

**POSTANOWIENIE**  
**z dnia 9 grudnia 2020 roku**

**Krajowa Izba Odwoławcza** - w składzie:

**Przewodniczący: Katarzyna Prowadzisz**

po rozpoznaniu na posiedzeniu niejawnym w dniu 9 grudnia 2020 roku wniosku z dnia 2 grudnia 2020 roku o uchylenie zakazu zawarcia umowy do czasu ogłoszenia przez Krajową Izbę Odwoławczą wyroku lub postanowienia kończącego postępowanie odwoławcze, wniesionego przez Zamawiającego Urząd Morski w Szczecinie

w postępowaniu o udzielenie zamówienia publicznego prowadzonego pod nazwą *Dostawa sprzętu komputerowego z oprogramowaniem, macierzy, serwerów, plotera ze skanerem oraz modernizacja systemu VTS (biblioteki taśmowe, macierze, serwery, switchy)* w zakresie części III – pn. *Modernizacja systemu VTS (dostawa serwerów, serwerów wirtualizacji oraz przełączników Fiber Channel)*

**postanowiła:**

**uchyla zakaz zawarcia umowy w postępowaniu o udzielenie zamówienia publicznego pod nazwą *Dostawa sprzętu komputerowego z oprogramowaniem, macierzy, serwerów, plotera ze skanerem oraz modernizacja systemu VTS (biblioteki taśmowe, macierze, serwery, switchy)* w zakresie części III – pn. *Modernizacja systemu VTS (dostawa serwerów, serwerów wirtualizacji oraz przełączników Fiber Channel)***

## Uzasadnienie

Zamawiający – Urząd Morski w Szczecinie prowadzi postępowanie o udzielenie zamówienia publicznego prowadzi postępowanie o udzielenie zamówienia publicznego pod nazwą *Dostawa sprzętu komputerowego z oprogramowaniem, macierzy, serwerów, plotera ze skanerem oraz modernizacja systemu VTS (biblioteki taśmowe, macierze, serwery, switche)*, w tym części III – pn. Modernizacja systemu VTS (dostawa serwerów, serwerów wirtualizacji oraz przełączników Fiber Channel).

W dniu 2 grudnia 2020 roku (prezentata na piśmie) pismem z dnia 2 grudnia 2020 roku Zamawiający działając w trybie art. 183 ust. 2 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2019r. poz. 1843 ze zmianami, dalej: „ustawa”) złożył do Prezesa Krajowej Izby Odwoławczej wnioski o uchylenie zakazu zawarcia umowy ww. postępowaniu o udzielenie zamówienia publicznego w zakresie części III - Modernizacja systemu VTS (dostawa serwerów, serwerów wirtualizacji oraz przełączników Fiber Channel)..

Zamawiający wyjaśnił na wstępie, że w dniu 17 września 2020 r. wszczął postępowanie w trybie przetargu nieograniczonego pn. *Dostawa sprzętu komputerowego z oprogramowaniem, macierzy, serwerów, plotera ze skanerem oraz modernizacja systemu VTS ( biblioteki taśmowe, macierze, serwery, switche)*. Postępowanie podzielone było na VI części. Przedmiotem wniosku jest postępowanie na cz. III pn. Modernizacja systemu VTS (dostawa serwerów, serwerów wirtualizacji oraz przełączników Fiber Channel).

W postępowaniu na część III złożone zostały trzy oferty:

- 1) SYSTEM-IT Sp. z o.o. Sp. k. ul. Krasieńskiego 10/17, 71-435 Szczecin, z oferowaną ceną brutto 798 129,78 zł oraz skróconym termin realizacji do dnia 9 grudnia 2020 r.,
- 2) IT SERWIS Sp. z o.o. ul. Żołnierska 5A, 71-210 Szczecin z oferowaną ceną brutto 584 397,60 zł oraz skróconym termin realizacji do dnia 16 grudnia 2020 r.,
- 3) EL TORO B. B. Sp. J ul. Raclawicka 23,73-110 Stargard z oferowaną ceną brutto 658 419,00 zł oraz skróconym termin realizacji do dnia 9 grudnia 2020 r.

W toku postępowania po uzyskaniu wyjaśnień od Wykonawców dotyczących treści złożonych ofert, po ich badaniu i ocenie Zamawiający uznał za najkorzystniejszą w części III ofertę firmy IT SERWIS Sp. z o.o. ul. Żołnierska 5A, 71-210 Szczecin uzasadniając, że oferta spełnia wszystkie wymagania Zamawiającego i otrzymała najwyższą ilość punktów w kryteriach cena i termin wykonania zamówienia. O wyniku postępowania Wykonawcy zostali poinformowani w dniu 18 listopada 2020 r., wynik postępowania w tym samym dniu został zamieszczony również na stronie internetowej prowadzonego postępowania. W dniach 17 i 19 listopada 2020

r. Wykonawca - SYSTEM-IT Sp. z o.o. Sp. k. ul. Krasińskiego 10/17, 71-435 Szczecin - złożył do Zamawiającego wnioski, w których podważa wybór najkorzystniejszej oferty w cz. III argumentując, że oferty zarówno firmy IT SERWIS Sp. z o.o. i EL TORO B. B.Sp. J powinny podlegać odrzuceniu. (*Kopie wniosków w załączeniu.*) Zamawiający w dniu 26 listopada 2020 odpowiadając na powyższe wnioski podtrzymał wybór oferty firmy IT Serwis Sp. z o.o. jako najkorzystniejszej, spełniającej wszystkie wymagania zawarte w SIWZ. (*Kopia pisma w załączeniu.*) W dniu 27 listopada 2020 r. Wykonawca złożył kolejny wniosek w przedmiotowym zakresie oraz odwołanie do Krajowej Izby Odwoławczej. Kopia wniosku w załączeniu.

Zamawiający w uzasadnieniu złożonego wniosku wniósł o uchylenie zakazu zawarcia umowy argumentował, że w związku ze złożeniem przez Wykonawcę odwołania i tym samym brakiem możliwości zawarcia umowy przez Zamawiającego do czasu ogłoszenia przez Izbę wyroku lub postanowienia kończącego postępowanie odwoławcze, zwraca się do uchylenie zakazu zawarcia umowy. Niemożność zawarcia umowy do czasu, o którym mowa powyżej skutkować może po pierwsze brakiem dostępności sprzętu na rynku, po drugie brakiem możliwości rozliczenia inwestycji w roku budżetowym. Środki nie wykorzystane będą musiały ulec zwrotowi, a niezrealizowanie przedmiotowego zamówienia może mieć negatywne skutki dla interesu publicznego z uwagi na fakt, że dostawa określona w części III zamówienia odnosi się do dostawy serwerów, serwerów wirtualizacji oraz przełączników służących modernizacji istniejącego w Urzędzie Systemu VTS.

System VTS na podstawie decyzji Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej z dnia 6 lutego 2019 r. został uznany za usługę kluczową, a Urząd Morski w Szczecinie za operatora usługi kluczowej. Decyzja została wydana na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ( t. j. Dz. U. 2020, poz. 1369) - zwanej dalej ustawą o krajowym systemie cyberbezpieczeństwa. (*Decyzja w załączeniu.*) Usługa kluczowa VTS jest świadczona w podsektorze transport morski, monitorowanie ruchu statków. Usługa jest pełniona na mocy przepisów dyrektywy Parlamentu Europejskiego i Rady 2002/59/WE z dnia 27 czerwca 2002 r. ustanawiającej wspólnotowy system monitorowania i informacji o ruchu statków i uchylającej dyrektywę 93/75/EWE (Dz. Urz. UE L 208 z 05.08.2002, str. 10; Dz. Urz. UE polskie wydanie specjalne, rozdz. 7 t. 7, str. 12 ), funkcji związanej z kontrolą ruchu statków w oparciu o Służbę Kontroli Ruchu Statków (Służbę VTS). Funkcja ta zobowiązuje państwa członkowskie Unii Europejskiej, również i Polskę, do uruchomienia zadań związanych z kontrolą ruchu statków, o której mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim ( t. j. Dz. U. z 2020 r. poz. 680 ze zm.), oraz zgodnie z rozporządzeniem Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 4 grudnia

2012 r. w sprawie Narodowego Systemu Monitorowania Ruchu Statków i Przekazywania Informacji ( t. j. Dz. U. z 2020 r. poz. 1496 ).

Zadania te polegają na: (-) prowadzeniu kontroli i zarządzaniu ruchem statków, zapewnieniu całodobowego, działającego przez 7 dni w tygodniu monitorowania ruchu statków i przekazywania informacji; (-) zapewnieniu całodobowego obiegu i przekazywania informacji za pomocą Narodowego Systemu SafeSeaNet oraz nadzoru i podejmowania działań korygujących mających na celu zapewnienie przekazywania prawidłowych informacji do centralnego systemu SafeSeaNet; (-) ustanowieniu regulaminu i szczegółowych procedur działania Służby VTS, z uwzględnieniem wytycznych Międzynarodowej Organizacji Morskiej (IMO) i Międzynarodowego Stowarzyszenia Służb Oznakowania Nawigacyjnego (IALA); (-) utrzymaniu w działaniu ciągłym i zapewnieniu wymaganej dostępności elementów podsystemu monitorowania ruchu statków.

Urząd Morski w Szczecinie jako operator usługi kluczowej musi spełniać wymagania ustawy o krajowym systemie cyberbezpieczeństwa oraz rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U z 2019 r. poz. 2479). Aby zapewnić zgodność z ustawą, a także ograniczyć ryzyka związane z usługą cyfrową, Urząd Morski w Szczecinie przeprowadził audyt bezpieczeństwa systemów informatycznych wykorzystanych w usłudze kluczowej zgodnie z wymogami art. 15 ustawy o krajowym systemie cyberbezpieczeństwa. Audyt jednoznacznie wykazał zwiększone ryzyko o charakterze krytycznym dla usługi kluczowej związane z brakiem wsparcia gwarancyjnego. Wykorzystywana infrastruktura serwerowa i macierze dyskowe mają ponad sześć lat i nie ma już możliwości zwiększenia okresu świadczenia wsparcia gwarancyjnego producenta, a także zwiększa się ryzyko braku możliwości dokupienia nowych części zamiennych w razie awarii np. dysków w macierzach dyskowych, których wymiana na nowe w przypadku awarii byłaby niemożliwa, ze względu na aspekty technologiczne.

Mając na uwadze obowiązki operatora usług kluczowych wynikające z art 8 ustawy o krajowym systemie cyberbezpieczeństwa, a także wyniki przeprowadzonego audytu bezpieczeństwa usługi kluczowej, Urząd Morski w Szczecinie jest zobowiązany niezwłocznie podjąć działania zmierzające do usunięcia wskazanych podatności. W tym celu zostało przeprowadzone postępowanie przetargowe, które miało dostarczyć niezbędny sprzęt do infrastruktury usługi kluczowej. Brak możliwości podpisania umowy i tym samym zakupu nowych serwerów i macierzy uniemożliwia wykluczenia powstałego ryzyka, ryzyka które może mieć krytyczny wpływ na zdolność do zachowania ciągłości działania usług świadczonych przez Urząd.

**Zdaniem Izby**, zgodnie z art. 183 ust. 2 zd. 2 ustawy Prawo Zamówień Publicznych (Dz. U. z 2019 r., poz. 1843) Izba może uchylić zakaz zawarcia umowy na wniosek Zamawiającego, *jeżeli niezawarcie umowy mogłoby spowodować negatywne skutki dla interesu publicznego, w szczególności w dziedzinach obronności i bezpieczeństwa, przewyższające korzyści związane z koniecznością ochrony wszystkich interesów, w odniesieniu do których zachodzi prawdopodobieństwo doznania uszczerbku w wyniku czynności podjętych przez zamawiającego w postępowaniu o udzielenie zamówienia.*

Konieczne jest zatem wykazanie przez Zamawiającego, że niezawarcie umowy przed ogłoszeniem przez Izbę wyroku lub postanowienia kończącego postępowanie mogłoby godzić w interes publiczny, w stopniu przewyższającym korzyści związane z koniecznością ochrony wszystkich interesów, w odniesieniu do których zachodzi prawdopodobieństwo doznania uszczerbku w wyniku czynności podjętych przez Zamawiającego w postępowaniu o udzielenie zamówienia.

Pojęcie „interesu publicznego” w polskim prawodawstwie nie zostało zdefiniowane (brak definicji legalnej), jednakże jego znaczenia można poszukiwać w orzecznictwie (np. postanowienie Sądu Najwyższego z dnia 17 marca 2016 roku, sygn. akt V CSK 588/17, wyrok Naczelnego Sadu Administracyjnego z dnia 2 lutego 2017 roku sygn. akt II FSK 4126/14). Klauzula generalna interesu publicznego w kontekście ustawy Prawo zamówień publicznych oraz regulacji odnoszącej się do wniosku o uchylenie zakazu zawarcia umowy stanowi możliwość odwołania się przez Zamawiającego stosującego prawo do wartości, które są wspólne i istotne dla danej społeczności. Dokonując oceny wykazania spełnienia przesłanki interesu publicznego w złożonym wniosku o uchylenie zakazu zawarcia umowy Izba dokonuje oceny argumentacji przedstawionej przez Zamawiającego. Wskazać należy na dwie płaszczyzny, których wartości stanowią kluczowy element oceny – pierwszą płaszczyzną jest zasada jaka obowiązuje w ramach prowadzonego postępowania o udzielenie zamówienia publicznego, tj. niemożliwość zawarcia umowy do czasu ogłoszenia przez Izbę wyroku lub postanowienia kończącego postępowanie odwoławcze; drugą płaszczyzną stanowi wyjątek od zasady, tj. podniesienie okoliczności, które w wyniku nie zawarcia umowy spowodowałyby negatywne skutki dla interesu publicznego, przewyższające korzyści związane z koniecznością ochrony wszystkich interesów, w odniesieniu do których zachodzi prawdopodobieństwo doznania uszczerbku w wyniku czynności podjętych przez Zamawiającego w postępowaniu o udzielenie zamówienia publicznego.

W efekcie, klauzula „interesu publicznego” w postępowaniu o udzielenie zamówienia publicznego, w przypadku złożenia wniosku o uchylenie zakazu zawarcia umowy, stanowi

przesłankę umożliwiającą ochronę określonych w art. 183 ust. 2 ustawy wartości. Wymaga również zaznaczenia, że treść pojęcia „interesu publicznego” w każdym przypadku będzie zależna od kontekstu w jakim jest powoływana, okoliczności i sytuacji, w której Zamawiający się na nią powołuje. W orzecznictwie wypełnia się pojęcie „interesu publicznego” przez zdefiniowanie go jako korzyści uzyskiwane w wyniku realizacji przedsięwzięć służących ogółowi w zakresie zadań ciążących na administracji rządowej oraz samorządowej, realizowanych w drodze świadczenia usług powszechnie dostępnych, związanych np. z ochroną zdrowia, oświaty, kultury, porządku publicznego (uchwała Trybunału Konstytucyjnego z dnia 12 marca 1997 r.).

Izba zaznacza, że brak zdefiniowania pojęcia „interesu publicznego” stwarza koniecznym w każdym przypadku, w którym pojęcie to ma znaczenie dla wykładni i oceny spełnienia przesłanek określonej w przepisie normy prawnej odniesienie do miejsca, czasu jak również okoliczności w jakich należy je stosować, co pozwoli na dokonanie oceny czy wartości odnoszące się do ogółu przewyższają korzyści związane z koniecznością ochrony wszystkich interesów w odniesieniu, do których zachodzi prawdopodobieństwo doznania uszczerbku w wyniku czynności podjętych przez Zamawiającego w postępowaniu o udzielenie zamówienia.

W ocenie Izby, mając na uwadze powyższe stanowisko, Zamawiający wykazał spełnienie przesłanek określonych w art. 183 ust. 2 zd. 2 ustawy, których to wykazanie jest niezbędne, aby Izba mogła uchylić zakaz zawarcia umowy do czasu ogłoszenia przez Izbę wyroku lub postanowienia kończącego postępowanie odwoławcze.

Zamawiający wykazał niezbędną konieczność zawarcia umowy i realizacji zamówienia objętego przedmiotowym postępowaniem o udzielenie zamówienia publicznego pod nazwą *Dostawa sprzętu komputerowego z oprogramowaniem, macierzy, serwerów, plotera ze skanerem oraz modernizacja systemu VTS (biblioteki taśmowe, macierze, serwery, switche)* w zakresie części III – *pn. Modernizacja systemu VTS (dostawa serwerów, serwerów wirtualizacji oraz przełączników Fiber Channel)* wskazując na konieczność podjęcia czynności związanych realizacją usługi kluczowej, którą realizuje Urząd Morski w Szczecinie jako operator usługi kluczowej. System VTS został zgodnie z decyzją Ministra Gospodarki Morskiej i Żeglugi Śródlądowej z dnia 6 lutego 2019 roku uznany za usługę kluczową.

Wymaga odnotowania, że na podstawie „Statutu Urzędu Morskiego w Szczecinie” nadanym na mocy zarządzenia nr 19 Ministra Gospodarki Morskiej i Żeglugi Śródlądowej z dnia 26 kwietnia 2018 r. w sprawie nadania statutu Urzędowi Morskiemu w Szczecinie (Dz. Urz.

MGMiŻŚ poz. 19) przedmiotem działalności Urzędu jest między innymi pełnienie, na mocy przepisów dyrektywy Parlamentu Europejskiego i Rady 2002/59/WE z dnia 27 czerwca 2002 r. ustanawiającej wspólnotowy system monitorowania i informacji o ruchu statków i uchylającej dyrektywę 93/75/EWE (Dz. Urz. UE L 208 z 05.08.2002, str. 10; Dz. Urz. UE polskie wydanie specjalne, rozdz. 7 t. 7, str. 12 ), funkcji związanej z kontrolą ruchu statków w oparciu o Służbę Kontroli Ruchu Statków (Służbę VTS).

Wskazana w ww. Decyzji dyrektywa – do czego również odwoływał się Zamawiający w swoim stanowisku – zobowiązuje państwa członkowskie Unii Europejskiej, również i Polskę, do realizacji zadań związanych z kontrolą ruchu statków, o której mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2018 r. poz. 181, z późn. zm.), zgodnie z rozporządzeniem Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 4 grudnia 2012 r. w sprawie Narodowego Systemu Monitorowania Ruchu Statków i Przekazywania Informacji (Dz. U. poz. 1412 z późn. zm.). Zadania te polegają na:

- 1) prowadzeniu kontroli i zarządzaniu ruchem statków, zapewnieniu całodobowego, działającego przez 7 dni w tygodniu monitorowania ruchu statków i przekazywania informacji;
- 2) zapewnieniu całodobowego obiegu i przekazywania informacji za pomocą Narodowego Systemu SafeSeaNet oraz nadzoru i podejmowania działań korygujących mających na celu zapewnienie przekazywania prawidłowych informacji do centralnego systemu SafeSeaNet;
- 3) ustanowieniu regulaminu i szczegółowych procedur działania Służby VTS, z uwzględnieniem wytycznych Międzynarodowej Organizacji Morskiej (IMO) i Międzynarodowego Stowarzyszenia Służb Oznakowania Nawigacyjnego (ALA);
- 4) utrzymaniu w działaniu ciągłym i zapewnieniu wymaganej dostępności elementów podsystemu monitorowania ruchu statków.

Tym samym podmiot będący operatorem usługi kluczowej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej, zobowiązany jest do realizacji zadań usługi kluczowej związanych z kontrolą ruchu statków, monitorowania w nieprzerwany sposób, z zachowaniem ciągłości świadczenia usługi oraz całodobowego przekazywania informacji i obiegu tych informacji oraz utrzymaniu w działaniu ciągłym i zapewnieniu wymaganej dostępności elementów podsystemu monitorowania ruchu statków.

Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369; dalej UKSC) określa operatorów usług kluczowych, jako firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej, do kluczowych sektorów gospodarki należy transport. Kluczowe sektory gospodarki to: energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej. Natomiast przez usługę kluczową, stosownie do art. 2 pkt 16 UKSC, należy rozumieć usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i została wymieniona w wykazie usług kluczowych. Wykaz usług kluczowych określa rozporządzenie Rady Ministrów z dnia 11 września 2018 r. *w sprawie wykazu usług kluczowych oraz istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych* (Dz. U. z 2018 r. poz. 1806) zgodnie z którym VTS (Służba Kontroli Ruchu Statków) – to aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, Stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2018 r. poz. 181, 1137 i 1669) dla określonego progu istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej – którą w tym wypadku jest monitorowanie ruchu statków – gromadzenie i dystrybucja informacji związanej z bezpieczeństwem ruchu morskiego na obszarze terytorialnego zakresu działania dyrektorów urzędów morskich określonym w przepisach wydanych na podstawie art. 40 ust. 1 i 2 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej.

Na podstawie art. 5 ust. 2 UKSC organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej – w tym wypadku operatorem usługi kluczowej jest Urząd Morski w Szczecinie – jeżeli ten podmiot świadczy usługę kluczową, ale również świadczenie tej usługi zależy od systemów informacyjnych a także incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora (a istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, określana jest na podstawie progów istotności skutku zakłócającego – art. 5 ust. 3 UKSC). Definicja systemu informatycznego została podana w art. 2 pkt 14 UKSC system informacyjny to „system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000, 1544 i 1669), wraz z przetwarzanymi w nim danymi w postaci elektronicznej, a więc zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia



16 lipca 2004 r. — Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954). Definicja incydentu wynika z art. 2 pkt 5 UKSC, to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Przy czym ustawodawca określił również definicje incydentu krytycznego, poważnego, istotnego precyzując zakres obowiązków i odpowiedzialności operatora usługi kluczowej.

Zgodnie z wytycznymi dla przyjętych regulacji prawnych oraz uzasadnieniem ich wdrożenia do najważniejszych obowiązków realizujących zadania bezpieczeństwa należy *wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (w tym utrzymanie i bezpieczną eksploatację systemu informacyjnego; bezpieczeństwo fizyczne i środowiskowe; bezpieczeństwo i ciągłość dostaw; wdrażanie, dokumentowanie i utrzymywanie planów działania)* źródło: [www.gov.pl/web/cyfrizacja](http://www.gov.pl/web/cyfrizacja).

Oznacza to, że świadczenie przez Urząd Morski w Szczecinie usługi kluczowej zależy od systemów informacyjnych zapewniających prawidłowe funkcjonowanie, w konsekwencji niezbędne jest utrzymywanie infrastruktury sprzętowej jak również możliwości świadczenia usług gwarancyjnych na nieprzerwanym poziomie, co gwarantuje ciągłość realizacji usługi kluczowej. Realizacji wniosków wynikających z przeprowadzonego Audytu bezpieczeństwa systemów informatycznych, który wskazał na zwiększone ryzyko o charakterze krytycznym dla usługi kluczowej związanej z brakiem wsparcia gwarancyjnego wymaga podejmowania natychmiastowych działań. Tym bardziej, że jak podał Zamawiający macierze dyskowe i infrastruktura serwerowa wykorzystywana do realizacji usługi kluczowej ma ponad sześć lat a to powoduje, że nie ma możliwości zwiększenia okresu gwarancyjnego producenta, jak również powoduje zwiększenie ryzyka możliwości dokupienia nowych części zamiennych w razie awarii. W ocenie Izby w przypadku świadczenia usługi kluczowej – o czym mowa wyżej - w sposób ciągły nieprzerwany z monitoringiem ruchu statków oraz przekazywaniem danych wymaga ciągłej i nieprzerwanej pracy systemu informatycznego.

Izba dostrzegła szczególny charakter przedmiotowych zadań, które bezpośrednio wpływają na wywiązywanie się Rzeczypospolitej Polskiej ze zobowiązań wynikających z regulacji prawa wspólnotowego jak również szczegółowo wskazanych w krajowym prawodawstwie.

Zadania jakie realizuje Urząd Morski w Szczecinie w ramach realizowanej usługi kluczowej do spraw cyberbezpieczeństwa dla podsektora — transport wodny podejmowane są w interesie publicznym, który należy oceniać w kontekście interesu obywateli Rzeczypospolitej Polskiej ładu społecznego i gospodarczego, przy jednoczesnym poszanowaniu obowiązujących Zamawiającego regulacji prawnych. Mając na uwadze powyższe zasadnym jest uchylenie zakazu zawarcia umowy, z uwagi na stwierdzenie istnienia zagrożenia dla interesu publicznego. Należy mieć bowiem na uwadze, że *Cyberbezpieczeństwo to zespół*

*zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. Z pojęciem tym związana jest również ochrona przetwarzania informacji oraz zachodzących interakcji w sieciach teleinformatycznych, a to związane jest z użytkowanym sprzętem, posiadanym oprogramowaniem oraz w wymaganych i koniecznych usługami dodatkowymi.*

Mając na uwadze powyższe, Izba uznała, że utrzymanie zakazu zawarcia umowy spowoduje negatywne skutki dla interesu publicznego, przewyższające korzyści związane z koniecznością ochrony wszystkich interesów, w odniesieniu do których zachodzi prawdopodobieństwo doznania uszczerbku w wyniku czynności podjętych przez Zamawiającego w postępowaniu o udzielnie zamówienia publicznego.

Wobec powyższego, orzeczono jak w sentencji.

Stosownie do art. 183 ust. 4 zd. 2 ustawy na niniejsze postanowienie nie przysługuje skarga.

**Przewodniczący:** .....