekomunikacyjnej” w rozumieniu, którego obawia się zamawiający, lecz standardowe wdrożenie systemu radiowego opartego o istniejące zasoby.

b/ Problemy wskazane przez zamawiającego nie występują

Argumenty dotyczące rzekomych problemów z wejściem w teren, dewastacją czy kradzieżami są chybione. Odwołujący, jako operator telekomunikacyjny, posiada doświadczenie w legalnym i bezpiecznym lokowaniu urządzeń radiowych oraz zawieraniu umów z gestoraми obiektów. Bramy LoRaWAN są urządzeniami o niewielkich rozmiarach, nie wymagają instalacji drogich masztów, zużywają minimalne ilości energii, a ich montaż jest prosty i nieuciążliwy społecznie.

c/ Brak proporcjonalności wymogu

Skoro celem OPZ jest zapewnienie określonych progów SLA i bezpieczeństwa, to nie ma podstaw, aby arbitralnie eliminować rozwiązania alternatywne tylko dlatego, że nie korzystają z infrastruktury GSM. W rzeczywistości LoRaWAN zapewnia te same parametry odczytu przy niższych kosztach eksploatacji i większej niezależności Zamawiającego od podmiotów trzecich. d/ Infrastruktura GSM nic jest bezproblemowa

Zamawiający pomija fakt, że także sieć GSM wymaga inwestycji i rozbudowy — operatorzy wciąż stawiają nowe stacje bazowe, a proces ten również wiąże się z kwestiami prawnymi, społecznymi i technicznymi. W dodatku rezerwacje częstotliwości GSM mają ograniczony horyzont czasowy i są podatne na zmiany regulacyjne, co oznacza, że wybór GSM nie daje „wiecznej gwarancji” ciągłości działania.

Nieuzasadnione przypisywanie przewagi technologiom GSM — argumenty odwołującego

Zamawiający wskazuje szereg zalet technologii komórkowych działających w pasmach licencjonowanych (NB-IoT, LTE-M), które — jego zdaniem — uzasadniają konieczność oparcia systemu w 900/0 0 GSM. Argumentacja ta jest jednak jednostronna, pomija faktyczne ograniczenia GSM oraz całkowicie ignoruje możliwości technologii alternatywnych, takich jak LoRaWAN. Poniższa tabela przedstawia zestawienie twierdzeń zamawiającego i odpowiadających im kontrargumentów odwołującego.

Twierdzenie Zamawiającego Kontrargument Odwołującego

1. Szeroki zasięg i dobra penetracja sygnału — GSM umożliwia odczyt nawet z piwnic czy studzienek.

W praktyce GSM często nie działa w piwnicach i studzienkach zamawiający sam przyznaje, że w 10% lokalizacji konieczne jest użycie innej technologii. LoRaWAN dzięki redundancji bram i lepszej propagacji w pasmach 868 MHz zapewnia równie skuteczny odczyt w trudnych lokalizacjach.

Duża liczba BTS-ów nie gwarantuje pokrycia w pomieszczeniach podziemnych czy za grubymi Ścianami. Jakość zasięgu GSM zależy od decyzji operatorów, na które Zamawiający ani wykonawca nic ma wpływu. LoRaWAN daje możliwość budowy dedykowanej sieci pod potrzeby zamawiającego, co zwiększa niezawodność.

2. Niezawodność dzięki wielu stacjom bazowym (BTS)

3. Skalowalność” - sieci GSM zaprojektowane do masowych połączeń

LoRaWAN również jest globalnym standardem IoT, używanym w milionach urządzeń w Europie. Sieć może obsłużyć dziesiątki tysięcy wodomierzy przy minimalnym zużyciu energii. Skalowalność jest w pełni porównywalna.

Twierdzenie Zamawiającego Kontrargument Odwołującego

4. Stabilność i niezawodność dzięki pasmom licencjonowanym Operatorzy GSM sami wykorzystują pasma nielicencjonowane w swoich sieciach (np. dosyły Emitela), co przeczy tezie, że tylko pasma licencjonowane są stabilne. LoRaWAN posiada mechanizmy redundancji (odbiór jednego pakietu przez kilka bram), które zwiększają stabilność transmisji.

5. Bezpieczeństwo transmisji (NIS2, UKSC) LoRaWAN zapewnia natywne szyfrowanie AES-128 end-to-end, a ruch odbywa się w prywatnej sieci operatora odwołującego, nie w publicznym Internecie. Odwołujący jako przedsiębiorca telekomunikacyjny podlega obowiązkowi PKE (art. 40–44), tak jak operatorzy GSM.

6. Żywotność modułów radiowych (10 lat i więcej) LoRaWAN cechuje się jeszcze niższym zużyciem energii niż NB-IoT/LTE-M, osiągając w praktyce ponad 10-letnią żywotność baterii. GSM wymaga częstszej komunikacji, co realnie skraca czas pracy urządzeń.

7. Konserwacja braku konieczności obsługi własnej sieci To argument pozorny — w GSM zamawiający i tak jest zależny od działań operatora (np. modernizacji sieci 4G 5G). LoRaWAN daje pełną kontrolę i niezależność: sieć należy do wykonawcy, co eliminuje ryzyko zmian w polityce operatora GSM.

8. Standaryzacja — technologie 3GPP globalnie uznane LoRaWAN również jest globalnym standardem (LoRa Alliance, setki producentów), stosowanym w wielu krajach UE. Standardy interoperacyjności są zapewnione, a urządzenia dostępne u wielu producentów, także polskich.

Argumenty zamawiającego na rzecz technologii GSM są wybiórcze i często sprzeczne z praktyką rynkową. Sieć komórkowa nie gwarantuje pełnego zasięgu (co sam Zamawiający przyznaje, dopuszczając 10% lokalizacji dla innych technologii), nie daje pełnej niezależności (wykonawcy pozostają zależni od decyzji operatorów) i nie zapewnia przewagi w zakresie żywotności czy bezpieczeństwa transmisji.

Technologia LoRaWAN, wsparta obowiązkami regulacyjnymi odwołującego jako operatora telekomunikacyjnego, w pełni spełnia cele OPZ w zakresie niezawodności, bezpieczeństwa i skalowalności. Tym samym wymóg narzucania proporcji 90%) technologii komórkowej i 10%) LoRaWAN nie jest ani konieczny, ani proporcjonalny, a w istocie prowadzi do nieuzasadnionego ograniczenia konkurencji.

Brak wiedzy zamawiającego o skalowalności sieci komórkowej i ryzyko konieczności rozbudowy infrastruktury Zamawiający twierdzi, że technologie komórkowe działające w pasmach licencjonowanych (NB-IoT, LTE-M) cechują się wysoką skalowalnością, umożliwiając obsługę masowej liczby urządzeń pomiarowych.

Argument ten jest gołosłowny i nieoparty żadnymi dowodami.

Po pierwsze, zamawiający nie dysponuje wiedzą o faktycznej pojemności i skalowalności sieci komórkowej w Katowicach. Dane dotyczące liczby urządzeń, które mogą być obsługiwane przez poszczególne stacje bazowe, obciążenia pasma, czy planów modernizacji stanowią poufne informacje operatorów i nie są publicznie dostępne. Tak cenne dla operatorów sieci komórkowych dane z pewnością nie zostały też przez nich przekazane zamawiającemu. Ponadto, ani w OPZ, ani w odpowiedzi na odwołanie nie przedstawiono żadnej analizy ani gwarancji od operatorów komórkowych potwierdzających, że istniejąca infrastruktura jest wystarczająca dla potrzeb zamawiającego.

Po drugie, należy wskazać, że mówimy o systemie obejmującym 24 000 urządzeń telemetrycznych. W praktyce może to wymagać od operatorów komórkowych budowy nowych stacji bazowych lub modernizacji istniejących, aby zapewnić odpowiednie SLA. Oznacza to, że zamawiający — wbrew własnej argumentacji — nie unika ryzyka konieczności „budowy infrastruktury”, lecz je generuje, ponieważ to operatorzy komórkowi będą musieli dostosować swoją sieć do obciążenia związanego z tym zamówieniem. Natomiast czas budowy stacji bazowej telefonii komórkowej jest wielokrotnie dłuższy niżeli stacji LoRaWAN. Inne jest bowiem tempo budowy stacji bazowej ważącej ok. 400 kilogramów a inne jest tempo budowy stacji bazowej LoRaWAN ważącej 5-10 kilogramów. Sama budowa stacji bazowej telefonii komórkowej często wymaga uzyskania pozwolenia na budowę.

Po trzecie, odwołujący podkreślił, że zamawiający i wykonawcy nie mają żadnego wpływu na decyzje inwestycyjne operatorów komórkowych. Jeżeli okaże się, że obecna sieć jest niewystarczająca, to wyłącznie operator zdecyduje, czy i kiedy rozbudować infrastrukturę, a Zamawiający pozostanie od niego całkowicie zależny.

W przeciwieństwie do tego, technologia LoRaWAN pozwala na zaplanowanie i wdrożenie dedykowanej sieci już na etapie realizacji zamówienia. Bramy LoRaWAN instaluje się w oparciu o istniejące obiekty (budynki, maszty, słupy), bez konieczności prowadzenia kosztownych inwestycji infrastrukturalnych. Dzięki temu zamawiający otrzymuje gwarancję zasięgu i niezależność od harmonogramów inwestycyjnych operatorów GSM.

Skokowy wzrost obciążenia GSM a przewaga skalowalności LoRaWAN

Zamawiający twierdzi, że technologie komórkowe w paśmie licencjonowanym (NB-IoT, LTE-M) zapewniają skalowalność i możliwość obsługi masowej liczby urządzeń. Twierdzenie to jest gołosłowne i nieoparte żadnymi dowodami.

Po pierwsze, zamawiający nie przedstawił żadnych danych ani analiz dotyczących faktycznej skalowalności sieci GSM w Katowicach. Informacje o pojemności stacji bazowych, maksymalnej liczbie obsługiwanych urządzeń IoT czy realnym obciążeniu pasma należą do tajemnicy operatorów i nie są dostępne publicznie. Zamawiający nie uzyskał też od operatorów GSM żadnych gwarancji, że obecna infrastruktura sprosta obsłudze 24 000 dodatkowych kart SIM.

Po drugie, sieć GSM w Katowicach została zbudowana z myślą o obsłudze ruchu ludności — połączeń głosowych, transmisji danych mobilnych i w ograniczonym zakresie LOT. Dodanie nagle 24 000 nowych urządzeń telemetrycznych oznacza istotny, skokowy wzrost obciążenia sieci, który może prowadzić do przeciążeń i wymusić rozbudowę

infrastruktury. Tym samym zamawiający — wbrew własnym twierdzeniom — nie unika konieczności „budowy infrastruktury”, lecz realnie takie ryzyko generuje, tyle, że w sposób całkowicie zależny od decyzji inwestycyjnych operatorów GSM.

Po trzecie, należy podkreślić, że LoRaWAN posiada ogromny zapas skalowalności. Pojedyncza stacja bazowa obsługuje do 20 000 urządzeń, a przy 60 stacjach całkowita pojemność sieci wynosi 1,2 miliona urządzeń. To wielokrotnie więcej niż potrzeby zamawiającego (24 000 urządzeń), co oznacza, że LoRaWAN nie tylko spełnia, ale z ogromnym zapasem przekracza wymagania OPZ.

Wniosek dowodowy karty katalogowej stacji bazowej LoRaWAN wskazuje że do jednej stacji bazowej można podłączyć 20.000 urządzeń.

W sieci zbudowanej przez Emitel we Wrocławiu pracuje 60 tysięcy urządzeń a więc nic ma ryzyka, że zaprojektowana sieć dla Katowic nie spełni wymogów pojemnościowych.

Odpowiedź na zarzut braku infrastruktury LoRaWAN w Katowicach

Po pierwsze, należy jasno wskazać, że odwołujący nie jest w sytuacji porównywalnej do operatorów komórkowych. Operatorzy komórkowi posiadają pełną wiedzę o zasięgu swoich sieci, dysponują szczegółowymi mapami pokrycia i wiedzą, w których lokalizacjach ich sieć NB-IoT/LTE-M działa poprawnie, a w których wymaga wzmocnienia. Informacje te są objęte tajemnicą przedsiębiorstwa i nie są udostępniane konkurentom.

Odwołujący, aby móc konkurować w warunkach uczciwej rywalizacji, zmuszony był zaprojektować własną sieć LoRaWAN dla całego obszaru Katowic, gdyż w odróżnieniu od operatorów komórkowych nie posiada dostępu do informacji o ich „białych plamach” zasięgu. W tej sytuacji stwierdzenie zamawiającego, że odwołujący „musi budować sieć ad hoc”, w rzeczywistości pokazuje wadliwość warunków konkurencji, jakie zostały stworzone w postępowaniu. Zamawiający, świadomie bądź nie, przyznał operatorom komórkowym przewagę wynikającą z dostępu do informacji o własnych sieciach, a pozostałych wykonawców zmusił do budowania rozwiązań kompleksowych.

Po drugie, należy podkreślić, że odwołujący — jako doświadczony operator telekomunikacyjny (Emitel) przygotował projekt sieci LoRaWAN dla całego miasta Katowice w oparciu o profesjonalne analizy propagacyjne przeprowadzone przez specjalistów z zakresu planowania i projektowania sieci radiowych. Jest to standard w branży i gwarantuje, że sieć zostanie zbudowana w sposób zapewniający pełne pokrycie zasięgiem wymaganych lokalizacji.

Po trzecie, budowa sieci LoRaWAN w żaden sposób nie obciąża zamawiającego — będzie to sieć prywatna Emitela, sfinansowana i utrzymywana przez odwołującego. W początkowym okresie, zanim sieć zostanie w pełni zbudowana, Odwołujący zaoferuje nakładki działające w technologii komórkowej, co zapewni pełną ciągłość i niezawodność realizacji zamówienia. Nakładki LoRaWAN zostaną wdrożone dopiero wtedy, gdy cała sieć będzie gotowa i pokryje obszar miasta Katowice.

Po czwarte, należy zauważyć, że zamawiający sam wybrał model realizacji zamówienia, który wymusza jednoczesne pokrycie całego miasta. Równie dobrze mógł przewidzieć model wdrożenia etapowego, tj. budowę sieci „wyspowo” — w poszczególnych dzielnicach — a wraz z tym dostarczanie nakładek dostosowanych do rozwoju sieci. Takie rozwiązanie jest powszechnie stosowane przy wdrażaniu systemów telemetrycznych i mogłoby zostać zastosowane również tutaj. Zamawiający jednak tego nic przewidział, co ponownie wskazuje, że warunki zamówienia zostały ukształtowane w sposób nieproporcjonalny i ograniczający konkurencję.

Brak jednoznaczności w definicji pojęcia „własna infrastruktura” w dokumentacji przetargowej Odnosząc się do przytoczonego fragmentu wyjaśnień zamawiającego:

„Zamawiający ponownie wskazuje, że nic stawia wymogu posiadania infrastruktury fizycznej w znaczeniu prawa własności, lecz wymaga, aby wykonawca miał pełną, niezależną kontrolę nad infrastrukturą transmisyjną wykorzystywaną w minimum 90% przypadków należy podkreślić, że w treści OPZ użyto sformułowania „co najmniej 90% wykorzystywać własną infrastrukturę”, a zatem literalnie chodzi o własność infrastruktury, a nie o bliżej nieokreśloną „kontrolę operacyjną”.

Definicja pojęcia „własnej infrastruktury” została w dokumentacji przetargowej użyta wprost i nie może być obecnie dowolnie reinterpretowana na etapie odpowiedzi zamawiającego, tym bardziej że zamawiający nie zdecydował się zmienić OPZ przez usunięcie tego postanowienia.

Co więcej, odpowiedź zamawiającego nie rozwiewa wątpliwości dotyczących kryteriów, według których ma być liczony wskaźnik 90%. Nie wskazano bowiem, czy chodzi o: długość sieci, liczbę lokalizacji, przepustowość, czy inne parametry techniczne.

Brak precyzyjnego kryterium powoduje, że ocena ofert będzie arbitralna, a tym samym naruszona zostaje zasada uczciwej konkurencji.

Ponadto należy zweryfikować, czy w przypadku pozyskania usług w modelu dzierżawionym (np. poprzez karty SIM od operatora komórkowego), wykonawca rzeczywiście posiada możliwość zapewnienia elementów, które zamawiający wskazuje jako niezbędne, tj.:

- stałego monitorowania i zarządzania ruchem IP,
- gwarancji poziomu SLA,
- pełnej niezależności operacyjnej w zakresie dostępności, rekonfiguracji i rozliczalności danych,
- jednoznacznego zapewnienia integralności i bezpieczeństwa danych w warstwie sieciowej.

Odpowiedź jest oczywista: korzystając z infrastruktury komórkowej w modelu usługowym (np. poprzez zakup karty SIM), wykonawca nie posiada pełnej kontroli nad tymi parametrami. W praktyce zarządzanie ruchem, konfiguracja, SLA i bezpieczeństwo na poziomie warstwy sieciowej pozostają po stronie operatora komórkowego. To oznacza, że wymagania OPZ mogą zostać spełnione wyłącznie przez operatorów komórkowych dysponujących własną siecią radiową i transmisyjną.

Wbrew twierdzeniu zamawiającego, że zapis ten „nie eliminuje żadnego typu podmiotu”, w rzeczywistości zapis eliminuje wszystkich potencjalnych dostawców innych niż operatorzy komórkowi. W efekcie konkurencja zostaje sztucznie ograniczona, a możliwość złożenia ofert przez operatorów hurtowych, MVNO czy integratorów praktycznie wyłączona.

Odwołanie do stanowiska Zamawiającego i testów pilotażowych

Zamawiający wskazuje, że wymóg posiadania 90% własnej infrastruktury w technologii GSM (NB-IoT /LTE-M) został uzasadniony przeprowadzonym pilotażem czterech technologii transmisyjnych (LTE-M, NB-10T, WIZE 169 MHz, LoRaWAN 868 MHz), w wyniku którego technologie oparte na paśmie licencjonowanym miały wykazać przewagę w zakresie niezawodności, bezpieczeństwa, propagacji sygnału oraz kosztów operacyjnych.

Jednak analiza materiałów z pilotażu, w tym wniosku dowodowego z wyniku testu prowadzonego przez Emitel, wskazuje, że technologia LoRaWAN osiągnęła bardzo wysoką skuteczność odczytów — rzędu 100% w cyklu miesięcznym po uruchomieniu sieci i instalacji wszystkich nakładek, w tym także w lokalizacjach trudnych, tj. piwnicach i studzienkach wodomierzowych.

Oznacza to, że technologia LoRaWAN spełniła podstawowe kryteria wskazane przez zamawiającego jako kluczowe w pilotażu (niezawodność transmisji, bezpieczeństwo, zasięg propagacji, koszty eksploatacyjne). W konsekwencji, argumentacja zamawiającego, że jedynie technologie komórkowe zapewniają „najlepszy bilans niezawodności, kosztów i bezpieczeństwa”, stoi w sprzeczności z wynikami uzyskanymi w ramach testów LoRaWAN. Zrzuty danych z systemu po realizacji testu (zamieszczony w tym dokumencie) jasno pokazuje, że LoRaWAN — mimo konieczności budowy własnej infrastruktury — potrafi zapewnić wysoką skuteczność odczytu i niezawodność transmisji w trudnych warunkach urbanistycznych Katowic.

Co więcej:

1/ Bezpieczeństwo transmisji — LoRaWAN opiera się na otwartym, ale standaryzowanym protokole z szyfrowaniem end-to-end, a wyniki testów wykazały stabilność i odporność na zakłócenia

2/ Koszty operacyjne — budowa własnej sieci LoRaWAN wiąże się z nakładem inwestycyjnym, lecz w długim horyzoncie pozwala na pełną kontrolę nad siecią, brak opłat za każdą kartę SIM i uniezależnienie od polityki operatorów komórkowych.

3/ Aspekt społeczny — teza zamawiającego o „negatywnym odbiorze społecznym montażu anten” jest nieudokumentowana; w wielu miastach w Polsce LoRaWAN jest wdrożone na szeroką skalę bez oporu społeczności lokalnych. Zamawiający nic nie podał przykładu zgodnie z którym taka realizacja została zatrzymana ze względu na takie protesty społeczne. Historia zna jednak liczne przypadki protestów przeciwko budowie stacji bazowych telefonii komórkowej (m.in. protest mieszkańców Woli Justowskiej w Krakowie, protesty mieszkańców w Bieżdziejcu oraz w Konstancynie Łódzkim).

4/ Należy więc wskazać, że wymóg 90% wykorzystania infrastruktury komórkowej nie wynika jednoznacznie z wyników pilotażu — przeciwnie, testy pokazały, że alternatywne technologie, takie jak LoRaWAN, również spełniają kryteria niezawodności i jakości transmisji.

5/ W rezultacie, podtrzymanie wymogu „90% własnej infrastruktury GSM” w OPZ:

- eliminuje z udziału podmioty inne niż operatorzy komórkowi, co narusza zasadę uczciwej konkurencji,
- nie znajduje pełnego uzasadnienia w wynikach pilotażu, które dowodzą skuteczności także innych technologii,
- prowadzi do zawężenia rynku wyłącznie do operatorów GSM, mimo że rozwiązania takie jak LoRaWAN zostały praktycznie zweryfikowane w Katowicach i wykazały wysoką skuteczność działania.

Odpowiedź na stanowisko Zamawiającego — Ad Zarzut 3 („dedykowana podsieć APN”)

Zamawiający wskazuje, że sformułowanie „dedykowana podsieć APN” nie jest nieprecyzyjne, ponieważ — jak twierdzi — ma ono ugruntowane znaczenie w praktyce operatorów komórkowych i oznacza logiczną separację ruchu (np. prywatny APN z tunelem IPsec/MPLS), a nie fizyczną izolację transmisji.

Taka odpowiedź nie usuwa jednak podniesionych wątpliwości:

1/ Brak definicji w OPZ — w dokumentacji przetargowej brak jest jednoznacznego zdefiniowania, czy wymóg dotyczy

fizycznej czy logicznej separacji. Sam fakt, że w praktyce operatorzy stosują różne modele APN (standardowy publiczny, prywatny z IPsec, MPLS, GRE) dowodzi, że termin nie ma jednolitego znaczenia. Zamawiający dopiero na etapie odpowiedzi na odwołanie próbuje tę definicję zawęzić. To powoduje naruszenie zasady przejrzystości i pewności prawa (art. 16 ustawy).

Uzależnienie od operatorów infrastrukturalnych — zamawiający wskazał, że wymóg ten „nie stanowi bariery konkurencyjnej”, ponieważ jest powszechnie dostępny. W praktyce jednak możliwość zestawienia prywatnego APN z tunelem IPsec/MPLS jest usługą świadczoną wyłącznie przez operatorów GSM i ewentualnie MVNO posiadających specjalne umowy operatorskie. Tym samym wymóg eliminuje większość integratorów i dostawców rozwiązań IoT, którzy nie mają bezpośredniego dostępu do konfiguracji APN u operatora. To faktycznie ogranicza konkurencję do podmiotów posiadających uprzywilejowaną pozycję na rynku telekomunikacyjnym.

2/Niespójność z praktyką testów pilotażowych — należy podkreślić, że w przeprowadzonych testach pilotażowych (m.in. w Katowicach, na bazie rozwiązań LoRaWAN) nie stosowano separacji transmisji w postaci dedykowanego APN — a mimo to osiągnięto skuteczność transmisji danych na poziomie 97—99% i spełniono wszystkie wymogi bezpieczeństwa (szyfrowanie end-to-end, autoryzacja). To dowodzi, że wymaganie dedykowanego APN nie jest obiektywnie konieczne dla zapewnienia bezpieczeństwa i ciągłości działania systemu.

3/ Brak proporcjonalności wymogu — skoro bezpieczeństwo i niezawodność transmisji może być zapewnione także w innych modelach (np. LoRaWAN z szyfrowaniem AES128/256, prywatne tunele VPN w modelu niezależnym od GSM), to żądanie wprost „dedykowanej podsieci APN” jest nadmiarowe i nieproporcjonalne względem celu.

Wniosek dowodowy nr 18

Wnioś o dopuszczenie i przeprowadzenie dowodu z dokumentu pn. „Metryka odpowiedzi na wniosek z dnia 21.07.2025 r.” (DK.WKR.0143.3.2025), sporządzonego przez Prezesa Urzędu Komunikacji Elektronicznej i udostępnionego w dniu 1 sierpnia 2025 r., na okoliczność ustalenia, że:

1. W okresie ostatnich trzech miesięcy (od 21 kwietnia 2025 r. do 21 lipca 2025 r.) do Prezesa Urzędu Komunikacji Elektronicznej nie wpłynęły żadne skargi dotyczące funkcjonowania sieci LoRaWAN pracujących w pasmach nielicencjonowanych.

2. Brak jest jakichkolwiek zgłoszeń dotyczących zakłóceń, problemów z łącznością czy innych nieprawidłowości w funkcjonowaniu tych sieci.

3. Żaden podmiot ani użytkownik nie zwracał się do Prezesa UKE o interwencję w związku z funkcjonowaniem sieci LoRaWAN w podanym okresie.

Uzasadnienie

Z przedłożonego dokumentu, sporządzonego w trybie ustawy o dostępie do informacji publicznej, wynika jednoznacznie, że w okresie objętym zapytaniem nic odnotowano żadnych skarg ani wniosków o interwencję Prezesa UKE dotyczących działania sieci LoRaWAN w pasmach nielicencjonowanych. Okoliczność ta ma istotne znaczenie dowodowe, albowiem potwierdza, że sieci LoRaWAN działają stabilnie i nie generują problemów wymagających interwencji organu regulacyjnego. W konsekwencji twierdzenia o rzekomych zagrożeniach lub braku bezpieczeństwa omawianej technologii nie znajdują potwierdzenia w praktyce i nie są poparte żadnymi formalnymi skargami złożonymi do właściwego organu państwowego.

Dowód ten dodatkowo wzmacnia tezę, że LoRaWAN jest technologią bezpieczną i prawidłowo funkcjonującą w ramach obowiązujących przepisów prawa telekomunikacyjnego, a jej eksploatacja nie rodzi problemów wymagających nadzoru ze strony Prezesa UKE.

Zestawienie wymogu OPZ i określenie spełnienia warunku przez protokół LoRaWAN Na potrzeby niniejszego postępowania Odwołujący przedstawia tabelaryczne zestawienie wymagań określonych w Opisie Przedmiotu Zamówienia (dalej: „OPZ”) wraz z oceną, czy technologia LoRaWAN spełnia dany wymóg.

W kolumnie pierwszej ujęto skrócony zapis wymogu OPZ (do uzupełnienia dosłownym cytatem z dokumentacji OPZ po przeprowadzeniu OCR).

W kolumnie drugiej wskazano, czy technologia LoRaWAN spełnia wymóg (TAK/NIE) wraz z krótkim uzasadnieniem technicznym.

Celem zestawienia jest wykazanie, że LoRaWAN spełnia wszystkie wymagania zamawiającego opisane w OPZ, w tym w zakresie kompatybilności z wodomierzami, parametrów transmisji, bezpieczeństwa, SLA odporności środowiskowej, integracji systemowej oraz zgodności z RODO i przepisami technicznymi.

Wymóg OPZ (skrót — do uzupełnienia tatem 1:1 0 OCRRaWAN spełnia? (tak/ nie + krótko dlaczego)

Moduły radiowe (nakładki) kompatybilne z TAK — moduły LoRaWAN dla wodomierzy produkowane wodomierzami DNI 5 — DN50; montaż bez w wersjach clip-on/dedykowanych dla rozmiarów DNI 5 — naruszenia legalizacji. DN50; odczyt impulsów/enkoder.

Pasmo pracy UE 868 MHz; zgodność z TAK — LoRaWAN EU868 działa w nielicencjonowanym przepisami (RED

ETSI). paśmie 868 MHz; urządzenia z oznakowaniem CE. Szyfrowanie danych endtoend; TAK - LoRaWAN stosuje AES128 (Nwk-SKey/AppSKey), bezpieczeństwo transmisji. unikalne klucze per urządzenie.

Częstotliwość odczytów/ telemetrii (np. min. TAK — profil odczytów konfigurowalny (np. 1—24/dobę) z I ></dobę) i harmonogram przesyłu. zachowaniem dutycycle EU868.

Buforowanie danych w urządzeniu w razie TAK — urządzenia wodomierzowe zwykle posiadają pamięć braku łączności i retransmisja. zdarzeń/odczytów i retransmisję.

Żywotność baterii min. X lat (np. 210 lat) TAK — ultralowpower; żywotność 10—15 lat przy 1—4 przy zadanym profilu pracy. wysyłkach/dobę.

TAK — dostępne moduły IP68, praca w zalanych Odporność środowiskowa (np. IP68), zakres studzienkach; anteny zoptymalizowane do montażu temp., zalanie studzienek. podziemnego.

Detekcje/zdarzenia: wyciek, cofniętyTAK — funkcje zdarzeniowe/ alarms dostępne w module i przepływ, manipulacja, pęknięcie instalacji. w platformie.

Platforma: dostęp WWW, role/ uprawnienia, TAK — platforma odczytowa/IoT z multitenant, RBAC, raporty, eksport danych, alerty.

API, raportowaniem.

Integracja z systemem bilingowym i IBO; TAK — API/CSV/FTP; wcbhooki; integracje referencyjne eksport/ REST AP harmonogramy.

(np. SUNTAR/inne).

Aplikacja montażowa na urządzenia mobilne (Android/iOS); skan kodów; weryfikacja sygnału.TAK — aplikacja do provisioningu z pomiarem RSSI/SNR; geotagowanie.

Zarządzanie siecią: ADR, zdalna zmiana konfiguracji, aktualizacje OTA.TAK — profile ADR; downlinki konfiguracyjne; OTA dla FW (jeśli wspiera producent).

Skalowalność — możliwość obsługi > N tys. urządzeń i wzrostu wolumenu.TAK — architektura chmurowa/ klastrowa; dodawanie bramek bez przestojów.

Raportowanie i analityka (np. bilanse strefowe, alarmy, KPI, eksport XLS/ PDF).TAK — dashboardy, harmonogramy raportów, eksport.

Wymogi RODO/bezpieczeństwa (logowanie, SSO/MFA, audyt, backup).TAK — RBAC, MFA, logi audytowe, szyfrowanie danych w spoczynku.

Serwis/gwarancja; czasy reakcji; wsparcie techniczne; szkolenia.TAK — SLA na platformę i urządzenia; pakiet szkoleń dla użytkowników.

Odporność na zalanie/ utrudnioną TAK — konfiguracja gęstości bramek; anteny dedykowane; propagację (studzienki, piwnice). retransmisje i bufor.

Odpowiedź na stanowisko Polkomtel

I.Uwagi ogólne

Stanowisko Polkomtelu w przeważającej mierze powiela argumentację zamawiającego, a jednocześnie — podobnie jak pismo zamawiającego — nic zawiera dowodów empirycznych potwierdzających arbitralnie przyjętą proporcję 90/10 w zakresie wykorzystania pasm licencjonowanych i nielicencjonowanych. Polkomtel ogranicza się do ogólnych twierdzeń o bezpieczeństwie i przewidywalności transmisji, nie przedstawiając ani badań, ani analiz, ani ekspertyz technicznych.

II.Brak własnej infrastruktury Polkomtelu w Katowicach

Polkomtel podnosi, że Emitel nie posiada własnej infrastruktury, podczas gdy sam w Katowicach również nic dysponuje niezależnymi stacjami bazowymi przeznaczonymi do realizacji usług w ramach zamówienia. Z dostępnych publicznie źródeł wynika, że w lutym 2021 r. Cyfrowy Polsat (wraz z Polkomtel) zawarł umowę sprzedaży około 99,99 % udziałów w spółce Polkomtel Infrastruktura do Cellnex Poland (grupa Cellnex Telecom) za ok. PLN 7 mld.

Brak jest tym samym dowodów, aby Polkomtel posiadał odrębną, własną infrastrukturę telekomunikacyjną związaną stricte z przedmiotem zamówienia.

III.Odpowiedź na argumenty o infrastrukturze krytycznej

Polkomtel powołuje się na bezpieczeństwo infrastruktury krytycznej. Jednak:

1/ prawo nie nakłada obowiązku korzystania wyłącznie z pasm licencjonowanych,

2/ technologia LoRaWAN jest stosowana w wielu krajach do obsługi infrastruktury krytycznej,

3/ bezpieczeństwo wynika z architektury systemu i szyfrowania, a nie z charakteru pasma, 4/ przedmiotem postępowania nie są usługi związane z dostawą wody, ani eksploatacja sieci wodociągowej, lecz usługi i urządzenia telekomunikacyjne, co wynika wprost z klasyfikacji kodów CPV. Wykonawca ma dostarczyć system telekomunikacyjny wraz z urządzeniami komunikacyjnymi, które służyć będą zdalnym odczytom wodomierzy. Nakładki na wodomierze nie stanowią elementu infrastruktury wodociągowej, lecz są urządzeniami telekomunikacyjnymi — elementami systemu transmisji danych, które z punktu widzenia prawa telekomunikacyjnego i prawa o komunikacji elektronicznej należą

traktować jako część sieci łączności, a nie jako część sieci wodociągowej.

Infrastrukturą krytyczną mogą być co do zasady systemy łączności, a więc sieci telekomunikacyjne, a nie wodomierze i transmisja danych z nich.

Sam zamawiający dopuścił możliwość użycia innych technologii w 10% lokalizacji, co przeczy tezie o absolutnej wyłączności pasm licencjonowanych.

IV. Odpowiedź na zarzut o czasie wdrożenia

Polkomtel twierdzi, że Emitel nic zdoła wdrożyć sieci w terminie 30 dni. Jednak Emitel zaproponował model hybrydowy — początkowe wykorzystanie kart SIM, a następnie sukcesywne uruchamianie bramek LoRaWAN.

Jest to rozwiązanie zgodne z OPZ, stosowane w praktyce rynkowej, pozwalające na płynne wdrożenie i stopniową migrację.

V. Ryzyka dla zamawiającego związane z Polkomtelem

Rezerwacje częstotliwości w pasmach 800/900 MHz wygasają w latach 2030—2032, a więc przed końcem kontraktu (2026—2036). Oznacza to brak gwarancji ciągłości usług komórkowych. Natomiast migracja operatorów do 5G w paśmie 700 MHz eliminuje możliwość korzystania z NB-IoT/LTE-M w horyzoncie 10 lat.

W konsekwencji to właśnie wybór technologii komórkowych rodzi dla Zamawiającego większe ryzyko przerw i nieciągłości niż dopuszczenie LoRaWAN.

5. Cyberbezpieczeństwo — nadużycie argumentacji

Polkomtel w swoim stanowisku odwołuje się do zagrożeń cybernetycznych, powołując się na przykład ataku na infrastrukturę wodociągową. Należy jednak podkreślić, że przypadki takie dotyczą ataków na systemy krytyczne — np. przepompownie, centrale sterowania czy SCADA — a więc elementy bezpośrednio związane z funkcjonowaniem sieci wodociągowej i bezpieczeństwem dostaw wody. Natomiast w przedmiotowym postępowaniu mówimy o transmisji danych z wodomierzy. Do chwili obecnej nie wskazano ani jednego przypadku ataku cybernetycznego, którego celem byłoby przejście lub manipulacja danymi odczytowymi liczników. Co więcej, same dane z liczników — tj. zużycie wody w danym gospodarstwie — nie mają charakteru krytycznego dla bezpieczeństwa infrastruktury. Należy również zauważyć, że wodomierze i nakładki odczytowe są często instalowane w miejscach publicznych (np. klatki schodowe, studzienki), a więc informacje o ich wskazaniach mogą być fizycznie dostępne dla osób trzecich. W tym kontekście twierdzenie, że to właśnie transmisja danych licznikowych stanowi obszar największego zagrożenia cybernetycznego, jest dalece przesadne i nie znajduje odzwierciedlenia w realiach.

Podnoszenie argumentu cyberbezpieczeństwa w tym zakresie ma charakter instrumentalny i nie uzasadnia narzucenia proporcji 90% GSM, skoro udowodnione zostało, że technologia LoRaWAN zapewnia wymagany poziom bezpieczeństwa.

Odpowiedź na stanowisko T-Mobile

I. Uwagi wstępne

Przystępujący w swoim piśmie utrzymuje, że wymóg stosowania pasma licencjonowanego w 900/0 lokalizacji nie stanowi wymogu nadmiernego ani nieproporcjonalnego, a także, że jedynie takie ograniczenie pozwala na należyte zaspokojenie potrzeb zamawiającego. Wskazuje przy tym na wyższość technologii NB-IoT nad LoRaWAN w zakresie niezawodności, skalowalności i bezpieczeństwa. Stanowisko to nie znajduje potwierdzenia ani w treści dokumentacji przetargowej, ani w dostępnych opracowaniach naukowych i branżowych. Co istotne, Zamawiający w OPZ nie różnicuje parametrów SLA dla poszczególnych technologii — zarówno LoRaWAN, jak i NB-IoT mają zapewnić identyczny poziom dostępności i jakości odczytów. Już samo to dowodzi, że technologie te są funkcjonalnie równoważne, a ograniczenie LoRaWAN do 10%) ma charakter arbitralny i eliminujący konkurencję.

II. Charakterystyka technologii LPWAN

W literaturze branżowej wyróżnia się dwie główne grupy standardów LPWAN:

działające w pasmach nielicencjonowanych:

LoRaWAN (868 MHz, przepływność 0,3-50 kb/s),

Sigfox (868 MHz, przepływność 100—600 kb/s); działające w pasmach licencjonowanych:

— NB-IoT (LTE-M, kilkanaście pasm od 450 do 2100 MHz, przepływność 32—66 kb/s), — Cat-M (LTE-M, przepływność 200 kb/s — 1 Mb/s).

O ile NB-IoT oferuje nieco wyższą przepływność, to nie jest to parametr mający znaczenie dla systemów zdalnego odczytu liczników. Wystarczy bowiem transmisja ramki tekstowej, a wysoka przepływność oznacza jedynie większe zużycie energii i skrócenie żywotności baterii. Tymczasem urządzenia mają pracować nieprzerwanie przez minimum 10 lat.

Co więcej, pasma wyższe — jak 1800 czy 2100 MHz — mają zdecydowanie gorsze właściwości propagacyjne. Gorzej przenikają przez Ściany, stropy czy pokrywy studni. To prosta konsekwencja praw fizyki. Jeśli T-Mobile zakłada wykorzystanie wysokich pasm, dwukrotnie wyższych niżeli 868 MHz na której pracuje LoRaWAN to de facto będzie

uzyskiwał dwukrotnie gorsze warunki przenikania przez przeszkody.

II. Raport IEEE — pełny obraz, nie tylko wybiórcze cytaty

T-Mobile powołuje się na raport "Low-Power Wide-Area Networks: Comparison of LoRaWAN and NB-IoT Performance (IEEE, 2022). Niestety, czyni to wybiórczo, akcentując jedynie te fragmenty, które mają przemawiać za NB-IoT. Tymczasem autorzy publikacji przedstawiają zrównoważony obraz obu technologii, wskazując również szereg przewag LoRaWAN. Przykładowo:

"LoRaWAN is more advantageous in terms of energy efficiency and cost, whereas NB-IoT offers more benefits in terms of reliability and resilience to interference and latency."

LoRaWAN jest korzystniejszy kosztowo i energetycznie. To kluczowe w projektach gdzie setki tysięcy urządzeń pracują na baterii przez dekadę.

"For LoRaWAN, the energy consumption remains stable regardless of the number of EDs in the network... "

Zużycie energii w LoRaWAN nie rośnie wraz z liczbą urządzeń. To gwarancja stabilnej skalowalności energetycznej.

... anyone in principle could offer LoRaWAN coverage; private deployments may be useful... LoRaWAN networks might be available for FCC in some areas. . .

LoRaWAN daje zamawiającemu elastyczność: można zbudować własną prywatną sieć, bez abonamentów i opłat licencyjnych, a nawet korzystać z darmowych sieci społecznościowych. "For LoRaWAN, using the ADR turns out to be the best choice..

Mechanizm ADR zwiększa efektywność i przepustowość LoRaWAN, optymalizując sieć dla dużej liczby urządzeń.

"NB-IoT almost always provides higher throughput whereas for very high traffic the two becomes comparable."

Przy bardzo dużej liczbie urządzeń różnice między NB-IoT a LoRaWAN się zacierają— a wtedy przewagę zyskuje technologia tańsza i mniej energochłonna, czyli LoRaWAN.

T-Mobile pomija te konkluzje, choć mają one istotne znaczenie dla niniejszego postępowania.

IV. Odpowiedź na szczegółowe tezy T-Mobile

1. „NB-IoT zapewnia lepszy zasięg w pomieszczeniach”

— Sieć Emitela została zaprojektowana w oparciu o 60 stacji bazowych LoRaWAN, zapewniających pokrycie także w piwnicach i studniach. Argument o braku zasięgu LoRaWAN jest czysto teoretyczny i nie odnosi się do realnego projektu.

2. „NB-IoT jest bardziej niezawodny”

— Niezawodność to nie tylko parametry radiowe, ale także czas reakcji na awarie. Operatorzy komórkowi usuwają je zgodnie z przepisami w terminie do 36 godzin bo po takim czasie są zobowiązani do zwrotu opłaty za abonament. Emitel ma zespoły gotowe do usuwania awarii niezwłocznie do uzyskaniu informacji o jej wystąpieniu, o w praktyce daje zamawiającemu wyższą niezawodność.

3. „NB-IoT lepiej się skaluje”

— Sieć Emitela została obliczona na obsługę 1,2 mln urządzeń, przy czym zamówienie obejmuje 24 tys. sztuk. Istnieje więc ogromny zapas wydolności. T-Mobile nie podał żadnych danych dotyczących pojemności swojej sieci.

4. „NB-IoT ma lepsze mechanizmy modulacji”

Sam powołany przez przystępującego artykuł stwierdza że NB-IoT jest lepszy przy małym ruchu ale przy dużym LoRaWAN dogania NB-IoT.

5. „NB-IoT zapewnia wyższe bezpieczeństwo”

Emitel nic stosuje procedury aktywacji przez personalizację, lecz OTAA (Over-the-Air Activation), która generuje unikalne klucze sesyjne dla każdego urządzenia. OPZ przewiduje identyczne wymagania bezpieczeństwa dla obu technologii, więc nie można twierdzić, że LoRaWAN jest mniej bezpieczny.

V. Problem pojęcia „pasmo licencjonowane”

W OPZ użyto terminu „pasmo licencjonowane”, który nie występuje w ustawie — Prawo komunikacji elektronicznej. Ustawa posługuje się pojęciem „rezerwaacja częstotliwości”.

Wprowadzenie do dokumentacji przetargowej pojęcia pozaprawnego czyni OPZ niejednoznacznym i otwiera drogę do interpretacji eliminujących wykonawców innych niż operatorzy sieci komórkowych, w tym Emitela. W skrajnym przypadku może oznaczać wymóg dzierżawy pasma od operatora, a więc de facto zamknięcie rynku dla innych podmiotów bo jakie może być „źródło” takiej licencji na pasmo?

VI. Podsieć APN i infrastruktura własna

Odwolujący nie ma wpływu na konfigurowanie podsieci APN w sieciach operatorów komórkowych jedyną możliwością jest zakup kart SIM. Wymóg „90% własnej infrastruktury” faworyzuje operatorów, choć większość z nich sprzedała swoje maszty i wieże spółce Cellnex i obecnie korzysta z infrastruktury dzierżawionej.

Emitel natomiast w projekcie przewidział budowę własnych bramek LoRaWAN, co daje zamawiającemu większą niezależność i kontrolę nad systemem.

VII. Konkurencja i równość wykonawców

T-Mobile twierdzi, że w postępowaniu może wziąć udział wielu operatorów, ponieważ dysponują oni własną infrastrukturą. W praktyce infrastruktura ta w dużej części nie jest własnością operatorów, lecz została zbyta na rzecz Cellnex. Operatorzy korzystają z niej na podstawie umów serwisowych, nie zaś w reżimie własności. W konsekwencji wymaganie 900/0 „własnej infrastruktury” nie jest spełnione nawet przez samych operatorów komórkowych.

Odpowiedź na stanowisko Orange Polska

I. Uwagi ogólne

Orange w swoim piśmie nic przedstawia nowych argumentów ani niezależnych dowodów ponad te, które zaprezentował zamawiający. Stanowisko to w całości powiela twierdzenia zamawiającego i nie wnosi żadnych ustaleń empirycznych, które mogłyby wykazać zasadność narzuconej proporcji transmisji 90%/10%.

Orange, jako operator komórkowy, ma bezpośredni interes ekonomiczny w utrzymaniu ograniczeń faworyzujących technologie GSM (NB-IoT, LTE-M). Jego stanowisko nie może być traktowane jako obiektywne, lecz jako wyraz ochrony własnej pozycji rynkowej.

II. Odniesienie do głównych tez Orange Pilotaż

Orange powołuje się na rzekome wyniki pilotażu przeprowadzonego przez zamawiającego. Jednak zarówno zamawiający, jak i Orange, nie przedstawił żadnych raportów, danych liczbowych czy analiz technicznych, które dowodziłyby, że spełnienie SLA wymaga akurat 900/0 transmisji w technologii komórkowej. Wskazanie na sam fakt przeprowadzenia pilotażu — bez ujawnienia jego rezultatów — nie spełnia wymogu dowodowego wynikającego z art. 534 ust. 1 ustawy. Cyberbezpieczeństwo i NIS2

Orange akcentuje, że zamawiający jako podmiot kluczowy musi stosować adekwatne środki bezpieczeństwa. Odwołujący w pełni podziela wagę tego obowiązku, jednak należy podkreślić, że przepisy NIS2 ani PKE nie przewidują obowiązku stosowania technologii GSM w proporcji 90%), LoRaWAN posiada własne mechanizmy bezpieczeństwa (m.in. szyfrowanie AES-128 end-to-end), które pozwalają spełnić wymogi bezpieczeństwa na równi z sieciami komórkowymi.

Orzecznictwo KIO (sygn. KIO 2516/23, KIO 32/24)

Orange powołuje się na wcześniejsze wyroki, w których Izba uznała ograniczenia na rzecz NB-IoT/LTE-M. Należy podkreślić, że:

1/ w tamtych sprawach zamawiający wykazał konkretne ryzyka techniczne i przedstawił materiał dowodowy,

2/ w sprawie brak jest jakichkolwiek twardych danych technicznych, a wymóg 90/10 został przyjęty arbitralnie,

3/ Izba nie jest związana ustaleniami faktycznymi ani poglądami prawnymi przedstawionymi w innej sprawie.

Powoływanie się na te orzeczenia nie eliminuje obowiązku wykazania proporcjonalności i rzeczywistych potrzeb w obecnym postępowaniu.

Własna infrastruktura

Orange bagatelizuje problem, wskazując, że wymóg korzystania w 90% z własnej infrastruktury

Wykonawcy nie stanowi warunku udziału. W ocenie odwołującego taki wymóg stanowi faktycznie ukryty warunek udziału, eliminujący integratorów i operatorów niezależnych, którzy opierają się na infrastrukturze dzierżawionej lub alternatywnej. To narusza art. 112 ust. 1 ustawy oraz art. 99 ust. 4 ustawy, ponieważ ogranicza konkurencję wyłącznie do grupy operatorów komórkowych.

**Stan faktyczny:**

Z SWZ wynika:

ROZDZIAŁ III

TERMIN WYKONANIA ZAMÓWIENIA

Termin wykonania zamówienia: do 30.09.2029r. od dnia jej zawarcia, w tym:

1. w zakresie systemu odczytowego (uruchomienie), konfiguracji urządzeń mobilnych z systemem odczytowym: do 30 dni od dnia zawarcia umowy;

2. w zakresie dostawy urządzeń mobilnych: do 7 dni od dnia podpisania umowy;

3. w zakresie przeprowadzenia szkoleń: do 5 dni od dnia uruchomienia systemu;

4. w zakresie dostawy (sukcesywne dostawy na podstawie częściowych zamówień Zamawiającego) i konfiguracji modułów radiowych (nakładek): do 30.09.2029 roku od dnia zawarcia umowy;

ROZDZIAŁ IV

DODATKOWE INFORMACJE DLA WYKONAWCÓW

I. Dodatkowe informacje dotyczące postępowania:

Zamawiający wystąpił z wnioskiem o dofinansowania realizacji projektu w ramach Fundusze Europejskie dla Śląskiego 2021-2027 dla działania FESL.01.04 cyfryzacja administracji publicznej, w przypadku uzyskania dotacji zamówienie będzie rozliczane zgodnie z wymaganiami tego programu.

2. W przypadku pozyskania dofinansowania przez Zamawiającego, wykonawca zobowiązuje się przestrzegać wszelkich wytycznych, zleceń i wymagań z umowy o dofinansowanie unijne zawarte przez Zamawiającego, oraz przyjmuje do wiadomości, że Zamawiający może powołać Koordynatora (Inżyniera Kontraktu), z którym Wykonawca zobowiązuje się bezwzględnie współpracować.

3. Zamawiający zastrzega sobie prawo do unieważnienia postępowania w oparciu o art. 257 Pzp, tzn. jeżeli środki publiczne, które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia nie zostały mu przyznane.

4. Cena oferty musi zawierać wszystkie elementy wymienione w Opisie Przedmiotu Zamówienia oraz Projekcie umowy + podatek VAT według obowiązującej stawki ustawowej.

5. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych w umowie, której projekt stanowi załącznik nr 8 do SWZ.

6. Zamawiający nie dopuszcza składania ofert częściowych.

7. Zamawiający nie dopuszcza składania ofert wariantowych.

8. Zamawiający nie przewiduje zawarcia umowy ramowej.

9. Zamawiający nie przewiduje wyboru oferty z zastosowaniem aukcji elektronicznej.

10. Zamawiający nie przewiduje możliwości udzielenie zamówień, o których mowa w art. 214 ust. 1 pkt. 7 i 8 Ustawy pzp  
Opis przedmiotu zamówienia

I. Opis ogólny

OPZ (Opis Przedmiotu Zamówienia) określa podstawowe wymagania Zamawiającego dotyczące przedmiotu zamówienia, jakim jest „Dostawa, wdrożenie i obsługa systemu smart City w zakresie monitoringu sieci wodociągowej”.

1. Przedmiot zamówienia

1.1. Wdrożenie oraz obsługę systemu odczytowego na terenie miasta Katowice opartego na technologii Internetu Rzeczy (IoT) stanowiącego element Smart city w zakresie monitoringu sieci wodociągowej. System musi korzystać z komunikacji radiowej w licencjonowanych pasmach radiowych i w uzasadnionych przypadkach (nie więcej niż 10% lokalizacji) w pasmach nielicencjonowanych.

1.2. Zamawiający przewiduje, że do systemu odczytowego, w okresie obowiązywania umowy, podłączone będzie łącznie 24 000 szt. modułów radiowych IoT. Rzeczywiste ilości modułów radiowych IoT do podłączenia w danym roku obowiązywania Umowy zastaną ustalone przez Zamawiającego w planie dostaw.

1.3. Prace przewidziane do zlecenia w ramach niniejszego zamówienia będą podzielone na poszczególne zadania które nie stanowią odrębnych zamówień, lecz składają się na całość realizowanego przedsięwzięcia.

1.4. W celu kompleksowej realizacji przedmiotu zamówienia niezbędna jest realizacja następujących zadań:

1) Dostarczenie oraz dostosowanie do potrzeb zamawiającego przez Wykonawcę systemu umożliwiającego odczyt danych z urządzeń pomiarowych.

2) Uruchomienie systemu w ciągu 30 dni od podpisania umowy, w tym zapewnienie Zamawiającemu dostępu do platformy odczytowej i aplikacji mobilnej oraz transmisji danych z całego obszaru działania Zamawiającego.

3) Świadczenie usług związanych z obsługą systemu odczytowego przez Wykonawcę przez 10 lat od daty zawarcia umowy, zgodnie z wymaganiami zawartymi w rozdziale V OPZ, w tym utrzymanie sprawności systemu (SLA), transmisję danych oraz ich przekazywanie do systemu komputerowego Zamawiającego.

4) Dostarczenie przez Wykonawcę modułów radiowych IoT spełniających wymagania z Rozdziału II OPZ do dnia 30.09.2029r. oraz ich integracja z systemem odczytowym.

5) Dostarczenie przez Wykonawcę Zamawiającemu Urządzeń mobilnych, o parametrach wskazanych w Rozdziale V pkt4 OPZ, Nużących do konfiguracji modułów radiowych IoT i odczytu danych, w łącznej ilości 10 sztuk w ciągu 7 dni od podpisania umowy.

v. INFRASTRUKTURA SYSTEMU ODCZYTOWEGO - WYMAGANIA OGÓLNE

1. Wymagania ogólne

1) Zakres zamówienia:

a. Wykonawca zobowiązuje się do wdrożenia systemu odczytowego umożliwiającego odczyt danych z urządzeń pomiarowych na całym obszarze działania Zamawiającego. System musi opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej Zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną Wykonawcy.

b. System odczytowy musi zostać uruchomiony w ciągu 30 dni od podpisania Umowy, co obejmuje:

- Udostępnienie Zamawiającemu dostępu do platformy odczytowej i aplikacji mobilnej.

- Zapewnienie transmisji danych z całego obszaru działania Zamawiającego.

2) Pokrycie obszaru działania Zamawiającego

a. System odczytowy wdrożony przez Wykonawcę musi obejmować cały obszar działania Zamawiającego.

### 3) Uruchomienie systemu:

a. System odczytowy zostanie uruchomiony w ciągu 30 dni od podpisania umowy.

b. Uruchomienie obejmuje udostępnienie Zamawiającemu dostępu do platformy odczytowej oraz aplikacji mobilnej i zapewnienie transmisji danych z całego obszaru działania.

c. Z procesu uruchomienia zostanie sporządzony protokół.

4) Wykonawca zapewni bieżące naprawy, konserwację i serwis systemu, utrzymując go w pełnej sprawności przez cały okres obowiązywania umowy.

5) Wykonawca będzie gromadził dane odczytowe z urządzeń pomiarowych i przechowywał je w swojej infrastrukturze.

6) Dane z platformy odczytowej będą przekazywane do systemu komputerowego Zamawiającego w czasie ustalonym przez Zamawiającego (dodatkowo na żądanie). Sposób, struktura i zakres wymiany danych zostaną ustalone w okresie 14 dni obowiązywania umowy.

7) Integracja systemów i zarządzanie danymi w ramach realizacji zamówienia:

a. Połączenie między systemem komputerowym Zamawiającego a systemem odczytowym zostanie zapewnione za pomocą bezpiecznego połączenia internetowego, które będzie wykorzystywać tunel VPN (oparty na protokołach IPSec/SSL) lub innych technologiach transmisji z utrzymaniem wysokich standardów bezpieczeństwa — na tym samym lub większym poziomie od wymienionych powyżej.

b. Aby zapewnić integralności danych, Wykonawca zapewni wymianę danych M2M, poprzez udostępnienie API w zakresie umożliwiającym:

- Zbiorczy import odczytów dla podanych numerów urządzeń pomiarowych na podaną datę. Jeden odczyt dla każdego urządzenia pomiarowego najbliższy podanej dacie (mniejszy lub równy).

Import odczytu dla pojedynczego urządzenia pomiarowego na podaną

- Dla utrzymania bazy danych po stronie Wykonawcy — numery urządzeń pomiarowych, adresy posesji, trasy, grupy podziału, strefy itp. Poprzez API będzie możliwość aktualizacji danych związanych z wymianami modułów radiowych IoT.

- Wykonawca zobowiązany jest do zapewnienia stabilności API i zarządzania jego wersjami, tak aby ewentualne zmiany w API nie zakłócały integracji z systemem Zamawiającego.

8) Przekazywanie danych musi odbywać się w formacie elektronicznym, zgodnym z ustaleniami dokonanymi podczas procesu wdrożeniowego.

### 2. Wymagania dla Systemu odczytowego

1) System odczytowy musi zapewniać efektywne odczyty danych z urządzeń pomiarowych za pośrednictwem modułów radiowych IoT, zgodnie z określonymi wymaganiami.

2) System powinien być przystosowany do obsługi minimum 24 000 wodomierzy. Architektura systemu powinna zapewniać możliwość dalszego rozszerzenia (skalowania) bez konieczności wymiany lub gruntownej przebudowy infrastruktury systemowej.

3) System musi umożliwiać rejestrację wskazań urządzeń pomiarowych co najmniej raz na godzinę oraz przesyłanie zarejestrowanych danych co najmniej raz na dobę do platformy odczytowej.

4) Harmonogram przekazywania danych z modułów radiowych IoT do platformy odczytowej powinien być konfigurowalny na dowolną godzinę w ciągu doby oraz umożliwiać ustawienie interwałów przekazywania danych według preferencji.

5) Wykonawca gwarantuje określony poziom odczytywania danych (SLA), który nie może być mniejszy niż:

a. 90% objętych nim modułów radiowych IoT - 1 raz w ciągu doby.

b. 95% objętych nim modułów radiowych IoT - 1 raz na 7 dni kalendarzowych.

c. 98% objętych nim modułów radiowych IoT - przynajmniej 1 raz w miesiącu.

Poziom odczytu będzie ustalany na podstawie faktycznie działających modułów radiowych IoT, a skuteczny odczyt obejmuje przesłanie wszystkich wymaganych danych (w tym Indeksów, alarmów, i danych historycznych itd.) do platformy odczytowej.

6) System odczytowy musi zapewnić odczytywanie każdego modułu radiowego IoT od momentu jego zamontowania w punkcie rozliczeniowym, z wymaganą docelową skutecznością, zgodną z wymaganiami SLA (punkt 4).

7) Wykonawca zobowiązany jest zapewnić wysoki poziom bezpieczeństwa systemu:

a. Szyfrowanie: od modułu radiowego IoT, poprzez system odczytowy do systemu komputerowego Zamawiającego

b. Obowiązek stosowania bezpiecznych standardów komunikacji (np. TLS 1.3)

c. Szyfrowanie:

Zabezpieczenie danych: System odczytowy musi zapewniać szyfrowanie danych za pomocą co najmniej klucza AES 128-bitowego.

System odczytowy musi być odporny na próby nieautoryzowanego dostępu do danych przy użyciu technik reverse engineering.

Zapewnienie integralności danych. Każda przesyłana wiadomość powinna zawierać kod uwierzytelnienia wiadomości

(Message Authentication Code, MAC lub zabezpieczenie transmisji zgodne ze standardem RFC 7636 zabezpieczający dane przed atakami typu XSRF), który gwarantuje integralność przesyłanych danych.

d. Zamawiający zastrzega prawo do przeprowadzenia kontroli bezpieczeństwa w trakcie trwania umowy przez niezależny podmiot (na koszt Zamawiającego). Kontrola polega na próbach obejścia lub przełamania zabezpieczeń w celu wykrycia potencjalnych luk i uchybień. W przypadku ich identyfikacji Wykonawca jest zobowiązany do ich usunięcia bez zbędnej zwłoki na własny koszt. Po ich usunięciu Wykonawca powiadomi Zamawiającego.

e. Wykonawca musi posiadać certyfikat ISO:27001 (Zarządzanie Bezpieczeństwem

Informacji). ISO 9001 — System Zarządzania Jakością oraz ISO 14001 - System Zarządzania Środowiskowego

f. Wykonawca jest zobowiązany do niezwłocznego raportowania Zamawiającemu wszelkich incydentów bezpieczeństwa, wykrytych luk w zabezpieczeniach lub podejrzeń naruszenia bezpieczeństwa danych, związanych z systemem odczytowym lub danymi Zamawiającego do 72 godzin od ich wykrycia. Raport powinien zawierać szczegóły Incydentu, podjęte działania naprawcze oraz plan działania prewencyjnego.

8) Wykonawca zapewni, że odczytane dane pomiarowe będą przechowywane w jego własnych zasobach infrastrukturalnych lub u dostawcy infrastruktury zewnętrznej (na terenie Polski lub UE). Jednocześnie Wykonawca zagwarantuje nieograniczony dostęp do podglądu oraz możliwość pobierania danych poprzez przeglądarkę internetową lub tunel VPN.

9) Moduły radiowe IOT muszą umożliwiać transmisję danych przez okres co najmniej 10 lat od momentu dostawy. W przypadku awarii lub zużycia modułu radiowego IoT, Zamawiający zgłosi ten fakt Wykonawcy, podając numer seryjny modułu, w celu jego dezaktywacji.

i3. Platforma odczytowa do zarządzania Modułami radiowymi IoT

1) Wykonawca zapewni dostęp do platformy odczytowej działającej na zasobach wykonawcy i aplikację na urządzenia mobilne, niezbędne do działania systemu odczytowego, które umożliwi obsługę modułów radiowych IoT oraz prezentację danych z urządzeń pomiarowych. 2) Platforma odczytowa musi pozwalać na zalogowanie się minimum 40 użytkowników.

3) Platforma odczytowa będzie rejestrować i przechowywać dane kluczowe dla funkcjonowania i monitorowania sieci wodociągowej, m.in. takie jak:

a. identyfikatory punktu rozliczeniowego,

b. adres punktu rozliczeniowego,

c. numer urządzenia pomiarowego,

d. numer seryjny modułu radiowego IOT,

e. współrzędne geograficzne punktu pomiarowego,

f. stan baterii modułu radiowego IOT,

g. temperatura otoczenia,

h. data ostatniego odczytu, stan ostatniego odczytu,

j. zużycie miesięczne,

k. strefa, trasa odczytowa,

m. oznaczenie rodzaju urządzenia pomiarowego (np. nadrzędny, podlicznik).

4) Oprócz standardowych funkcjonalności dla tego typu aplikacji, zasadniczą opcją będzie możliwość wykonania różnego typu analiz i raportów, które umożliwią efektywne zarządzanie infrastrukturą siecią m.in.:

a. analizę działania urządzeń pomiarowych w celu wykrycia nieprawidłowości,

b. analiza pod kątem możliwości wystąpienia awarii,

c. zdalne ustawianie harmonogramów pracy modułów radiowych IoT,

d. historyczność pomiarów oraz gospodarki urządzeniami pomiarowymi i modułami radiowymi IoT.

5) Platforma odczytowa musi umożliwiać:

a. Zarządzanie użytkownikami i uprawnieniami

• tworzenie, edycję i usuwanie kont użytkowników,

• przydzielanie indywidualnych uprawnień uwzględniając różne poziomy dostępu do funkcji aplikacji.

6) w okresie realizacji umowy Wykonawca zapewni Zamawiającemu dostęp do najnowszej wersji platformy odczytowej i aplikacji mobilnej. Aktualna wersja oprogramowania ma zapewnić bezpieczeństwo systemu odczytowego, optymalną wydajność, naprawę ew. błędów, zgodność z regulacjami i standardami prawnymi, dostęp do nowych funkcji. Dostawca zobowiązuje się w okresie gwarancji dostosowywać oprogramowanie do zmieniających się systemów operacyjnych, przeglądarek internetowych itp.

7) Wykonawca zobowiązany jest zapewnić regularne (codzienne) tworzenie kopii bezpieczeństwa wszystkich przechowywanych danych, które umożliwiają przywrócenie stanu systemu oraz danych na dowolny dzień roboczy z ostatnich 90 dni. Kopie bezpieczeństwa powinny być przechowywane w sposób zapewniający ich integralność oraz

poufność.

8) Wykonawca przeprowadzi szkolenie obejmujące obsługę i konfigurację platformy odczytowej w tym generowanie raportów i zestawień 9) Czas trwania i organizacja szkolenia:

a. Każdy dzień szkoleniowy powinien zawierać:

- Szkolenie dla dwóch grup pracowników - po ok. 20 osób musi trwać minimum 3 godziny dla jednej grupy, co daje łącznie 2 dni szkoleniowe.

10) W przypadku realizacji szkolenia w formie online, Wykonawca zobowiązany jest dodatkowo udostępnić Zamawiającemu film instruktażowy lub nagranie z przeprowadzonego szkolenia.

11) Szkolenie kończy się wydaniem certyfikatu ukończenia szkolenia dla każdego przeszkolonego pracownika.

Platforma odczytowa musi działać poprawnie z następującymi przeglądarkami internetowymi: Google Chrome, FireFox, Microsoft Edge, Opera oraz poprawnie wyświetlać się na urządzeniach mobilnych.

Platforma odczytowa powinna być łatwa w obsłudze, posiadać intuicyjny interfejs użytkownika oraz umożliwiać eksport danych w popularnych formatach (np. CSV, XLS, PDF). Wymagana jest wysoka dostępność systemu oraz odpowiednie zabezpieczenia danych, zgodnie z obowiązującymi regulacjami prawnymi (NIS2, KSC)

4. Wymagania dla Urządzeń mobilnych oraz aplikacji na Urządzenia mobilne

1) Zakres dostawy

a. Wykonawca dostarczy fabrycznie nowe urządzenia mobilne zgodne z parametrami opisanymi w sekcji 4 (poniżej), w terminie do 7 dni od daty podpisania umowy.

b. Wraz z urządzeniami zostanie dostarczone oprogramowanie (aplikacja mobilna) do Inicjacja/konfiguracja modułów radiowych IoT z poziomu urządzeń mobilnych

- Przeprowadzenie wymiany urządzenia pomiarowego z synchronizacją systemem informatycznym Zamawiającego.

2) Urządzenia mobilne muszą zapewniać niezawodną i nieprzerwaną transmisję danych (aktywną kartę sim) do końca umowy, z uwzględnieniem zgodności z obowiązującymi standardami sieciowymi oraz technologiami wykorzystywanymi przez krajowych operatorów telekomunikacyjnych. Wykonawca zapewni możliwość instalacji aplikacji mobilnej na dodatkowych urządzeniach mobilnych (spełniających wymagania sprzętowo-programowe aplikacji) użytkowanych przez Zamawiającego.

3) W okresie realizacji umowy Wykonawca zapewni Zamawiającemu dostęp do najnowszej wersji aplikacji mobilnej, kompatybilnej z wymaganiami sprzętowymi.

4) W okresie wdrożenia systemu oraz w okresie gwarancyjnym Dostawca będzie dokonywał aktualizacji Aplikacji mobilnej uwzględniającej pojawianie się na rynku nowych wersji Systemu Android, umożliwiające działanie Aplikacji na urządzeniach mobilnych z najnowszą wersją Oprogramowania. Aktualizacja nie może uniemożliwiać czy też ograniczać działania Aplikacji mobilnej na urządzeniach mobilnych wykorzystujących starsze wersje systemu operacyjnego. Aplikacja mobilna w sposób autonomiczny lub we współpracy z platformą odczytową zapewni:

a. Powiązanie modułu radiowego IoT z platformą odczytów, poprzez wprowadzenie danych identyfikacyjnych,

b. odczytywanie stanu liczydła urządzenia pomiarowego,

c. odczytywanie danych alarmowych (min ostatnie 60 dni),

d. odczytywanie pamięci przechowującej zapisane pomiary (min ostatnie 30 dni),

e. przeprowadzenie procedury kalibracji impulsu pomiarowego,

f. odczytywanie stanu baterii z modułów radiowych IoT,

g. sprawdzenie stanu połączenia sieciowego z platformą odczytową

h. Przeprowadzenie wymiany urządzenia pomiarowego z synchronizacją systemem informatycznym Zamawiającego.

5) Wymagania dotyczące urządzeń mobilnych:

a. Wymagania techniczno-fizyczne:

1) odporność na upadek z wysokości min. 1,5 m,

2) klasa odporności min. IP65,

3) ekran o wielkości co najmniej 8 cali o rozdzielczości min. 1280x800

4) zakres pracy w temperaturach od -200C do 400 C,

b. Wymagania sprzętowe:

1) dostęp do Internetu w terenie (wbudowany modem LTE/5G obsługujący sieci GSM poprzednich generacji),

2) gniazdo kart nanoSIM,

3) procesor min. 6 rdzenie,

4) pamięć wbudowana min. 64 GB typ UFS,

5) pamięć RAM min. 6 GB,

6) aparat fotograficzny,

7) możliwość skanowania kodów ID i 2D,

- 8)opcjonalnie czytnik linii papilarnych,
- 9)bateria o pojemności nie mniejszej niż 7500 mAh (ciągła praca urządzenia przez mln 8 godzin)
- 10)porty: USB-C min. 1 szt,
- 11)komunikacja: Bluetooth. NFC, Wi-Fi, LTE/5G,
- 12) system nawigacji satelitarnej (min. GPS, Galileo)
- 13) system operacyjny Android wersja min. 13.
- 14) opcjonalnie rysik w zestawie.

6) Gwarancja:

a.Wykonawca udziela gwarancji na dostarczone urządzenia mobilne na okres minimum 24 miesięcy, licząc od daty dostawy..

b.Gwarancja obejmuje wszelkie wady fabryczne, usterki oraz inne nieprawidłowości wynikające z użytkowania zgodnie z przeznaczeniem.

c.W okresie gwarancji Wykonawca zobowiązuje się do bezpłatnej naprawy lub wymiany urządzenia na nowe, wolne od wad, w terminie nie dłuższym niż 14 dni roboczych od zgłoszenia usterki.

d.W przypadku, gdy naprawa lub wymiana urządzenia nie będzie możliwa w ww. terminie, Wykonawca zobowiązuje się do dostarczenia urządzenia zastępczego o parametrach nie gorszych niż urządzenie objęte zgłoszeniem gwarancyjnym.

e.Gwarancja nie obejmuje uszkodzeń mechanicznych powstałych z winy Użytkownika.

5.Wymagania w zakresie wsparcia technicznego dla systemu odczytowego i platformy odczytowej

1)Wsparcie obejmuje eliminację awarii (zarówno krytycznych, Jak i niekrytycznych) oraz rozwiązywanie problemów związanych z systemem odczytowym a w tym platformą odczytową, znajdującą się na serwerze zewnętrznym Wykonawcy. Celem jest zapewnienie nieprzerwanej pracy systemu odczytowego za wyjątkiem prac serwisowych uzgodnionych z Zamawiającym.

2)Zgłoszenie krytyczne obejmują awarie uniemożliwiające działanie systemu, takie jak brak możliwości logowania do platformy odczytowej, brak rejestrowania danych z urządzeń pomiarowych przez system odczytowy lub brak synchronizacji danych między platformą odczytową a innymi systemami informatycznymi Zamawiającego.

3)Zgłoszenie niekrytyczne obejmuje usterki utrudniające działanie platformy odczytowej, np. nieprawidłowe wyświetlanie serwisu w przeglądarce Internetowej, brak działania filtrów w tabelach, czy problemy z generowaniem i pobieraniem raportów.

4) Czas reakcji i naprawy:

a.Awaria krytyczna: Reakcja w ciągu 1 godziny, naprawa w ciągu 8 godzin.

b.Awaria niekrytyczna: Reakcja w ciągu 1 dnia roboczego, naprawa w ciągu 5 dni roboczych.

5)Zamawiający może zgłaszać awarie e-mailowo lub poprzez system zgłoszeń Wykonawcy (system musi generować potwierdzenie przyjęcia zgłoszenia spełniające cechy trwałego nośnika, np. w formie raportu e-mail). Zgłoszenia mogą być dokonywane w języku polskim, w dni robocze w godzinach 7:00—16:00 — zgłoszenia dokonane poza godzinami roboczymi uważa się za dokonane z chwilą rozpoczęcia kolejnej godziny roboczej. Za moment przyjęcia zgłoszenia uznaje się czas potwierdzenia odebrania wiadomości e-mail widoczny w skrzynce Zamawiającego lub zarejestrowania w systemie zgłoszeń Wykonawcy.

6)Wykonawca nie może jednostronnie zmieniać klasyfikacji awarii zgłoszonej przez Zamawiającego. Zmiana klasyfikacji jest możliwa jedynie za obu Stron.

7)W przypadku zgłoszeń dokonanych poza dniami roboczymi, czas reakcji I naprawy liczony jest od godziny 7:00 pierwszego dnia roboczego następującego po zgłoszeniu.

8)Naprawa oznacza całkowite i trwałe usunięcie awarii. Tymczasowe rozwiązania lub obejścia problemu nie są uznawane za usunięcie awarii.

Współpraca w ramach wsparcia technicznego odbywa się za pośrednictwem dedykowanych kanałów: systemu zgłoszeń, infolinii lub e-maila.

Załącznik nr 1 a – Harmonogram dostaw modułów radiowych IoT

Do końca 2025 – 1500 szt.,

2026 – 6700 szt.

2027 – 6500szt.

2028- 6500 szt.

2029- 2800 szt.

Ogłoszenie nr 458218-2025 data publikacji 14 lipca 2025 r.

Wyjaśnienia treści SWZ z 6 sierpnia 2025 r. :

Pytanie III.12:

OPZ V.1.2a Czy przypadku realnego braku zapewnienia pokrycia siecią w paśmie licencjonowanym 90% obszaru Wykonawca będzie zobowiązany do rozbudowy sieci telekomunikacyjnej w paśmie licencjonowanym, czy Zamawiający dopuści doświetlenie obszaru w paśmie nielicencjonowanym? Wskazujemy, że zapewnienie zasięgu sieci w paśmie licencjonowanym 4G/5G wiąże się w kosztownym i długotrwałym procesem przebudowy sieci. Cały proces może trwać do 2 lat.

Odpowiedź Zamawiającego:

Nie, Wykonawca zobowiązuje się do wdrożenia systemu odczytowego, który w 90% musi opierać się na technologii transmisji danych w paśmie licencjonowanym.

Pytanie V.9:

„Dot. II. WYMAGANIA DLA MODUŁÓW RADIOWYCH IOT – Ust. 4 pkt. 3)

Zapis istniejący:

„Moduły radiowe IoT muszą komunikować się z urządzeniami sieci radiowej dostarczonej przez Wykonawcę za pośrednictwem transmisji danych.”

Pytanie:

Czy Zamawiający dopuszcza wykorzystanie usług operatorów telefonii komórkowej, z której Wykonawca będzie korzystał (jako podwykonawca)?”

Odpowiedź Zamawiającego:

Tak, Zamawiający dopuszcza wykorzystanie usług operatorów telefonii komórkowej z zastrzeżeniem że Wykonawca będzie miał realny wpływ na działanie sieci radiowej.

Pytanie V.11:

„Dot. V INFRASTRUKTURA SYSTEMU ODCZYTOWEGO – WYMAGANIA OGÓLNE – Ust. 1. pkt 1. lit a)

Zapis istniejący:

„a) Wykonawca zobowiązuje się do wdrożenia systemu odczytowego umożliwiającego odczyt danych z urządzeń pomiarowych na całym obszarze działania Zamawiającego. System musi opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej Zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną Wykonawcy.”

Pytanie 1:

Zwracamy uwagę, że przywołany powyżej zapis OPZ nie jest zbieżny z zapisami projektu umowy w Par. 3 Ust. 5., dlatego prosimy o ujednoczenie zapisu zgodnie z zapisami Umowy.

„a) Wykonawca zobowiązuje się do wdrożenia systemu odczytowego umożliwiającego odczyt danych z urządzeń pomiarowych na całym obszarze działania Zamawiającego. System musi opierać się na technologii transmisji danych w wydzielonej podsieci APN dedykowanej Zamawiającemu i w co najmniej 90% wykorzystywać własną infrastrukturę telekomunikacyjną Wykonawcy.”

Pytanie 2:

Zwracamy również uwagę, że przywołany powyżej zapis OPZ nie jest zbieżny z zapisami projektu umowy w Par. 3 Ust. 5. Zwracamy się z prośbą o ujednoczenie zgodnie z zapisami Umowy.

Uzasadnienie:

Zapis taki bardzo poważnie ogranicza możliwość wzięcia udziału w postępowaniu, a co za tym idzie narusza zasadę uczciwej konkurencji. Pozostawienie zapisu w takiej formie powoduje, że ofertę może złożyć wyłącznie operator telefonii komórkowej, który posiada własną infrastrukturę komunikacyjną na terenie Katowic, a takie wymaganie spełnia prawdopodobnie wyłącznie Orange Polska SA. Wyklucza tym samym innych profesjonalnych dostawców rozwiązań radiowych i GSM, którzy specjalizują się w dostarczaniu takich rozwiązań od wielu lat, bazując jednak na infrastrukturze innych podmiotów na podstawie długoterminowych umów.”

Odpowiedź Zamawiającego:

Zamawiający dokona ujednoczenia z zapisami OPZ: w UMOWIE par 3 Ust 5 dopisując zwrot "...własną infrastrukturę telekomunikacyjną Wykonawcy" Zamawiający pod pojęciem „własnej infrastruktury” rozumie: Sieci będą własnością wykonawcy; Sieci dzierżawione, kolokacyjne; infrastruktura współdzielona. W OPZ pojęcie „własna infrastruktura” należy rozumieć jako infrastrukturę, do której wykonawca posiada wyłączne prawo dysponowania na poziomie operacyjnym i konfiguracyjnym.

Wyjaśnienia SWZ z 7 sierpnia 2025 r.

W W odpowiedzi na pytanie z 7 sierpnia 2025 r. o następującej treści:

„W rozdziale V ppkt 1 pppkt 1 Zamawiający wymaga, aby system odczytowy w co najmniej 90% wykorzystywał własną infrastrukturę telekomunikacyjną wykonawcy, opartą na wydzielonej podsieci APN. Taki zapis w praktyce uniemożliwiłby złożenie oferty przez podmioty inne niż operatory sieci komórkowej, ograniczając krąg potencjalnych wykonawców. Branżowe firmy niebędące operatorami telekomunikacyjnym dysponują odpowiednim doświadczeniem, zapleczem

technicznym oraz referencjami, które w pełni kwalifikują je do realizacji przedmiotu zamówienia. Tym samym zapis ten narusza zasadę zachowania uczciwej konkurencji i równego traktowania wykonawców, o której mowa w art. 16 ustawy. Zwracamy uwagę, że udział operatorów komórkowych w realizacji tego typu zamówień najczęściej ogranicza się jedynie do dostarczenia kart SIM i zapewnienia transmisji danych, co stanowi jedynie niewielki procent całkowitej wartości zadania. Wnosimy i wykreślenie lub modyfikację przedmiotowego zapisu w celu zapewnienia równego dostępu do postępowania i zwiększenia konkurencyjności.”

Zamawiający odpowiedział:

Zamawiający udzielił odpowiedzi w piśmie PW/2002/2025/ZDP/KLD z dnia 06.08.2025r. Powyższa odpowiedź jest wiążąca dla wszystkich wykonawców ubiegających się o zamówienie.

Dowody odwołującego:

Informacja o zajętości widma w pasmach 420 MHz, 450 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2600 MHz 3600 MHz potwierdza dane zawarte na str. 8 odwołania.

Załącznik przedstawiający informację z systemu obsługi sieci MPWIK Wrocław za miesiąc (TAJEMNICA PRZEDSIĘBIORSTWA), z którego wynika, że SLA dzienne i miesięczne dla tego systemu wskazują na możliwość osiągnięcia poziomów SLA wymaganych przez zamawiającego w tym postępowaniu przy zastosowaniu rozwiązania, którego dopuszczenia domaga się odwołujący.

Protokół odbioru częściowego nr (TAJEMNICA PRZEDSIĘBIORSTWA) z dokumentu tego wyniku wykonanie przedmiotu zamówienia w zakresie oraz jakości zgodnej z warunkami umowy oraz ze str. 3 tego dokumentu wynika, że SLA dzienne i miesięczne dla tego systemu wskazują na możliwość osiągnięcia poziomów SLA wymaganych przez zamawiającego w tym postępowaniu przy zastosowaniu rozwiązania, którego dopuszczenia domaga się odwołujący.

Wniosek o przeprowadzenie kontroli doraźnej do Prezesa Urzędu Zamówień Publicznych w postępowaniu „Dostawa, wdrożenie i obsługa stacjonarnego systemu odczytu danych z wodomierzy” nr ZP-014/D/RZ/2023 organizowanego przez Miejskie Wodociągi i Kanalizacja w Bydgoszczy spółka z ograniczoną odpowiedzialnością wraz z SWZ, ogłoszeniem o udzieleniu zamówienia firmie T-Mobile spółka akcyjna przy udziale WES spółka z ograniczoną odpowiedzialnością, wykazem lokalizacji wodomierzy, potwierdzeniem otrzymania wniosku o wszczęcie kontroli – KIO pominęła te dowody jako nie mające istotnego znaczenia dla rozstrzygnięcia, bo nie dotyczą spornego postępowania o udzielenie zamówienia, ani tego samego zamawiającego, nadto dotyczą postanowień SWZ, które nie są skarżone w tym postępowaniu. KIO uznała zatem, że czynienie ustaleń z tych dowodów nie służy rozstrzygnięciu przedmiotowego sporu.

Artykuł z Businessinsider.com.pl „Spółka Z.S. za miliardy złotych sprzeda maszty i wieże Polkomtela Hiszpanom”, z którego wynika, że Spółka Polkomtel wprowadza model biznesowy oparty o koncepcję współdzielenia aktywnej i pasywnej infrastruktury, skupiając się na zapewnieniu najwyższej jakości usług i produktów, a nabywca Cellnez Telecom jako operator infrastruktury jest odpowiedzialny za dostarczenie zamówionej pojemności sieciowej w sposób najbardziej efektywny kosztowo.

Artykuł z wirtualnemedi.pl pt: „Play sprzedał infrastrukturę pasywną za 6,7 mld zł., z którego wynika, że P4 sp. z o.o. sprzedał infrastrukturę ok. 7 tys. wież sieci Play za 6,7 mld zł. Jednocześnie P4 zawarł z On Tower Poland umowy serwisowe na okres 20 lat z możliwością przedłużenia na kolejne okresy dziesięcioletnie, na podstawie których spółka będzie nadal korzystać ze sprzedanej w ramach tej transakcji infrastruktury pasywnej na potrzeby swojej działalności telekomunikacyjnej.

Opracowanie eksperckie mgr inż. P.Z. , z którego wynika, że:

Techniki komunikacji radiowej wykorzystywane w IoT:

Tradycyjne systemy telekomunikacyjne zaprojektowane z myślą o człowieku jako odbiorcy, takie jak połączenia wykorzystujące istniejące sieci komórkowe (GPRS, UMTS, LTE), rozwiązania WiFi, RF Mesh, a nawet łączność satelitarna, mają pewne wady, czy to ze względu na złożoność techniczną ich wdrożenia, brak interoperacyjności i wystarczającego zasięgu, szczególnie w pomieszczeniach, czy też z powodu wysokich kosztów instalacji i/lub konserwacji. Tym nie mniej te techniki radiowe często wykorzystywane są w rozwiązaniach lokalnych, obsługujących stosunkowo niewielką ilość urządzeń na ograniczonym obszarze (np. w budynkach) lub w miejscach geograficznie trudno dostępnych (systemy satelitarne).

Dlatego opracowano i udostępniono na rynku, w tym również w Polsce, dedykowane dla potrzeb 10T metody komunikacji radiowej, stosowane szczególnie w dużych i rozproszonych geograficznie systemach [OT, które można podzielić na:

wykorzystujące pasmo radiowe objęte rezerwacją częstotliwości, np. NB-IoT, czy Cat-M,

wykorzystujące otwarte (wskazane dla tego celu w przepisach prawa) pasmo radiowe, np. LoRaWAN, czy SigFox.

Powyższe techniki komunikacji, określane jako LPWAN (Low Power Wide Area Network), posiadają trzy podstawowe wspólne cechy:

niskoenergetyczność, czyli maksymalne wydłużenie czasu pracy na baterii połączonych w tym systemie „przedmiotów”

(jest to o tyle istotne, że najczęściej urządzenia końcowe w tych systemach wymagają zasilania lokalnego, zwykle baterijnego, a częsta wymiana baterii jest kosztowna i pracochłonna),  
duży zasięg (pokrycie) działania, umożliwiając także instalację urządzeń w miejscach, w których obecnie z tego względu nie jest to często możliwe (piwnice, szyby windowe, lasy  
wysoka pojemność sieci wspierająca massive IoT.

Charakterystyka technik komunikacji radiowej LPWAN dedykowanych dla IoT:

A. Wykorzystujące pasmo radiowe objęte rezerwacją częstotliwości:

NB-IoT (Narrow Band - Internet of Things) - zestandaryzowana w 3GPP w wydaniu 13 "LTE Advanced Pro" (standard sieci komórkowej) technika komunikacyjna LPWAN, wykorzystująca istniejącą infrastrukturę nadajników LTE (4G), zasadniczo przeznaczona dla stacjonarnych urządzeń, które zarejestrowane są w tej samej komórce sieci. NB-IoT jest wprawdzie częścią systemu komórkowego LTE, jednakże z punktu widzenia technicznego jest to nowa technologia dostępu radiowego (nie ma kompatybilności pomiędzy urządzeniami NB-IoT, a zwykłej sieci LTE). Sieć komórkowa NB-IoT może zostać uruchomiona na bazie istniejącej sieci LTE poprzez aktualizację oprogramowania w sieci operatora, co ma wpływ na koszt i czas jej wdrożenia. NB-IoT jest zaprojektowane dla prostych urządzeń, które nie wymagają wysokich przepływności danych, a także łączą się z siecią stosunkowo rzadko. NB-IoT zapewnia wysoką wydajność energetyczną pod warunkiem, że wysyłane dane są względnie małe (np. krótkie raporty zużycia mediów, przekazanie alarmu, odczyty z sensorów) i raportowane są rzadko (kilka razy na godzinę, lub rzadziej). Podstawowe parametry NB-IoT to:

pasmo częstotliwości LTE 700 — 2100 MHz (w zależności od kanału) objęte rezerwacją częstotliwości, a tym samym konieczność uwzględnienia przez inwestora w kosztach operacyjnych opłat za te częstotliwości, które zawarte są w cenach świadczonych usług przez operatorów telekomunikacyjnych,

konieczność korzystania w systemie [OT z usług oferowanych tylko przez operatorów telekomunikacyjnych, będących dysponentami takiego pasma częstotliwości,

półdupleks (naprzemienne przesyłanie i odbieranie danych),

opóźnienie: 1,5 — 10 s, prędkość przesyłania danych < 250 kb/s,

jedna komórka sieci obsługuje 50 -100 tys. urządzeń,

zasięg od nadajnika (LTE): 2-8 km w obszarze zurbanizowanym i do 20 km w otwartej przestrzeni,

dobra penetracja przeszkód takich jak ściany (możliwość instalowania urządzeń na niskich kondygnacjach budynków),

uwierzytelnienie i szyfrowanie: zabezpieczenia oparte na tokenizacji i ochrona interfejsu radiowego. Szczegóły zgodne z LTE definiuje 3GPP,

publiczny model sieci, opłaty za korzystanie z systemu pobierane przez operatorów telekomunikacyjnych sieci komórkowych (rozbudowa lub uruchomienie kolejnych usług IoT wymaga zakupu dodatkowych usług telekomunikacyjnych od tego samego operatora),

ze względu na okres rozwojowy dosyć wysoki koszt zakupu modułów radiowych, możliwość rozbudowy sieci transmisji uzależniona od aktualnych możliwości technicznych operatora telekomunikacyjnego dostarczającego system [OT (ze względu na duże rozmiary stacji bazowych oraz potrzebę uwzględnienia wymogów środowiskowych w trakcie budowy takich stacji bazowych, często wymaga to odpowiedniego czasu, a w niektórych przypadkach jest niemożliwe lub nieopłacalne dla operatora).

CAT-M (Category-M) często nazywana także eMTC (Enhanced Machine-Type Communication) lub LTE-M (Long Term Evolution for Machines), podobnie jak NB-IoT została zestandaryzowana w 3GPP Release 13 oraz działa w oparciu o istniejącą sieć LTE (4G), jednak nie jest rozpatrywana jako osobna technika dostępu radiowego. Wykorzystuje specjalną kategorię terminala sieci LTE, który ma uproszczoną budowę i ograniczone możliwości względem innych kategorii występujących w LTE. Główna różnica to obsługiwana szerokość pasma (1,4 MHz lub 5 MHz), względem standardowych 20 MHz. Do uruchomienia Cat-M w sieci operatora wystarczająca jest aktualizacja oprogramowania na stacjach bazowych i niektórych urządzeniach sieci szkieletowej.

Cat-M jest standardem przeznaczonym głównie dla tanich urządzeń mobilnych z małymi wymaganiami na przepływność danych (poniżej 1 Mb/s). CAT-M w stosunku do NB-IoT charakteryzuje się z jednej strony mobilnością i większą prędkością przesyłania danych, ale z drugiej strony gorszą przenikalnością sygnału przez przeszkody, większym opóźnieniem i gorszą wydajnością energetyczną.

Podstawowe parametry CAT-M to:

pasmo częstotliwości LTE 700 — 2100 MHz (w zależności od kanału) objęte rezerwacją częstotliwości, a tym samym konieczność uwzględnienia przez inwestora w kosztach operacyjnych opłat za te częstotliwości, które zawarte są w cenach świadczonych usług przez operatorów telekomunikacyjnych,

konieczność wykorzystywania w systemie [OT dedykowanego terminala LTE operatora będącego dysponentem

pasma z tego zakresu częstotliwości,

pełny duplex lub półduplex,

opóźnienie 10 — 15 ms,

prędkość przesyłania danych < 1 Mb/s,

szybkie przełączanie pomiędzy komórkami sieci,

możliwość przesyłania głosu (technologia VoLTE),

uwierzytelnienie i szyfrowanie: zabezpieczenia oparte na tokenizacji i ochrona interfejsu radiowego.

Szczegóły zgodne z LTE definiuje 3GPP,

publiczny model sieci, opłaty za korzystanie z systemu pobierane przez operatorów telekomunikacyjnych sieci komórkowych (rozbudowa lub uruchomienie kolejnych usług [OT wymaga zakupu dodatkowych usług telekomunikacyjnych w postaci terminali, kart SIM od tego samego operatora),

możliwość rozbudowy sieci transmisji uzależniona od aktualnych możliwości technicznych operatora telekomunikacyjnego dostarczającego system IoT (ze względu na duże rozmiary stacji bazowych oraz potrzebę uwzględnienia wymogów środowiskowych w trakcie budowy takich stacji bazowych, często wymaga to odpowiedniego czasu, a w niektórych przypadkach jest niemożliwe lub nieopłacalne dla operatora).

B. Wykorzystujące otwarte (dedykowane przepisami prawa ) pasmo radiowe:

LoRaWAN (Long Range Wide Area Network) stworzona i rozwijana przez konsorcjum non-profit LoRa Alliance (skupiające ponad 500 firm członkowskich, w tym globalnych operatorów telekomunikacyjnych), jako standard wykorzystujący pasma częstotliwości ISM poniżej 1 GHz. W przypadku zastosowań IOT takie pasmo częstotliwości jest najlepszym wyborem do komunikacji na duże odległości, ponieważ zapewnia wysoką wydajność urządzeń radiowych w stosunku do ich niewielkich rozmiarów. LoRaWAN wykorzystuje technikę modulacji bezprzewodowej opartą na technologii CSS (ang. Chirp Spread Spectrum). Taka modulacja jest niezwykle odporna na zakłócenia i może być odbierana na dużych odległościach w zależności od możliwości sprzętowych.

Architektura sieci LoRaWAN bazuje na topologii gwiazdy, której bramki zapewniają transmisję pomiędzy urządzeniami końcowymi, a serwerem centralnym, przy czym specyfikacja tego standardu ze względu na jego otwartość, umożliwia bezproblemową integrację z urządzeniami innych producentów. Zastosowania LoRaWAN są w zdecydowanej większości takie same jak NB-IoT. Podstawowe parametry LoRaWAN to:

pasmo częstotliwości otwarte — wskazane dla tego celu w przepisach prawa (w Europie system ten pracuje w paśmie 433 lub 868 MHz), brak konieczności uwzględnienia kosztów opłat za częstotliwości w realizacji usług,

prędkość przesyłania danych < 50 kb/s,

opóźnienie: od kilku do kilkudziesięciu sekund,

półduplex (naprzemienne przesyłanie i odbieranie danych),

zasięg do 5 km w obszarze zurbanizowanym i do 15 km w otwartej przestrzeni,

uwierzytelnienie i szyfrowanie: dwie warstwy zabezpieczeń,

• jedna na poziomie sieciowym, druga na poziomie aplikacji. Klucze i szyfrowanie - algorytm AES 128,

otwarta technologia, brak opłat za korzystanie z częstotliwości,

ze względu na dłuższy rozwój w porównaniu do komórkowych odpowiedników, obecnie znacznie niższe koszty zakupu modułów radiowych,

możliwość szybkiej rozbudowy sieci ze względu z jednej strony na niewielkie rozmiary bramek (stacji bazowych) oraz nieznaczne ich oddziaływanie na środowisko, a z drugiej strony niezależność od aktualnych możliwości technicznych operatora sieci radiowej (w przypadku LoRaWAN inwestor jest właścicielem całej infrastruktury systemu [OT).

SigFox jest technologią radiową działającą podobnie do LoRaWAN w otwartych pasmach radiowych [SM poniżej 1 GHz. Jest to standard częściowo zamknięty, a jego właściciel buduje własne sieci dostępne samodzielnie lub na zasadzie partnerstwa z lokalnymi operatorami (bramki i infrastruktura transmisyjna, ogólnie rzecz biorąc są obsługiwane przez Sigfox), co wymaga wnoszenia przez użytkowników niewielkich stałych opłat miesięcznych za każde zainstalowane urządzenie w sieci IoT (czujnik, licznik, itp.). Ze wszystkich powyżej opisanych standardów bezprzewodowych [OT jest to standard o najmniejszych możliwościach transmisyjnych. Można wysłać do 6 komunikatów na godzinę, każdy zawierający do 12 bajtów danych. Zastosowanie SigFox to przede wszystkim bardzo proste urządzenia typu czujniki, czy też tagi geolokalizacyjne.

Podstawowe parametry SigFox to:

pasmo częstotliwości otwarte — wskazane dla tego celu w przepisach prawa (w Europie system ten pracuje w paśmie 868 MHz), prędkość przesyłania danych < 100 b/s, opóźnienie: od kilku do kilkudziesięciu sekund,

nie ma możliwości dwustronnej komunikacji,

zasięg do 10 km w obszarze zurbanizowanym i do 50 km w otwartej przestrzeni, uwierzytelnienie i szyfrowanie:

symetryczny algorytm szyfrowania AES 128, identyfikacja i uwierzytelnienie pomiędzy urządzeniem KOT, a stacją bazową, technologia tylko częściowo otwarta, brak opłat za korzystanie z częstotliwości, ale występują stałe niewielkie opłaty za każde urządzenie włączone do sieci IoT operatora, niewielki koszt zakupu modułów radiowych, możliwość dosyć szybkiej rozbudowy sieci przez inwestora ze względu na opcję wykorzystania sieci radiowej każdego operatora telekomunikacyjnego, przy czym w tym przypadku inwestor nie jest właścicielem całego systemu [OT].

Opiniujący zamieścił porównanie parametrów technik komunikacji radiowej LPWAN dedykowanych dla 10T:

LoRaWAN vs. NB-10T / Cat-M

Podsumowując:

- NB-IoT, czy Cat\_M mogą być lepszym wyborem dla aplikacji wymagających częstej komunikacji (np. systemy bezpieczeństwa), krótszych opóźnień lub większych ilości danych, podczas gdy LoRaWAN i SigFox będą lepsze w zamierzeniach wymagających niższych kosztów wdrożenia, a przede wszystkim późniejszego utrzymania, dłuższej żywotności baterii i rzadszej wymaganej komunikacji między „przedmiotami”.

Jeśli chodzi o zasięg działania sieci to w przypadku NB-IoT czy Cat-M oczywistą zaletą jest to, że wdrożenie systemu [OT można zapewnić poprzez modernizację istniejących obiektów sieciowych infrastruktury radiowej operatora telekomunikacyjnego, ale po pierwsze jest ona ograniczona tylko do stacji bazowych z urządzeniami 4G/LTE, a po drugie użytkownik systemu IOT uzależniony jest w tym przypadku od zamiarów inwestycyjnych operatora takiej infrastruktury. W przypadku LoRaWAN bramki sieci budowane są przez inwestora takiego rozwiązania w lokalizacjach niezbędnych dla osiągnięcia zamierzonego dla danego zastosowania zasięgu, a w razie potrzeby mogą być elastycznie rozbudowywane (ze względu na niewielkie wymiary do ich umieszczenia można wykorzystać istniejące budynki, czy obiekty budowlane). W przypadku SigFox praktycznie całą infrastrukturę dostarcza operator, ale w zamian pobiera stałą opłatę za korzystanie z sieci.

Z wyników szczegółowych badań wykonanych przez zespół niezależnych naukowców (Analiza zużycia energii przez technologie LPWAN i szacowanie żywotności aplikacji IoT, opublikowana w 2020r.) wynika, że LoRaWAN ma lepszą efektywność zużycia energii przy wydłużonej żywotności baterii w porównaniu do NB-IoT, z zastrzeżeniem że zużycie energii w dużej mierze zależy od rodzaju wybranego sprzętu i podłączonych urządzeń peryferyjnych (np. czujniki, liczniki pomiarowe) jak i warunków środowiskowych, w których urządzenia takie są zainstalowane oraz częstotliwości przekazywania danych (długość okresów uśpienia, czy bezczynności urządzeń peryferyjnych).

W zakresie bezpieczeństwa transmisji w tym cyberbezpieczeństwa NB-IoT, czy Cat-M wykorzystują szyfrowanie standardu LTE, oparte na tokenizacji i ochronie interfejsu radiowego ale również LoRaWAN zapewnia bezpieczeństwo transmisji, wprowadzając oparte o algorytm AES 128b szyfrowanie typu end-to-end przy użyciu klucza sieciowego i aplikacji (dwie warstwy zabezpieczeń, jedna na poziomie sieciowym, druga na poziomie aplikacji, w celu zachowania integralności danych), a SigFox wykorzystuje algorytm szyfrowania AES 128 do identyfikacji i uwierzytelnienia pomiędzy urządzeniem [OT, a stacją bazową.

Należy zauważyć, że oferowany przez wszystkie wyżej opisane technologie poziom cyberbezpieczeństwa jest wysoki, szczególnie biorąc pod uwagę potrzeby przeciętnego użytkownika systemów IOT oraz często niewielką wrażliwość przesyłanych danych, np. informacja o zajętości miejsc parkingowych w systemach nadzoru parkingów.

Porównanie graficzne parametrów technologii: LoRaWAN vs. NB-IoT:

Battery Life- żywotność baterii

Cost Efficiency- efektywność kosztowa

Geolocation- geolokalizacja

Latency- opóźnienie

Security- bezpieczeństwo

Throughput- wydajność

Coverage- pokrycie (zasięg)

Bandwidth- przepustowość łącza

Podsumowanie:

Analizując kwestię równoważności technologicznej dla różnych metod komunikacji radiowej LPWAN dedykowanych dla potrzeb IoT, należy wziąć pod uwagę wiele czynników, takich jak:

koszt węzła, koszt sieci, koszt utrzymania (OPEX), wydajność energetyczna systemu (żywotność baterii zasilających urządzenia końcowe), prędkość transmisji danych, opóźnienie, mobilność, liczba obsługiwanych urządzeń („przedmiotów”), zasięg sieci, bezpieczeństwo, typ wdrożenia (sieć publiczna, prywatna).

Można z dużą dozą pewności powiedzieć, że żadna z obecnie stosowanych technologii nie jest w stanie zaspokoić w pełni wszystkich potrzeb użytkowników IOT (nie ma technologii [OT uniwersalnej). NB-IoT, Cat-M i LoRaWAN mają różne cechy techniczne i handlowe, jednak w bardzo wielu przypadkach parametry techniczne, w tym transmisyjne każdej z nich są wystarczające dla obecnych, a nawet przyszłych potrzeb inwestorów.

Z doświadczenia wynikającego z obserwacji zrealizowanych w niedalekiej przeszłości różnych projektów telekomunikacyjnych można - szczególnie w przypadku inwestycji sektora publicznego — wysnuć wniosek, że wiele z nich zostało wykonanych ze znaczącą, nigdy nie wykorzystaną nadmiarowością (sprzętu lub funkcjonalności systemu) w stosunku do rzeczywistych . potrzeb danego inwestora. Związane to było w dużej mierze z niewielkim obciążeniem początkowym inwestorów kosztami zakupu i wdrożenia systemu

(wysokie dotacje bezzwrotne z budżetu państwa i dotacji unijnych), co wpływało na akceptacje rozwiązań przedstawianych przez ich dostawców (vendorów), którzy oczywiście byli zainteresowani sprzedażą jak naj bardziej technologicznie, a zatem zazwyczaj drożych produktów. Zasadniczo w interesie kupującego jest nabycie produktu/usługi o jak najlepszych parametrach, ale w tym przypadku inwestorzy (szczególnie jednostki samorządu terytorialnego) spotkali się z bardzo bolesnym problemem, związanym z wysokimi i trudnymi do akceptacji kosztami utrzymania i ewentualnej rozbudowy takich systemów po zakończeniu okresu gwarancyjnego.

Standardy LoRaWAN i SigFox jak i NB-IoT, oraz Cat-M zostały zaprojektowane w celu zwiększenia efektywności energetycznej, bezpieczeństwa i interoperacyjność urządzeń [OT, a więc spełnienia kluczowych potrzeb w dziedzinie Internetu Rzeczy. Jednak sam wybór jednej z tych technologii nie gwarantuje jeszcze sukcesu takiej inwestycji. Skuteczność działania systemu [OT zależy zasadniczo od tego, jak dany system zostanie zaprojektowany, zbudowany i w końcu wdrożony. Odpowiedni dobór komponentów, sprzętu i oprogramowania, ale także opracowanie właściwego scenariusza działania całego systemu (np. częstotliwości przekazywanych przez czujniki systemu danych), jest kluczowy dla zapewnienia jego wydajności i niezawodności. Wadliwe zaprojektowanie i wykonanie takiego systemu może prowadzić do awarii, przestojów i kosztownych napraw.

Wdrożenie kompletnego systemu IOT wymaga więc z jednej strony rozpoznania wymogów projektu, a z drugiej strony odpowiedniego doboru parametrów technicznych, konfiguracji urządzeń, optymalizacji sieci oraz przetestowania działania systemu w rzeczywistych warunkach. Po wdrożeniu, nie można zapominać o stałym monitorowaniu prawidłowości działania tego systemu.

Przy czym z punktu widzenia realizacji zadań, dotyczących monitorowania różnego rodzaju parametrów, czy zbierania i przekazywania niewielkich ilości danych z umiarkowaną częstotliwością przez urządzenia IoT, rozmieszczone w wielu odległych geograficznie lokalizacjach, wszystkie opisane wyżej metod komunikacji radiowej LPWAN dedykowane dla potrzeb IoT są w stosunku do siebie w dużym zakresie równoważne. Zapewniają odpowiednią jakość i bezpieczeństwo przesyłanych danych, efektywność energetyczną (długą żywotność baterii zasilających urządzenia końcowe) oraz wymagany zasięg działania.

Przewaga konkurencyjna dostawców takich systemów powinna być budowana - według opinii eksperta — przede wszystkim w oparciu o zapewnienie przez dostawcę gwarancji terminowego przekazywania przez system IOT wymaganego zakresu danych, na poziomie jakości akceptowalnym przez inwestora (SLA), co w umowach na realizację takiego systemu powinno być zabezpieczone stosownymi karami umownymi (szczególnie w przypadku zamówień publicznych), a także cenę, warunki dostaw, w tym zakresu udzielonej gwarancji na dostarczane systemy. Z pewnością istotną sprawą jest posiadanie przez dostawcę pozytywnej opinii o systemie wydanej przez użytkowników podobnych w skali i zakresie technicznym rozwiązań, potwierdzonej referencjami.

Warto w tym miejscu zacytować także i wziąć pod uwagę konkluzję z raportu grupy roboczej ds. Internetu Rzeczy przy Ministerstwie Cyfryzacji — „KOT w polskiej gospodarce”<sup>3</sup> . „Projekty takie powinny wspierać możliwość dywersyfikacji dostawców, aby nie doprowadzić do zjawiska monopolizacji dla dostawcy rozwiązania w nowej technologii, które zamiast stymulować innowacyjność i rozwój. konserwują rynek na lata. Kluczem do rozwoju IoT w Polsce jest otwartość standardów, rozumiana jako pełna jawność metod wymiany danych na wszystkich warstwach gwarantowana ustawowo. W modelu tym, każde wdrożenie IoT wymagałoby dostarczenia zarówno samego rozwiązania jak i kompletnej jawnej dokumentacji dla zamawiającego wraz z wymogiem dostępności dla innych podmiotów. Takie podejście da praktycznie nieograniczone możliwości integracji zarówno dla małych projektów lokalnych jak i ogólnokrajowych i będzie stymulatorem innowacyjności, łączenia heterogenicznych rozwiązań. Jawność przełoży się także na poziom bezpieczeństwa, który wzrasta w systemach o otwartym dostępie do protokołów, gdzie bezpieczeństwo bazuje na przyjętych metodach kryptograficznych a nie „tajności protokołu”.

Dowody odwołującego dołączone do pisma złożonego na rozprawie z:

— raportu z pomiarów pasma LoRaWAN 868 MHz, przeprowadzonych na terenie miasta Katowice (tajemnica przedsiębiorstwa, z którego wynika, że przeprowadzony proces pomiarów i analizy porównawczej nie wykazał przeszkód uniemożliwiających działanie systemu Smart City w technologii LoRaWAN w Katowicach na poziomie SLA wymaganym przez zamawiającego,

- karty katalogowej stacji bazowej LoRaWAN firmy Kerlink Wirnet iStation, oraz prezentacji sprzedażowej polskiego dystrybutora urządzeń Kerlink spółki JM elektronik Sp z o.o. z dowodu wynika, że jest to brama LoRaWAN spełniająca standardowe wymagania operatorów publicznych, operatorów MVNO, operatorów kablowych, przedsiębiorstw

prywatnych czy jednostek administracji publicznej chcących rozwijać swoją działalność w oparciu o IoT oraz wdrażać elastyczne i niezawodne sieci, obsługiwać duże wolumeny urządzeń końcowych i zarządzać milionami dwukierunkowych komunikatów każdego dnia. Łączność backhaul moduł 4 G obsługujący częstotliwości na całym świecie z możliwością przełączenia na 3G/2G oraz port Ethernet (RJ45), w pełni zintegrowane, wewnętrzne anteny: GPS, 4G, LoRa. Wbudowane filtry o wysokim tłumieniu pozwalające na współistnienie z innymi urządzeniami radiowymi i zapewniające wysoką odporność na zakłócenia, Zapewnia wysoki poziom bezpieczeństwa dzięki innowacyjnej architekturze sprzętowej i programowej oraz integracji rozwiązań Prove&Run SecureBoot i Secure Storage

- Decyzji Wykonawczej Komisji (UE) 2019/1345 z dnia 2 sierpnia 2019 r. zmieniającej decyzję 2006/771/WE w sprawie aktualizacji zharmonizowanych warunków technicznych w zakresie wykorzystania widma radiowego na potrzeby urządzeń bliskiego zasięgu (notyfikowana jako dokument nr C(2019) 5660, Tekst mający znaczenie dla EOG). Urządzenia bliskiego zasięgu to zazwyczaj przeznaczone dla masowego odbiorcy lub przenośne urządzenia radiowe, które można łatwo przewozić za granicę i stosować w komunikacji transgranicznej. Zróżnicowanie warunków dostępu do widma stwarza ryzyko szkodliwych zakłóceń w stosunku do innych zastosowań i usług radiowych, uniemożliwia swobodny przepływ tego rodzaju urządzeń oraz powoduje wzrost kosztów ich produkcji.

»urządzenie bliskiego zasięgu« oznacza urządzenie radiowe, które zapewnia łączność jednokierunkową lub dwukierunkową i za pomocą którego prowadzi się odbiór lub nadawanie na bliską odległość i z małą mocą;

»na zasadzie niepowodowania zakłóceń i braku ochrony przed zakłóceniami« oznacza niepowodowanie żadnych szkodliwych zakłóceń w odniesieniu do wszelkich służb radiokomunikacyjnych oraz brak możliwości ubiegania się o ochronę urządzeń, których to dotyczy, przed zakłóceniami wytwarzanymi przez służby radiokomunikacyjne.”;

84:

863–868 MHz Urządzenia do szerokopasmowej transmisji danych

25 mW e.r.p. Stosuje się wymogi dotyczące technik dostępu do widma oraz osłabiania zakłóceń [7]. Szerokość pasma: > 600 kHz i ≤ 1MHz.

Maksymalny poziom aktywności nadajnika: ≤ 10 % w przypadku punktów dostępu do sieci [g].

Maksymalny poziom aktywności nadajnika: ≤ 2,8 % w pozostałych przypadkach.

Niniejsze warunki wykorzystania dotyczą tylko urządzeń bliskiego zasięgu do szerokopasmowej transmisji danych w sieciach danych [g].

1 stycznia 2018 r.

47:

865–868 MHz Urządzenia bliskiego zasięgu ogólnego stosowania

25 mW e.r.p. Stosuje się wymogi dotyczące technik dostępu do widma oraz osłabiania zakłóceń [7].

Alternatywnie można stosować maksymalny poziom aktywności nadajnika wynoszący 1 %.

1 stycznia 2020 r.

47b: 865–868 MHz Urządzenia bliskiego zasięgu ogólnego stosowania

500 mW e.r.p. Transmisje dozwolone wyłącznie w zakresach częstotliwości 865,6–865,8 MHz, 866,2–866,4 MHz, 866,8–867,0 MHz i 867,4–867,6 MHz. Wymagane jest adaptacyjne sterowanie zasilaniem. Ewentualnie inna technika osłabiania zakłóceń o co najmniej równoważnym poziomie zgodności widma.

Stosuje się wymogi dotyczące technik dostępu do widma oraz osłabiania zakłóceń [7].

Szerokość pasma: ≤ 200 kHz.

Maksymalny poziom aktywności nadajnika: ≤ 10 % w przypadku punktów dostępu do sieci [g].

Maksymalny poziom aktywności nadajnika: ≤ 2,5 % w pozostałych przypadkach.

Niniejsze warunki wykorzystania dotyczą tylko sieci danych [g].

1 stycznia 2018 r.

868–868,6 MHz Urządzenia bliskiego zasięgu ogólnego stosowania 25 mW e.r.p. Stosuje się wymogi dotyczące technik dostępu do widma oraz osłabiania zakłóceń [7].

Alternatywnie można stosować maksymalny poziom aktywności nadajnika wynoszący 1 %.

1 stycznia 2020 r.

- dokumentu publikacji naukowej N.A. „The ALOHA System — Another alternative for computer communications” (University of Hawaii, 1970) dotyczy formy łączności radiowej typu random-access opracowanej do zastosowania w ramach systemu Aloha System Aloha system planuje połączyć interaktywnych użytkowników komputerów oraz urządzenia wejścia/wyjścia zdalnego dostępu znajdujące się poza głównym kampusem z centralnym komputerem za pomocą kanałów radiowych UHF. Ma być to alternatywa dla tradycyjnej komunikacji przewodowej, przy czym wskazano, że metoda random access communications pozwala każdej konsoli korzystać ze wspólnego szybkiego kanału danych

bez konieczności stosowania centralnego sterowania lub synchronizacji, może ona generować dwójakiego rodzaju błędy – losowe wynikające z szumu i spowodowane interferencją z pakietem nadanym w tym samym czasie przez inną konsolę, co wymusza potrzebę retransmisji i staje się istotny dopiero, gdy duża liczba użytkowników próbuje korzystać z kanału jednocześnie. Te błędy ograniczają liczbę użytkowników oraz ilość danych jakie mogą być przesyłane przez taki kanał dostępu losowego. Opracowanie zawiera także wyliczenia maksymalnej ilości użytkowników interaktywnych, których system jest w stanie obsłużyć.

- wykazu rezerwacji ogólnopolskich Prezesa UKE (plik „2025-08-01 \_rezerwacje\_cala\_pl.xlsx”, stan na 01.08.2025 r.)

Pasmo 700 MHz do 31 maja 2040 posiadają T-Mobile, Orange Polska, Polkomtel, P4 pasmo 800 MHz posiadają do 25 stycznia 2031 lub 23 czerwca 2031 lub do 31 maja 2031 Orange Polska, P4, T-Mobile, pasmo 900 MHz posiadają Polkomtel - i P4 do 31.12.2038, Polkomtel i T-Mobile 24, 26.02.2026, Orange Polska – 06.07.2029

- wydruków ze stron internetowych oraz materiałów Urzędu Komunikacji Elektronicznej:

„Pierwsi klienci Orange mogą już korzystać z 5G w paśmie 700 MHz” — opublikowanej w serwisie Orange Polska (biuroprasowe.orange.pl), z którego wynika że Orange uruchomił pierwsze 45 stacji bazowych w częstotliwości 700 MHz dla dostępu technologii 5G

„T-Mobile 5G w paśmie 700 MHz” — opublikowanej w serwisie Benchmark.pl (benchmark.pl), z którego wynika, że T-Mobile to pierwszy operator w Polsce, którego sieć 5G działa w niskim paśmie 700 MHz, to pasmo pozwala pokryć kilkakrotnie większy obszar niż te z zakresu 3,4 GHz. Pasma 700 MHz dotychczas było zajęte przez telewizję cyfrową DVB-T

Prezentacji Urzędu Komunikacji Elektronicznej pt. „Aukcja pasm 700 i 800 MHz” (plik PDF opublikowany na stronice UKE załączony do akt sprawy),

Prezentacji UKE pt. „Aukcja pasm 700 i 800 MHz” (plik PDF opublikowany na stronice UKF., załączony do akt sprawy), pierwotna kalkulacja ceny – cena wywoławcza 580 mln zł za blok 700 MHz, 635 mln zł za blok 800 MHz i 356 mln zł. za blok 700/800 MHz

- z systemu z opisem skuteczności odczytów 50 nakładek w trybie 28 dni”, obejmującego slajd zatytułowany „Skuteczność odczytów”, sporządzonego po zakończeniu pilotażowego wdrożenia technologii LoRaWAN przez Emitel S.A. w aglomeracji katowickiej w 2023 roku, z którego wynika skuteczność w okresie 28 dni przewyższająca miesięczne wymagania SLA w spornym postępowaniu

- informacja o wyborze oferty najkorzystniejszej w postępowaniu na zakup i wymianę wodomierzy oraz stacjonarny odczyt wskazań wodomierzy w latach 2025-2030 ZWIK Grodzisk Mazowiecki, z którego wynika, że wybrano AQUARD spółka z ograniczoną odpowiedzialnością,

- informacja z otwarcia ofert z Łubianki na zakup i montaż wodomierzy wraz z modułami do zdalnego odczytu radiowego w ilości 1350 szt wraz z niezbędną infrastrukturą – oferty złożyli WES spółka z ograniczoną odpowiedzialnością i GlobTree spółka z ograniczoną odpowiedzialnością, SWZ Miasta i Gminy Piekoszów na modernizację infrastruktury wodno-kanalizacyjnej na terenie gminy Piekoszów część 1 instalacja wodomierzy u odbiorców z systemem zdalnego odczytu wraz z informacją z otwarcia ofert, gdzie ofertę na część 1 złożył METERING Anna Moder z Buczka oraz informacją o wyborze tej oferty jako najkorzystniejszej,

- informacji z otwarcia ofert na dostawę nakładek i systemu do stacjonarnych odczytów wodomierzy na terenie Chorzowa i Świętochłowic, gdzie ofertę złożyła firma AIUT sp. z o.o.

- SWZ Przedsiębiorstwa Komunalnego Wronki spółka z ograniczoną odpowiedzialnością na system zdalnego odczytu wodomierzy, gdzie przedmiotem jest dostawa i wdrożenie systemu do zdalnego odczytu wodomierzy z wykorzystaniem technologii radiowej. Dane z nakładek na wodomierze odczytywane będą za pośrednictwem koncentratorów i przesyłane dalej za pośrednictwem sieci komórkowej do systemu informatycznego, a w miejscach gdzie koncentratory nie będą zainstalowane bądź gdzie zasięg koncentratorów nie będzie wystarczający odczyty będą dokonywane zdalnie przez inkasentów wyposażonych w terminale inkasenckie. Urządzenia do zdalnego odczytu stanu wodomierzy muszą spełniać wymagania m. in. oprócz możliwości komunikacji z terminalami inkasenckimi muszą równolegle posiadać możliwość komunikacji z bramami/koncentratorami za pośrednictwem ustandaryzowanej technologii do przesyłu danych typu LoRa (lub innej równoważnej, ustandaryzowanej o tej samej lub lepszej efektywności komunikacji)

- informacją z otwarcia ofert w postępowaniu na usługę wdrożenia i utrzymania systemu sterowania i zarządzania oświetleniem na terenie m. st. Warszawy, gdzie oferty złożyli, odwołujący, konsorcjum Orange Polska-Schreder Polska-Lumiqon, Pollight, Deloitte Consulting wraz z OPZ dla usługi, z którego wynika, że zamawiający dopuszcza sieć typu mesh, mesh/hybryda lub jednolitą sieć na pasmach komercyjnych, która to rzez cały czas trwania umowy umożliwi zamawiającemu rozwój, optymalizację usług oraz dwukierunkową komunikację w czasie rzeczywistym

- artykułu „LoRaWAN@ jest bezpieczny (ale implementacja ma znaczenie)” (oryg. „LoRaWAN@ Is Secure (but Implementation Matters)”), opublikowanego przez LoRa Alliance i dostępnego pod adresem: <https://rcsources.loraalliancc.org/security/lorawan-is-secure-but-implementation-matters>, wraz z tłumaczeniem na język

polski, z którego wynika, że LoRaWAN z założenia jest bardzo bezpieczny – uwierzytelnianie i szyfrowanie są w nim obowiązkowe – jednak sieci i urządzenia mogą zostać skompromitowane, jeśli klucze bezpieczeństwa nie są odpowiednio chronione, nie są losowo generowane dla poszczególnych urządzeń lub jeśli liczby kryptograficzne używane jednokrotnie (nonce) są ponownie wykorzystywane. Dlatego tak istotne jest wybieranie urządzeń z certyfikatem LoRaWAN CertifiedCM, aby mieć pewność, że sprzęt został przetestowany zgodnie ze standardem i działa zgodnie z oczekiwaniami. Specyfikacja definiuje dwie warstwy kryptografii:

- unikalny 128 bitowy klucz sesji sieciowej współdzielony między urządzeniem końcowym, a serwerem sieciowym
- unikalny 128 bitowy klucz sesji aplikacji (AppSKey) współdzielony end-to-end na poziomie aplikacji. LoRa WAN posiada wszystkie fundamentalne elementy stosowane przez każdą nowoczesną technologię komunikacji bezprzewodowej i to przy sile szyfrowania AES – 128. Opracowano:

- interfejsy backend LoRaWAN, które izolują przechowywanie kluczy głównych w serwerze join

- rozwiązania typu secure element, które zapewniają dodatkową ochronę sprzętową przed manipulacjami fizycznymi

- artykułów naukowych opublikowanych na platformie ResearchGate, które wskazują na podatności technologii komórkowych NarrowBand IoT (NB-IoT) oraz LTE Cat-M takie jak słabe zabezpieczenie aplikacji i punktów końcowych, niewystarczająca autoryzacja/uwierzytelnianie, brak bezpieczeństwa fizycznego, nadmierna ilość danych wrażliwych, niezabezpieczone domyślne dane logowania. Autorzy wskazują środki zaradcze: traktowanie bezpieczeństwa urządzeń i aplikacji IoT jako priorytetu, zapewnienie uwierzytelniania i autoryzacji w urządzeniach inteligentnych podłączonych do IoT, priorytet dla bezpieczeństwa danych przekazywanych między urządzeniami, wprowadzenie systemu monitorowania nadzorującego ekosystem, wdrożenie wielowarstwowego systemu ochrony dla systemu IoT oraz z drugiego artykułu o nowych atakach wykorzystujących niechronione sygnalizacje w płaszczyznach danych w komórkowych sieciach IoT (tj. NB-IoT oraz cat-M). Mimo wdrożonych mechanizmów bezpieczeństwa zarówno dla sygnalizacji w płaszczyźnie sterowania jak i przekazywania pakietów w płaszczyźnie danych, nadal możliwe są nowe ataki w płaszczyźnie danych. Ataki te przybierają różne formy, wykraczające poza proste zakłócanie pakietów i ataki typu odmowa usługi (DoS) obejmując m. in. naruszenie prywatności lokalizacji, zapętlanie dostarczania pakietów, wydłużone dostarczanie danych, ograniczanie przepustowości, wyczerpywanie zasobów radiowych oraz resetowanie połączeń. W artykule omówiono nowe rodzaje ataków i przedstawiono sposoby obrony przed nimi. Aby chronić sygnalizację w płaszczyźnie danych przy niskim koszcie proponuje się wdrożyć rozwiązanie oparte na czasie w warstwie MAC. Wykorzystuje ono zsynchronizowane timery w MAC do generowania kluczy szyfrujących i integralności.

- studium przypadku Cisco CILE, dostępnego również na oficjalnej stronie Cisco pod adresem; w ramach którego zbudowaną własną sieć telekomunikacyjną IoT oszczędzając czas i koszty oraz zapewniając bezpieczeństwo danych przez zwiększenie wydajności operacyjnej, zmniejszenie kosztów prowadzenia działalności i uczyniono operacje bardziej zrównoważonymi. W zadaniu chodziło o zarządzanie wodą przez wgląd w punkty wzdłuż 3 500 kilometrów rur. W opracowaniu wskazano, że powodem budowy własnej sieci był wysoki koszt publicznej sieci komunikacyjnej. Cisco zamontowało 48 anten, które pozwoliły objąć zasięgiem 24 gminy. ! antena pokrywa zasięg 15 km i gromadzi dane z czujników o żywotności baterii 15 lat. Czujniki są zainstalowane co 5 km, aby kontrolować przepływ i wycieki, a także czujniki do pomiaru zużycia wody przez poszczególnych klientów. Wszystkie dane z czujników przepływają przez sieć LoRaWAN do firmowego jeziora danych, gdzie modele danych pomagają analizować dane wejściowe. . Możliwe jest także wykorzystanie sieci do innych zastosowań jak inteligentne opomiarowanie jakości powietrza, inteligentne parkowanie, inteligentne oświetlenie.

- / opublikowanego na oficjalnej stronie Rzeczypospolitej Polskiej — Ministerstwo Spraw Wewnętrznych i Administracji (gov.pl) pt.

„Modernizujemy system alarmowy — ponad 4 tys. lokalizacji z nowoczesnymi syrenami”

(<https://www.gov.pl/wcb/obrona-cywilna/modernizujemy-sys-tem-alarmowy--ponad-4- tys-lokalizacji-z-nowoczesnymi-syrenami>), z którego wynika, że Państwowa Straż Pożarna wdraża nowoczesny system ostrzegania i alarmowania, który obejmie aż 4 060 lokalizacji w całej Polsce. Jednym z kluczowych elementów modernizacji jest wymiana analogowych syren alarmowych na nowoczesne cyfrowe urządzenia. Obecne alarmy uruchamiane są głównie drogą radiową. Nowy system będzie wykorzystywał technologie LoRaWAN, cyfrową łączność radiową DMR oraz GSM, co zwiększy jego niezawodność i zasięg działania. Technologia LoRaWAN umożliwi przesłanie danych na duże odległości przy minimalnym zużyciu energii. Dodatkowo pozwala na integrację z innymi systemami, co oznacza możliwość monitorowania i zarządzania różnymi sensorami w czasie rzeczywistym.

2/z decyzji Prezesa UKE z dnia 8 lipca 2019 roku potwierdzającego że Emitel jest dysponentem infrastruktury krytycznej i ta jest wyłączona obowiązków zapewnienia dostępu telekomunikacyjnego str. 6 decyzji – zakres oferty nie obejmuje infrastruktury i obiektów ujętych w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, dla których właścicielem, posiadaczem samoistnym lub zależnym jest Emitel.

- „End Device Certification Requirements for LoRaWAN 1.0.4” wydanego przez organizację LoRa Alliance, wraz z tłumaczeniem na język polski kluczowych fragmentów dotyczących bezpieczeństwa dokument ten opisuje wdrożone w systemie LoRaWAN rozwiązania pozwalające na podniesienie poziomu bezpieczeństwa przesyłu danych

- dane dotyczące Miasta Wrocławia:

1/ dokumentu pt. Dane Głównego Urzędu Statystycznego (GUS) za 2024 r., Załącznik „Powierzchnia i ludność w przekroju terytorialnym w 2024 roku — tablice”, arkusz Tabl. 2. Powierzchnia, ludność oraz lokaty według powiatów i miast na prawach powiatu.

2. zdjęć zalanych studni wodociągowych wykonanych na terenie miasta Wrocławia

- „Projekt techniczny sieci telekomunikacyjnej LoRaWAN opracowany przez Odwołującego, wykonany w profesjonalnym oprogramowaniu do planowania radiowego przez specjalistów z zakresu telekomunikacji potwierdza stanowisko odwołującego przedstawione na rozprawie, że łączność komórkowa stanowi warstwę umożliwiającą uruchomienie systemu na całym obszarze Katowic, dla pierwszego etapu, równolegle będzie budowana sieć LoRaWAN, która będzie drugą warstwą, to rozwiązanie wynika stąd, że zamawiający wymusza szybkie uruchomienie pokrycia, a pokrycie zasięgiem LoRaWAN jest możliwe w perspektywie dłuższej niż 30 dni. Projekt opisuje sposób przeprowadzenia uruchomienia usługi oraz jej zalety. Zawiera również zrzut z ekranu z oferty Orange Polska dla kart sim IoT oraz kartę katalogową w języku obcym bramy sieciowej.

- artykułu naukowego pt. „LoRaWAN Network: Radio Propagation Models and Performance Evaluation in Various Environments in Lebanon” (IEEE Internet of Things Journal, DOI:

10.1109/JIOT.2019.2906838) — wraz z tłumaczeniem na język polski.

artykułu naukowego pt. „LoRaWAN Network: Radio Propagation Models and Performance Evaluation in Various Environments in Lebanon” (IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2019.2906838) — wraz z tłumaczeniem na język Polski, z którego wynika, że przeprowadzono badania w Libanie zarówno w kampusie uniwersyteckim, jak i w obszarze miejskim i wiejskim i stwierdzono, że LoRaWAN to atrakcyjne rozwiązanie dla komunikacji IoT o niskim zużyciu energii i dużym zasięgu. Charakterystyka kanału radiowego jest kluczowym zagadnieniem w projektowaniu i wdrażaniu systemów komunikacyjnych. Przeprowadzono szeroko zakrojone kampanie pomiarowe w środowisku wewnętrznym, miejskim i wiejskim. Na podstawie pomiarów empirycznych opracowano modele PL. Wykazano, że zaproponowane modele lepiej dopasowują się do pomiarów i są znacznie prostsze w użyciu w obszarach podobnych do Libanu. Ponadto oceniono wydajność LoRaWAN pod kątem PDR i SNR. Uzyskane wyniki pokazują niezawodność tej technologii w praktycznych wdrożeniach. Komunikacja LoRaWAN w rzeczywistych środowiskach na duże odległości:

- w gęsto zabudowanym obszarze miejskim uzyskano zasięg do 9 km, w środowisku wiejskim zasięg do 47km przy użyciu jednej wdrożonej bramy GW. Jakość transmisji w środowisku o silnym cieniowaniu i blokadach (budynki, profil wysokościowy terenu) może zostać poprawiona przez instalację dodatkowych bram GW oraz optymalizację ich lokalizacji.

Wyniki wydajności potwierdziły niezawodność LoRaWAN dla wielu zastosowań IoT takich jak inteligentne miasta, inteligentne rolnictwo.

- 10 umów (zamówień) usług dzierżawy łączy radiowych podpisanych pomiędzy Emitel S.A. a T-Mobile Polska S.A., dokumentujących świadczenie usług transmisji danych w paśmie nielicencjonowanym, z gwarantowanym SLA Tajemnica przedsiębiorstwa)

„Metryka odpowiedzi na wniosek z dnia 21.07.2025 r.” (DK.WKR.0143.3.2025), sporządzonego przez Prezesa Urzędu Komunikacji Elektronicznej i udostępnionego w dniu 1 sierpnia 2025 r., z której wynika, że w okresie ostatnich 3 miesięcy tj. od 21 kwietnia 2025 do 21 lipca 2025 do Urzędu Komunikacji Elektronicznej nie wpłynęły żadne skargi dotyczące funkcjonowania sieci LoRaWAN w pasmach nielicencjonowanych.

Dowody zamawiającego:

Z mapy dzielnic Katowic z uwzględnieniem ilości mieszkańców i trudnych lokalizacji pod względem możliwości stacjonarnego odczytu wodomierzy wynika liczba mieszkańców danej dzielnicy, liczba studni wodomierzowych w danej dzielnicy i liczba trudnych sytuacji i studni w danej dzielnicy, z mapy wynika, że w każdej dzielnicy występują trudne lokalizacje do stacjonarnego odczytu wodomierzy, natomiast nie wynikają informacje, czy występują lokalizacje trudne do odczytu radiowego w paśmie licencjonowanym lub nielicencjonowanym, ani czy te same lokalizacje będą trudne dla nowo budowanego systemu. Sam zamawiający przyznał, że aktualne określenie lokalizacji trudnych dotyczy tych, które okazały się problematyczne dla obecnie funkcjonującego systemu. Dowód ten ma tylko takie znaczenie, że wskazuje na potencjalną możliwość trudności dla systemu z odczytem dla około 10% lokalizacji.

Notatka służbowa sporządzona w dniu 5.12.2024 r. na okoliczność wyboru technologii stacjonarnego odczytu wodomierzy.

W dniu 5.12.2024 r. na spotkaniu dotyczącym podejmowanych działań w zakresie wyboru technologii do stacjonarnego odczytu wodomierzy omówiono wnioski z przeprowadzonych pilotaży.

Sprawdzono skuteczność działania systemów odczytowych i technologii następujących firm:

- GSM (NB-10T/LTE CAT-MI): T-mobile, Orange.
- LoRa: Aiut
- WIZE 169 - AquaRD.

Przeprowadzone testy wykazały, że rozwiązania GSM(NB-10T/LTE CAT-MI) firm T-mobile, Orange, (analogiczne rozwiązanie PlusGSM) są najkorzystniejsze dla potrzeb i uwarunkowań miasta Katowice.

Stacjonarny system odczytu wodomierzy TECHNOLOGIA GSM

- Wykorzystanie istniejącej infrastruktury - Technologie LPWAN (Low Power WAN) takie jak NB-10T oraz LTE CAT-MI korzystają z istniejących sieci komórkowych eliminując potrzebę budowy własnej sieci komunikacyjnej przez Spółkę a w tym:

Kłopoty z wejściem w teren.

Potrzebę wykorzystania elementów urbanistycznych koszty dzierżawy i energii elektrycznej.

Zaangażowanie służb technicznych do obsługi sieci. o Dewastacje i kradzieże. o Aspekt społeczny.

Zasięg — technologie NB-10T oraz LTE CAT-MI cechują się szerokim zasięgiem i dobrą penetracją sygnału pozwalając na pozyskanie odczytu z trudnych lokalizacji tj. piwnice, studzienki wodomierzowe itd.

Niezawodność - dostępność i odporność sieci komunikacyjnej są fundamentalne dla zapewnienia ciągłości przepływu danych. NB-10T jak i LTE CAT-MI korzysta z potencjalnie niezawodnych sieci operatorskich GSM. Dostępna duża ilość BTSów (stacji bazowych) w Katowicach jest gwarantem pokryciem zasięgiem całego miasta.

Skalowalność - system zdolny do obsługi dużej liczby punktów pomiarowych oraz przetwarzania generowanej przez nie objętości danych. NB-10T i LTE CAT-MI zostało zaprojektowane z myślą o masowych połączeniach.

Stabilność i niezawodność - działanie w licencjonowanym paśmie minimalizuje zakłócenia i zapewnia większą skuteczność odczytów.

Bezpieczeństwo - ochrona danych podczas transmisji i przechowywania jest absolutnym priorytetem dla podmiotów kluczowych. Systemy IoT wprowadzają nowe potencjalne wektory ataków. NB-10T oraz LTE CAT-MI wykorzystują najwyższe standardy bezpieczeństwa sieci komórkowych — zgodne z UKSC oraz dyrektywą NIS2.

Żywotność modułów radiowych - czas pracy baterii jest krytycznym czynnikiem, szczególnie dla wodomierzy zainstalowanych w trudno dostępnych miejscach. Technologie takie jak NB-10T i LTE CAT-MI są projektowane pod kątem niskiego zużycia energii, celując w żywotność baterii na poziomie 10 lat lub więcej. Rzeczywista żywotność zależy jednak od czynników takich jak częstotliwość transmisji i warunki środowiskowe.

Konserwacja — korzystanie z sieci komórkowej GSM do transmisji danych niweluje potrzebę konserwacji elementów sieci transmisyjnej.

Standaryzacja - jako standardy 3GPP - NB-10T i LTE CAT-MI są globalnie uznane i standaryzowane, co może ułatwić interoperacyjność i dostępność urządzeń.

Dowody z wyroków KIO sygn. akt KIO 2516/23 i KIO 32/24 KIO potraktowała jako element argumentacji stanowisko zamawiającego, bo w ocenie KIO prawomocny wyrok KIO nie ma skutku erga omnes i jest wiążący jedynie pomiędzy stronami orzeczenia. W żadnym przypadku stroną w tych wyrokach nie był obecny zamawiający. Nadto stany faktyczne częściowo różnią się od stanu faktycznego tej sprawy, zatem również z tego powodu powołane wyroki nie stanowią dowodu w tej sprawie.

Dowody przystępującego T-Mobile:

Wnioski z artykułu „Low-Power Wide-Area Networks: Comparison of LoRaWAN and NB-10T Performance” R.M. , K.M. Senior Member, IEEE, G.P. , Member, IEEE, and C.B.

Opublikowano w: IEEE Internet of Things Journal ( tom: 9 , numer: 21 , 1 listopada 2022 r. )

Strony: 21051 - 21063

Data publikacji: 19 maja 2022 r.

Informacje o ISSN:

DOI: 10.1109/JIOT.2022.3176394

Wydawca: IEEE :

uwzględniając aspekty techniczne, zarówno w warstwie fizycznej (PHY), jak i łącza (Link), a także kwestie regulacyjne. Podsumowując, obie technologie różnią się pod wieloma względami i obie mają mocne i słabe strony. W zależności od konkretnego zastosowania, najlepsze rozwiązanie można zidentyfikować na podstawie powyższych rozważań i wyników numerycznych. Podsumowując, NB-10T implementuje bardziej niezawodny schemat modulacji i kodowania, wraz z wysoce niezawodną warstwą łącza, kosztem większego zużycia energii. Dlatego NB-10T jest bardziej odpowiedni dla aplikacji wymagających niezawodności i przepustowości sieci. Ponadto nie jest ograniczony żadnymi regulacjami dotyczącymi prądu stałego (DC), dzięki czemu urządzenia mogą przesyłać częściej lub większe wolumeny danych. Z

drugiej strony, LoRaWAN jest wygodny w aplikacjach o wysokich wymaganiach dotyczących żywotności (tj. w przypadkach użycia z ograniczoną baterią) i gdzie wymagania dotyczące niezawodności mogą zostać złagodzone. Jednocześnie nasze wyniki pokazują, że konfiguracje sieciowe (np. obsługa ADR dla LoRaWAN lub obsługa poziomu CE i konfiguracje RACH dla NB-IoT) mają znaczący wpływ na wydajność rozważanych technologii. Co istotne, jak wykazaliśmy w niniejszym badaniu, w pewnych konfiguracjach i scenariuszach każda z rozważanych technologii może przewyższyć swoją odpowiedniczkę.

Dowody:

KIO dopuściła i przeprowadziła dowody z dokumentacji postępowania oraz dowody z dokumentów wnioskowane przez strony i uczestników postępowania.

KIO nie dopuściła dowodu z opinii biegłego Instytutu Łączności Państwowego Instytutu Badawczego zakresu telekomunikacji na okoliczność, czy istnieje techniczna możliwość zbudowania sieci LoRaWAN w aglomeracji katowickiej obejmująca swoim zasięgiem wymaganą liczbę użytkowników zgodnie z SWZ przy wykorzystaniu pasma nielicencjonowanego EU 868 Mhz, ustalenia, jakie są możliwości techniczne i ograniczenia sieci LoRaWAN aglomeracji katowickiej, w szczególności liczby wymaganych stacji bazowych, możliwości dotarcia sygnałem w miejscach trudnych, przepustowości sieci i możliwości obsługi jednocześnie wielu urządzeń, spełnienia wymogów dotyczących cyklu pracy i emisji radiowych, odporności sieci na zakłócenia radiowe w aglomeracji katowickiej, niezawodności oraz możliwości zbudowania bezpiecznej sieci LoraWAN. W ocenie KIO przeprowadzenie tego dowodu nie jest niezbędne dla rozstrzygnięcia, przedmiotem sporu nie jest bowiem niezawodność i możliwość zbudowania sieci telekomunikacyjnej LoRaWAN w aglomeracji katowickiej, ale postanowienia SWZ, zakreślona zaś przez odwołującego teza zmierzałaby do oceny wykonalności takiej sieci, a nie dopuszczalności ograniczenia świadczenia usługi w proporcji 90% w poasmach licencjonowanych i 10% w pasmach licencjonowanych, zatem zakres opinii wykraczałby poza granice postawionych zarzutów odwołania, nadto w ocenie KIO wydanie takiej opinii, aby możliwa była ocena jej wiarygodności i przydatności dla rozstrzygnięcia wykraczałoby poza zakreślony dla biegłego materiał dowodowy to jest dokumentację postępowania o udzielenie zamówienia publicznego i dowody odwołującego oznaczone numerami 1 i 15. Co więcej większość opinii przy tak zakreślonym materiale dowodowym opierałaby się o badania, analizy i pomiary wykonane przez odwołującego, a nie ustalenia własne czynione przez biegłego, zwłaszcza, że dokumentacja zamawiającego nie referuje do sieci LoRaWAN, która miałaby być przedmiotem opiniowania przez biegłego. W końcu w ocenie KIO powołany dowód prowadziłby do przewlekłości postępowania odwoławczego.

#### **Rozważania Krajowej Izby Odwoławczej:**

Krajowa Izba Odwoławcza (KIO) dopuściła w charakterze uczestników postępowania wykonawców przystępujących po stronie zamawiającego Polkomtel spółka akcyjna, Orange Polska spółka akcyjna i T-Mobile spółka akcyjna.

KIO nie dopatrzyła się okoliczności, które skutkowałyby odrzuceniem odwołania na podstawie art. 528 ustawy. KIO oceniła, że odwołujący wykazał przesłankę materialnoprawną dopuszczalności odwołania, o której mowa w art. 505 ust. 1 ustawy.

Odwołanie nie zasługuje na uwzględnienie w całości.

W pierwszej kolejności KIO odniesienie się do zarzutu niejednoznaczności sformułowania „infrastruktura własna”, bowiem w tym zakresie z uwagi na udzielone już po wniesieniu odwołania przez zamawiającego wyjaśnienia treści SWZ precyzujące to pojęcie, rozstrzygnięcie w tym zakresie stało się bezprzedmiotowe. Pojęcie uzyskało bowiem definicję, jak na gruncie tej SWZ należy je rozumieć, która nie była objęta przedmiotem zarzutów. Tym samym rozstrzygnięcie musiałby się odnosić do pierwotnej treści SWZ, która na chwilę orzekania już nie istnieje. Tym samym w tym zakresie zarzut podlegałby umorzeniu na podstawie art. 568 pkt. 2 ustawy.

W dalszej kolejności należy dostrzec, że odwołujący bardzo precyzyjnie sformułował swoje żądania zaznaczając w jaki sposób oczekuje nakazania przez KIO modyfikacji treści SWZ, zatem w tym zakresie KIO nie mogłaby orzekać ponad sformułowane żądania. W konsekwencji jest to główny powód oddalenia odwołania w przedmiotowej sprawie, bowiem nawet wprowadzenie zmian postulowanych przez odwołującego nie zapewniłoby mu możliwości złożenia oferty w sposób przewidziany w dowodzie nr 15 – dokumentacja projektowa dla przedmiotowego zadania. Wskazać bowiem należy, że odwołujący nie skarżył ani rozdziału IV pkt. 7 SWZ, w którym zamawiający nie dopuścił składania ofert wariantowych, ani Wymagań dla Systemu odczytowego z pkt 2 ppkt. 2 zd. 2, w którym zamawiający wskazał, że architektura systemu powinna zapewniać możliwość dalszego rozszerzania (skalowania) bez konieczności wymiany lub gruntownej przebudowy infrastruktury systemowej, a przecież sam odwołujący na rozprawie i w dowodzie 15 wyraźnie przyznał, że pierwotnie zbudowany system oparty na sieci telefonii komórkowej będzie następnie wymieniał na równoległe zabudowywany system oparty na sieci LoRaWAN, a więc zakładał wykonanie niezgodnie warunkami zamówienia wprost przewidzianymi przez zamawiającego. Jedynie dodatkowo można zauważyć, że zamawiający wymagał jednego systemu odczytowego, a w praktyce w toku świadczenia usługi miał by wprowadzić jeden system odczytowy, ale przenoszony w trakcie świadczenia usługi na inną infrastrukturę sprzętową, czego SWZ nie

przewidywało, ani nie dopuszczało. Odwołujący w ocenie KIO nie tyle oczekuje, jak wskazywał w odwołaniu, usunięcia postanowień w opisie przedmiotu zamówienia charakteryzujących usługi dostarczane przez konkretnego wykonawcę, ale wskazuje na zamiar złożenia oferty wariantowej zakładającej wykonanie zamówienia przez zastosowanie równoważnej technologii prowadzącej do osiągnięcia założonego celu. Odwołujący jednak nie postawił zarzutu naruszenia art. 92 ustawy, ani nie domagał się wprowadzenia minimalnych wymagań dla oferty wariantowej oraz wymagań dotyczących jej złożenia, ani określenia kryteriów oceny ofert, w sposób zapewniający możliwość ich zastosowania w odniesieniu do oferty podstawowej jak i wariantowej. Odwołujący przedstawił bardzo obszerny materiał dowodowy skupiony na wykazywaniu równoważności technologicznej technologii sieci komórkowej i technologii sieci LoRaWAN, przedstawiał zalety i wady obu technologii IoT, a mimo to nie dostrzegł, że są to odmienne technologie, jedna dopuszczona w 90%, a druga niezabroniona w 10%, ale nawet w tych 10%, o których pisze szeroko odwołujący, nie ma zakazu zestawienia systemu na pasmach licencjonowanych, czy jeszcze inne technologie np. GPS, WIZE 169, może to być także LoRaWAN. Nadto to co słusznie podkreślał zamawiający, że przedmiotem zamówienia jest świadczenie usługi, a nie budowa infrastruktury. W rozwiązaniu wariantowym oferowanym przez odwołującego dochodziłoby właśnie do budowy infrastruktury w trakcie trwania usługi, a następnie do przeniesienia systemu z jednej technologii sieciowej na drugą. Zamawiający nie przewidział takiego sposobu świadczenia usługi. Oznacza to, że byłby to odmienny sposób wykonania zamówienia, a więc wariant, a zamawiający oferty wariantowej nie dopuścił, a odwołujący tego nie zaskarżył. Tym samym nawet gdyby uznać równoważność technologii komórkowej i technologii LoRaWAN, to skoro odwołujący planuje nie tylko świadczyć zamawiającemu usługę, ale także budować niezależną infrastrukturę, to ocena takiej oferty nie byłaby na gruncie tej SWZ porównywalna z ofertami oferującymi wyłącznie świadczenie usługi. Musiałby istnieć specjalnie opisane kryteria oceny ofert gwarantujące wybór porównywalny. Oczywiście można sobie takie kryteria wyobrazić np. choćby przez wskazywany przez odwołującego poziom SLA, tylko tu powstaje obawa o mierzalność tego kryterium w przypadku odwołującego, który nie ma zbudowanej na terenie aglomeracji katowickiej sieci LoRaWAN, na której można by dokonać pomiarów niezawodności tej technologii. Zapewne możliwe byłoby tak jak w przypadku dowodu nr 1 – Raportu, czy dowodu nr 7 skuteczności odczytów 50 nakładek w trybie 28 dni. Pozostaje także trudność w sferze porównania pod kątem kryterium ceny lub kosztu, bo czym innym jest uruchomienie wyłącznie usługi, a czym innym uruchomienie usługi z budową infrastruktury pod odmienną technologią. Dlatego brak zaskarżenia przez odwołującego niedopuszczalności składania oferty wariantowej powoduje, że nawet gdyby KIO doszła do przekonania, że obie technologie są sobie równoważne, to jednak zakładają inny sposób wykonania zamówienia, a co za tym idzie prowadzą do trudności z wzajemną oceną ofert i ich porównywalnością bez wskazania kryteriów oceny ofert umożliwiających realne ich porównanie. Co do niejednoznaczności i braku definicji pojęcia pasmo nielicencjonowane, to KIO dała wiarę odwołującemu, że nie ma definicji legalnej tego pojęcia, jednak w ocenie KIO pomiędzy stronami nie było, w ocenie KIO sporne, jak to pojęcie należy rozumieć, czyli jako pasmo z przyznaną rezerwacją częstotliwości. O tym, że to pojęcie funkcjonuje na rynku telekomunikacyjnym i jest jednolicie rozumiane świadczy wprost dowód nr 18 złożony przez samego odwołującego, gdzie tym pojęciem posługuje się zarówno on jak i Prezes Urzędu Komunikacji Elektronicznej w odpowiedzi na pytanie odwołującego. Gdyby to pojęcie nie było dla Prezesa UKE jasne i jednoznaczne, to albo przedstawiona korespondencja obrazowałaby ustalenie znaczeniowe tego pojęcia pomiędzy odwołującym, a Prezesem UKE, albo Prezes UKE użyłby innego bardziej precyzyjnego, czy poprawnego pojęcia udzielając odpowiedzi. Taka sytuacja jednak nie miała miejsca, z czego należy wnosić, że jest to pojęcie znane na rynku usług telekomunikacyjnych o ustalonym znaczeniu. Tym samym zarzut w tym zakresie również nie zasługiwał na uwzględnienie. Wreszcie jak wynika z dowodu nr 15 odwołujący ma możliwość świadczenia usługi w oparciu o sieci komórkowe, bo sam założył taki sposób świadczenia usługi w wymaganym przez zamawiającego terminie uruchomienia usługi to jest 30 dni od dnia podpisania umowy, zatem dla złożenia oferty przez odwołującego nie jest konieczne zbudowanie infrastruktury LoRaWAN. Tym samym odwołujący nie wykazał, że ograniczenie przedmiotu zamówienia do przeważającej technologii komórkowej uniemożliwia mu złożenie oferty, czy też świadczenie usług przez zakładany przez zamawiającego czasookres. Przeciwnie wydaje się, że istotą odwołania jest umożliwienie odwołującemu biznesowego rozwoju w aglomeracji katowickiej technologii LoRaWAN w celu możliwości jej oferowania dla innych przedsięwzięć czy to publicznych np. inteligentne parkingi, inteligentne oświetlenie czy prywatnych. Mając na uwadze te wszystkie okoliczności KIO oddaliła odwołanie.

O kosztach postępowania odwoławczego orzeczono na podstawie art. 574 i 575 ustawy, tj. stosownie do wyniku postępowania, z uwzględnieniem postanowień Rozporządzenia Prezesa Rady Ministrów w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania z dnia 30 grudnia 2020 r. (Dz.U. z 2020 r. poz. 2437) na podstawie par. 8 ust. 2 pkt. 1 cyt. rozporządzenia zaliczając w poczet kosztów koszty wpisu, koszty wydatków pełnomocnika odwołującego, koszty wydatków

pełnomocnika zamawiającego. Skoro zarzuty odwołania nie potwierdziły się, żaden z zaliczonych kosztów odwołującego nie podlegał rozliczeniu. Zamawiający przedstawił dowód poniesienia kosztów w postaci wydatków pełnomocnika w maksymalnej dopuszczonej rozporządzeniem wysokości, z tego względu KIO nakazała odwołującym zwrot na rzecz zamawiającego tych poniesionych wydatków. KIO nie uwzględniła wniosku zamawiającego o zasądzenie dodatkowo zwrotu kosztów poniesionej opłaty skarbowej, bo zwrot kosztów wydatków pełnomocnika jest zgodnie z par. 5 pkt. 2 lit. b rozporządzenia limitowany i ograniczony do kwoty 3 600zł, z tego względu zasądzenie wydatków ponad tę kwotę nie było możliwe.

Przewodnicząca: .....

.....

.....