Sygn. akt: KIO 2362/21

WYROK

z dnia 15 września 2021 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: **Ewa Kisiel**

Protokolant: **Mikołaj Kraska**

po rozpoznaniu na rozprawie w dniu 10 września 2021 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 6 sierpnia 2021 r. przez wykonawców wspólnie ubiegających się o udzielenie zamówienia jako **Konsorcjum firm: 1. Comp S.A. z siedzibą w Warszawie, 2. Enigma Systemy Informacji Sp. z o.o. z siedzibą w Warszawie** w postępowaniu prowadzonym przez zamawiającego **Agencję Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie,**

przy udziale wykonawców wspólnie obiegających się o udzielenie zamówienia jako **Konsorcjum firm: 1. Ratels Sp. z o. o z siedzibą w Warszawie, 2. T-Systems Polska Sp. z o.o. z siedzibą we Wrocławiu,** zgłaszających przystąpienie do postępowania odwoławczego po stronie zamawiającego

orzeka:

1. **Oddala odwołanie.**

2. Kosztami postępowania obciąża wykonawców wspólnie ubiegających się o udzielenie zamówienia jako **Konsorcjum firm: 1. Comp S.A. z siedzibą w Warszawie, 2. Enigma Systemy Informacji Sp. z o.o. z siedzibą w Warszawie** i zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez wykonawców wspólnie ubiegających się o udzielenie zamówienia jako **Konsorcjum firm: 1. Comp S.A. z siedzibą w Warszawie, 2. Enigma Systemy Informacji Sp. z o.o. z siedzibą w Warszawie**, tytułem wpisu od odwołania.

Stosownie do art. 579 i 580 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm.) na niniejszy wyrok - w terminie 14 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Warszawie.

Przewodniczący: ……..……..…….

Sygn. akt KIO 2362/21

Uzasadnienie

Agencję Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie (dalej: „Zamawiający" lub „ARiMR") prowadzi na podstawie przepisów ustawy z dnia 19 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm.) - zwanej dalej: „ustawą" lub „Pzp" w trybie przetargu nieograniczonego postępowanie o udzielenie zamówienia publicznego na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji". Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 7 kwietnia 2021 r. pod nr 2021/S 067-173426. Wartość zamówienia jest większa niż progi unijne wskazane w art. 3 ust. 1 Pzp.

W dniu 6 sierpnia 2021 r. wykonawcy wspólnie ubiegający się o udzielenie zamówienia jako Konsorcjum firm: 1. Comp S.A. z siedziba w Warszawie, 2. Enigma Systemy Informacji Sp. z o.o. z siedzibą w Warszawie – dalej: „Odwołujący" lub „AID „Konsorcjum Comp" lub „Wykonawca" wnieśli odwołanie od niezgodnych z prawem czynności i zaniechań Zamawiającego w postępowaniu.

Odwołujący zarzucał Zamawiającemu naruszenie art. 226 ust. 1 pkt 5 w zw. z art. 16 pkt 1-3 Pzp przez odrzucenie jego oferty pomimo, iż jej treść jest zgodna z warunkami zamówienia.

Odwołujący wnosił o uwzględnienie odwołania i nakazanie Zamawiającemu:

- unieważnienia czynności wyboru oferty najkorzystniejszej;

- unieważnienia czynności odrzucenia oferty Konsorcjum Comp;
- dokonania powtórnej czynności badania i oceny ofert z uwzględnieniem zarzutów postawionych w odwołaniu;
- dokonania wyboru oferty najkorzystniejszej.

W uzasadnieniu odwołania Odwołujący wskazywał, że Zamawiający podjął decyzję o odrzuceniu oferty na podstawie udzielanych w odpowiedzi na wezwanie wyjaśnień treści oferty, będących rezultatem złożonych wyjaśnień w zakresie ceny, w których Odwołujący prezentując kalkulację kosztów, wskazał również szczegółowo elementy oferowanego przez siebie rozwiązania. Zarzucana przez Zamawiającego niezgodność oferty z warunkami zamówienia oparta jest na interpretacji treści wymagań dokonanej przez Zamawiającego, która, jednakże nie znajduje potwierdzenia w faktycznym brzmieniu opisu przedmiotu zamówienia. Zamawiający dopiero w treści wezwania do udzielenia wyjaśnień i następnie uzasadnieniu odrzucenia oferty, wyraził swoje oczekiwania w zakresie wymaganych funkcjonalności/elementów oferowanego rozwiązania, których nie dało się odczytać z treści udostępnionych wykonawcom dokumentów zamówienia.

Zdaniem Odwołującego stanowi to naruszenie zasad równego traktowania wykonawców i poszanowania zasad uczciwej konkurencji. Ponadto, w treści SWZ Zamawiający nie zobowiązał wykonawców do określenia w ofercie, jakie rozwiązanie oferują oraz nie oczekiwał podania jakichkolwiek szczegółów dotyczących jego elementów, parametrów itp. Przewidziana w SWZ weryfikacja zgodności oferty z warunkami zamówienia w zakresie wymagań dotyczących systemu DLP polegała na potwierdzeniu oferowanych parametrów zgodnie z Tabelą nr 1 zawartą w Formularzu ofertowym. Odwołujący zgodnie z wymaganiami SWZ wykazał zgodność rozwiązania w zakresie wymagań i w sposób zgodny z postanowieniami SWZ (tabelą zawartą w Formularzu ofertowym), a więc w taki sposób, jaki został przewidziany również w odniesieniu do pozostałych wykonawców. Wszystkie podnoszone przez Zamawiającego rzekome niezgodności dotyczą odrębnego badania, skierowanego tylko w stosunku do Odwołującego na podstawie złożonych wyjaśnień w zakresie ceny, przy czym Zamawiający nie podał żadnych okoliczności świadczących o tym, iż oferta zawiera cenę rażąco niską. Również powyżej opisane podejście do badania oferty Odwołującego nie zasługuje na uznanie za prawidłowe ze względu na naruszenie zasad ogólnych postępowania określonych w art. 16 Pzp i żądania od Odwołującego podania informacji i przedstawienia dokumentów przedmiotowych nie przewidzianych w postanowieniach SWZ.

Odwołujący podnosił, że Zamawiający, przywołując punkty Rozdział I podrozdział I.1 pkt 14 i 20 SWZ, wskazał, że oferta Odwołującego jest niezgodna z warunkami zamówienia,

ponieważ nie oferuje funkcjonalności Discovery dla aplikacji SaaS (m.in. SharePoint Online, Exchange Online) oraz nie posiada możliwości budowania polityk ochrony informacji uwzględniając kontekst, w jakim informacja jest używana (komponentu Cloud Access Security Broker (CASB)". Przy czym, w kontekście pkt 14 powołał w uzasadnieniu odrzucenia stwierdzenie niezgodności w zakresie podpunktu 14.2, bez wskazania okoliczności faktycznych dotyczących pozostałych podpunktów wymagania. Opisana przez Zamawiającego niezgodność nie odpowiada treści wymagań faktycznie zawartych w warunkach zamówienia.

Odwołujący podnosił, że Zamawiający w pkt 14 precyzyjnie określił, czym jest dla niego „kontekst w jakim informacja jest używana" wymieniając 4 konkretne scenariusze. W pierwszym podpunkcie Zamawiający jasno wskazał, że chodzi mu o nadawcę informacji „kto". Z kolei w podpunkcie 14.2 Zamawiający nie użyl już określenia adekwatnie precyzyjnego tzn. „do kogo", ale posłużył się zaimkiem „gdzie", który w języku polskim odnosi się nie do osoby odbiorcy (jak zaimek „kto"), ale do miejsca. Sformułowanie „gdzie informacje są wysyłane" jasno wskazuje, że chodzi o lokalizację, miejsce lub przestrzeń odbioru, a nie o adresata. Takie rozumienie, jak przyjęte przez Wykonawcę, właściwe jest zarówno odnosząc się do literalnego brzmienia wymagania, jak i w kontekście branżowym, w odniesieniu do przedmiotu zamówienia. W świecie technologii informacyjnych określenie „gdzie" może oznaczać aplikację, serwer przekazujący informację, adres docelowy do którego informacja jest wysyłana, udział w przesyłaniu i odbieraniu cyfrowej informacji. Gdyby Zamawiający chciał wyrazić wymaganie wskazania osoby (użytkownika), do której informacje są wysyłane, posłużyłby się zaimkiem „do kogo", odpowiednio do sposobu, w jaki wskazał na wymóg uwzględnienia okoliczności, kto jest nadawcą posługując się zaimkiem „kto". np. adres IP sieci odbiorcy i wiele innych elementów pośrednich biorących. Tłumaczenie Zamawiającego zawarte w uzasadnieniu odrzucenia, iż „określenie „gdzie" oznacza kierunek przepływu informacji, czyli „do kogo" informacje są wysyłane" stanowi nadinterpretację postanowień SWZ niedopuszczalną na tym etapie i wskazującą, że nawet jeśli zamiar Zamawiającego byt inny, to jego potrzeby zostały określone w sposób nieprecyzyjny i nieodpowiadający tym intencjom. Bowiem „kierunek" wysyłania informacji cyfrowych nie jest powiązany bezpośrednio z użytkownikiem, a wynika ze sposobu działania całej infrastruktury np. kierunkiem może być firma/aplikacja/serwer, do którego jest informacja wysyłana a konkretny użytkownik definiowany jest jako odbiorca informacji. Wskazany brak precyzji w wyrażeniu w treści wymagań SWZ faktycznych intencji Zamawiającego stanowi okoliczność obciążającą tylko samego Zamawiającego, który nie może oczekiwać od wykonawców spełnienia wymagań niezamieszczonych w treści SWZ - byłoby to sprzeczne zarówno z przepisami dotyczącymi sposobu opisu przedmiotu

zamówienia, jak i prowadziłoby do nieporównywalności składanych w postępowaniu ofert. Dodatkowo Odwołujący wskazywał, że wymaganie przez Zamawiającego dostarczenia przez Odwołującego w ramach przedmiotu zamówienia licencji dla komponentu Cloud Access Security Broker (CASB) jest nieuzasadnione. Zgodnie z udzielonymi w toku postępowania wyjaśnieniami, standardowa licencja na oferowany produkt zapewnia spełnienie wymagań pkt I.1.14 SWZ, w szczególności podpunktu 14.2 zgodnie z jego faktycznym i literalnym brzmieniem. Licencja rozszerzona o wskazywany przez Zmawiającego CASB byłaby wymagana tylko, gdyby w treści pkt 14 jako okoliczność wymagającą uwzględnienia wskazano odbiorcę okoliczność „do kogo" informacje są wysyłane.

Kolejno Odwołujący podnosił, że w pkt 20, Zamawiający sformułował wymaganie dzieląc je wyraźnie na dwie części. Odwołujący podniósł, że wbrew zatem twierdzeniom Zamawiającego, wykonawca był uprawniony do rozumienia wymagania w sposób wyjaśniony Zamawiającemu w odpowiedzi na wezwanie z dnia 28 czerwca 2021 r. Podział wymagania na dwa zdania i użycie odrębnych sformułowań wskazują, że należy rozróżnić wymaganie w zakresie funkcjonalności Discovery dla serwerów i stacji końcowych w sieci Zamawiającego od funkcjonalności dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online. Przytaczane przez Zamawiającego przykłady różnych stosowanych przez niego określeń nie mają przy tym kluczowego znaczenia w tej sytuacji, w której mówimy o zastosowaniu odrębnych pojęć w ramach jednego wymagania, zawartego w tym samym punkcie SWZ. Zatem również na płaszczyźnie wykładni językowej, zasadne jest rozumienie wymagania SWZ prezentowane przez Odwołującego.

Odwołujący podtrzymał również wyjaśnienia udzielone Zamawiającemu w dniu 28 czerwca 2021 r., wskazujące, iż dostarczenie funkcjonalności Discovery dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online nie stanowiło zakresu przedmiotu zamówienia w ramach tego postępowania, jakkolwiek dostarczane rozwiązanie miało zapewnić możliwość uzyskania licencji w takim rozszerzonym zakresie: „Funkcjonalność ta powinna być również oferowana".

Następnie Konsorcjum Comp powołało się na pkt I.1.28 SWZ, w którym jego zdaniem Zamawiający wskazywał wyraźnie, że zakres ochrony aplikacji w chmurze, w tym pakietu Microsoft Office 365, pozostaje opcjonalnie jako możliwość rozbudowy, a zatem nie jest wymagane dostarczenie licencji w tym zakresie w ramach tego zamówienia. W opinii Odwołującego wymaganie nr 28 należało rozumieć jako wyłączające ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS poza zakres zamówienia, stawiając jedynie wymóg zapewniania możliwości rozbudowy o taki zakres licencji. Zgodnie z materiałami producenta tj. firmy Microsoft (dostępne przykładowo pod linkiem:

https://www.microsoft.com/pl-pl/microsoft-365/compare-microsoft365-enterprise-plans), aplikacje przechowujące informacje jako SaaS w pakietach Microsoft 365 (zgodnie z informacjami Zamawiającego, posiada on obecnie pakiet Microsoft Office 365 w wersji E3) to między innymi chmurowa usługa SaaS Sharepoint Online oraz Exchange Online, a zatem te aplikacje, o których mowa w zdaniu 2-gim wymagania w pkt 20. Interpretacja przedstawiona przez Odwołującego wbrew obecnie podnoszonym argumentom Zamawiającego, jest zatem spójna z pozostałymi postanowieniami opisu przedmiotu zamówienia i logiczna. Jeżeli Zamawiający w osobnym punkcie 28. wskazuje, iż cały pakiet rozwiązań Microsoft 365 i jego ochronę należy traktować jako opcjonalną rozbudowę funkcjonalności, to brak podstaw do przyjęcia, że Odwołujący nieprawidłowo zrozumiał, iż również funkcjonalność Discovery dla takich aplikacji nie wchodzi w zakres aktualnego zamówienia i wymaga tylko zapewnienia, że jest ona „oferowana" - będzie dostępna na wypadek rozbudowy systemu. Funkcjonalność Discovery służy wykrywaniu informacji objętych politykami ochrony. Jeśli ochrona aplikacji SaaS nie jest objęta tym postępowaniem i ma być jedynie możliwa w wyniku rozbudowy, to funkcjonalność taka znajdzie zastosowanie jedynie „na przyszłość", w wyniku rozbudowy, zaś obecnie dostarczany system ma umożliwiać jej oferowanie.

Zdaniem Konsorcjum Comp nie jest zasadne powoływanie się przez Zamawiającego, w celu poparcia jego argumentacji, na wymaganie w pkt 29, gdyż w żaden sposób nie potwierdza ono konieczności zaoferowania w bieżącym postepowaniu funkcjonalności Discovery dla aplikacji SaaS. W punkcie tym, Zamawiający wymagał, aby ochrona informacji w chmurze wykorzystywała te same mechanizmy, co w przypadku aplikacji lokalnie instalowanych w sieci zamawiającego. Punkt ten należy odczytywać wspólnie z poprzedzającym go pkt 28 oraz pozostałymi postanowieniami SWZ. Jeżeli Zamawiający zdecyduje się na opcjonalne rozszerzenie ochrony o aplikacje SaaS (zgodnie z pkt 28), to producent systemu musi zapewnić, iż w tych aplikacjach funkcjonalność Discovery będzie wykorzystywała te same mechanizmy. Wymóg taki jest spełniony przez rozwiązanie zaoferowane przez Konsorcjum Comp, jednak dopiero w momencie, gdy Zamawiający zdecyduje się na rozszerzenie ochrony również na aplikacje SaaS. Zatem punkt ten w żaden sposób nie potwierdza, iż ochrona dla Exchange online czy Sharepoint online musi być dostarczona w niniejszym postepowaniu, lecz jedynie ze musi być spełniona wymagana funkcjonalność dla tych aplikacji w momencie rozbudowy systemu. Fakt wskazania przez Zamawiającego, iż w bieżącej działalności wykorzystuje m. in. aplikacje Sharepoint online oraz Exchange online w żaden sposób nie potwierdza, iż wymaga to dostarczenia funkcjonalności, o której mowa w pkt 20 już na obecnym etapie, gdyż podobnie Zamawiający odpowiedział na pytanie nr 6 odnoszące się do całego pakietu Microsoft 365 (czyli aplikacji SaaS, której wyłączenie z zakresu przedmiotu zamówienia wyraźnie wynika z pkt 28 SWZ).

W ocenie Odwołującego udzielona odpowiedź wskazująca na korzystanie obecnie z aplikacji chmurowych (SaaS), nie zmienia faktu, iż wiążące jest wymaganie z pkt 28 i wykorzystywane pakiety nie są przewidziane do ochrony w ramach systemu DLP w tym zamówieniu, a jedynie na wypadek rozbudowy. Zamawiający w ramach postępowania określił zakres swoich zasobów, który ma być objęty ochroną systemu DLP i nie znaczy, że ma być nim objęta całość tych zasobów - pkt 28 wskazuje, np. że z zakresu usługi wyłączono na tym etapie aplikacje SaaS, wymagając jedynie możliwości rozbudowy.

Odwołujący następnie wyjaśniał, że w ramach wymagań dla funkcjonalności systemu opisanych w pkt I.1.30 SWZ, Zamawiający twierdzi, iż zaoferowane rozwiązanie nie spełnia wymagania w ppkt 17, tj. funkcjonalności „wymuszania szyfrowania poczty elektronicznej". Zamawiający, w uzasadnieniu odrzucenia oferty w sposób zamienny traktuje dwie różne funkcjonalności, tj. wymaganą w pkt 17 funkcję wymuszania szyfrowania i funkcję/narzędzie, które taki proces szyfrowania przeprowadza. Zamawiany system DLP ma zgodnie z SWZ wymuszać szyfrowanie, ale nigdzie w SWZ nie wskazano, aby takie narzędzie do szyfrowania (czy też funkcjonalność szyfrowania) miało zostać dostarczone w ramach zamawianej usługi. Powyższego zakresu przedmiotu zamówienia nie zmienia przytaczana przez Zamawiającego odpowiedź na pytanie nr 12. Ani w tej odpowiedzi, ani w żadnym punkcie SWZ Zamawiający nie oczekuje dostarczenia narzędzia i technologii wykonującej szyfrowanie danych. Oczekuje za to, by system klasyfikacji wymuszał szyfrowanie poczty elektronicznej lub jak później doprecyzował właśnie w odpowiedzi na pytanie nr 12: by narzędzie klasyfikacji było elementem oznaczania wiadomości email do zaszyfrowania. „Wymuszenie szyfrowania" nie oznacza, że system klasyfikacji czy system DLP ma być narzędziem ją wykonującym. Wymuszenie możliwe jest poprzez zlecenie realizacji tej akcji do narzędzia dostarczanego przez podmiot trzeci, nie wymaganego w niniejszym postępowaniu. Doprecyzowanie w zakresie „oznaczanie wiadomości email do zaszyfrowania" w żaden sposób nie jest równoważne twierdzeniu, iż to system klasyfikacji czy system DLP ma owe szyfrowanie samodzielnie wykonać. Wymuszenie czy oznaczenie nie jest tożsame z wykonaniem w ramach posiadanych w systemie narzędzi.

Odwołujący zapewnił, iż dostarcza rozwiązanie, które zrealizuje funkcjonalność wymuszenia szyfrowania informacji - wykazał to (mimo braku żądania takiego dokumentu w SWZ) w udzielonych wyjaśnieniach i opisie sposobu realizacji funkcjonalności. Odwołujący wskazał na możliwość integracji systemu z narzędziami/technologiami innych producentów i podał przykładowe narzędzie wykonujące szyfrowanie np. Sealpath, ale jako takie narzędzie może być też wykorzystany posiadany przez zamawiającego system Microsoft Information Protection, będący składową pakietu Microsoft Office 365 E3 (zgodnie z informacją udzieloną przez Zamawiającego, iż posiada pakiet Microsoft Office 365 E3). Zatem realizacja

funkcjonalności opisanej w pkt 30 ppkt 17 SWZ została przez Konsorcjum Comp potwierdzona, zaś powoływane przez Zamawiającego w uzasadnieniu odrzucenia informacje uzyskane ze strony internetowej producenta oprogramowania dotyczą funkcjonalności szyfrowania, a zatem nie mają znaczenia dla oceny zgodności oferty z warunkami zamówienia.

Stanowisko Zamawiającego.

Zamawiający odpowiedział na odwołanie, w którym wniósł o jego oddalenie jako bezzasadnego.

W ocenie Zamawiającego do spełnienia funkcjonalności systemu DLP niezbędne jest posiadanie przez zaoferowany produkt komponentu Cloud Access Security Broker (CASB), który zapewni spełnienie wymagań dla pkt 20, oraz uwzględni kontekst np. dla punktu 14.2 (przykładowo; czy pracownik A może przez komunikator Teams wysłać dane informacje do pracownika B). Brak licencji CASB de facto powoduje, że system DLP oferowany przez Odwołującego nie spełnia założeń Zamawiającego w zakresie kontroli nad sposobem korzystania ze swoich danych wysyłanych nie realizując identyfikowania i zwalczania cyber zagrożeń (brak kontroli nad przenoszeniem danych niezależnie od kierunku przesyłania danych). Zamawiający podkreślał, że usługa Microsoft Cloud App Security (licencja CASB) musi być natywnie zintegrowana z rozwiązaniem dotyczącymi zabezpieczeń i tożsamości. W przypadku infrastruktury Zamawiającego jest to AD (MS Active Directory), co w konsekwencji sprawia, że zapis „gdzie są informacje wysyłane" odnosi się de facto do kogo w aspekcie tej integracji. Zamawiający wskazywał, że Odwołujący przyznał, że złożona przez niego oferta nie zapewnia „funkcjonalności Discovery" dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online.", tj. wymagania opisanego w pkt 20 zd. 2. Odwołujący przyznał również, że jeśli z pkt 14 wynikałby wymóg uwzględnienia pojęcia „do kogo", to zaoferowanie licencji CASB byłoby niezbędne dla wypełnienia tego wymagania. W treści uzasadnienia zarzutu Odwołujący podaje mianowicie, że wymaganie przez Zamawiającego dostarczenia przez Odwołującego w ramach przedmiotu zamówienia licencji dla komponentu CASB jest nieuzasadnione. Standardowa licencja na oferowany produkt zapewnia spełnienie wymagań pkt I.1.14 SWZ, w szczególności podpunktu 14.2 zgodnie z jego faktycznym i literalnym brzmieniem. Licencja rozszerzona o wskazywany przez Zmawiającego CASB byłaby wymagana tylko, gdyby w treści pkt 14 jako okoliczność wymagającą uwzględnienia wskazano odbiorcę - okoliczność „do kogo" informacje są wysyłane". W ocenie Zmawiającego wymóg dostarczenia licencji CASB wynika z całego kontekstu punktu 14, a budowa punktu 14 w podziale na podpunkty sprawia, że wszystkie wskazane tam argumenty

należy traktować łącznie. Odwołujący bezpodstawnie zawęża przy tym branżowe znaczenie określenia „gdzie” sprowadzając je do „aplikacji, serwera przekazującego informację". W sposób nieuzasadniony wyklucza z zakresu pojęciowego tego określenia pojęcie „do kogo”. Wbrew tezom Odwołującego „kierunek” wysyłania informacji obejmuje swoim znaczeniem także użytkownika będącego odbiorcą informacji. Odpowiada to zresztą potocznemu znaczeniu sformułowania „gdzie”. W odpowiedzi na zapytanie „gdzie idziesz” wielokrotnie słyszymy odpowiedź wskazującą w sposób niekiedy bardzo precyzyjny konkretnego „adresata”, a nie wyłącznie miejsce (jak to sugeruje Odwołujący), jak np. „do kolegi”, „do M.”, „do lekarza". Uwzględnienie zgodnie z zasadami wykładni językowej znaczenia sformułowania „gdzie” nakazuje przyjęcie, iż obejmuje ono swoim zakresem znaczeniowym także określenie „do kogo". Podkreślenia wymaga, iż Odwołujący nie oferuje żadnego argumentu mogącego uzasadniać tezę, iż to znaczenie potoczne nie ma zastosowania dla „języka branżowego” właściwego dla przedmiotu postępowania. Mając na względzie wskazane wyżej reguły wykładni językowej, która winna mieć zastosowanie w sprawie niniejszej oraz nie budzące wątpliwości przyznanie przez samego Odwołującego, iż w przypadku w którym zakresem pojęciowym spornego wymagania SWZ należy objąć także „do kogo", to wówczas dla spełnienia wymagania SWZ niezbędne byłoby zaoferowanie licencji CASB, należy uznać, iż bezzasadne są zarzuty odwołania w zakresie referującym do niezgodności oferty z wymaganiem opisanym w Rozdziale I, podrozdział 1.1 pkt 14 SWZ.

Następnie Zamawiający odniósł się do uzasadnienia zarzutu odwołania w zakresie w jakim referuje on do niezgodności oferty Odwołującego z wymaganiem opisanym w Rozdziale I, podrozdział 1.1 pkt 20. ARiMR wskazał, że sporna jest między stronami wykładnia znaczenia zdania 2. Odwołujący twierdzi, że wymaganie to oznacza, iż „dostarczenie funkcjonalności Discovery dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online nie stanowiło zakresu przedmiotu zamówienia w ramach tego postępowania". Dostarczane rozwiązanie miało według Odwołującego jedynie zapewnić możliwość uzyskania licencji w takim rozszerzonym zakresie, co wywodzi ze sformułowania „funkcjonalność ta powinna być również oferowana”. Zamawiający wskazywał, że wszelkie użyte w opisie przedmiotu zamówienia w SWZ sformułowania takie jak: „musi umożliwiać", „musi realizować”, „powinien odbywać się", „musi wykorzystywać”, „musi zawierać", „powinien oferować”, „musi udostępniać", „powinien posiadać" wskazywały wymagane funkcjonalności oferowanego w ramach niniejszego postępowania systemu DLP. W przypadku funkcjonalności aplikacji, które nie zostały objęte niniejszym zamówieniem, posłużono się sformułowaniem „powinien posiadać możliwość rozbudowy”, co pozwoliłoby na rozwój systemu DLP w przyszłości (tzn. rozbudowę o inne niż wymienione w Rozdziale I, podrozdział 1.1 SWZ aplikacje SaaS i/lub funkcjonalności). W odniesieniu do usług

Discovery dla Exchange Online, Sharepoint Online (które są usługami SaaS), należy zauważyć, iż zawierają się ona w przedmiocie niniejszego zamówienia, na co wskazuje zapis w Rozdziale I, podrozdział 1.1 pkt 20 w zdaniu drugim, tj. „Funkcjonalność ta powinna być również oferowana dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online". Ponadto konieczność zaoferowania w bieżącym postępowaniu funkcjonalności Discovery dla usługi SaaS wynikała z wymagania określonego w Rozdziale I, podrozdział 1.1 pkt 29 SWZ: „29. Ochrona informacji w chmurze powinna opierać się o te same mechanizmy stosowane w rozwiązaniu lokalnym włączając Fingerprinting oraz Machine Learning." Dodatkowo w piśmie z dnia 5 maja 2020 r. znak: ZP.103.DPiZP.2610.30.2020.KaMa w sprawie wyjaśnienia SWZ, w odpowiedzi na pytanie nr 5 zadane przez Wykonawcę, Pyt. „Dotyczy punktu 1.1 SWZ podpunkt 20. Zdaniem Zamawiającego powyższe pytanie dowodzi tego, iż Wykonawcy, w tym sam Odwołujący, już na tym etapie odróżniał usługi od aplikacji w chmurze Microsoft. W opinii ARiMR potwierdzeniem obligatoryjności posiadania funkcjonalności opisanej przy pomocy sformułowania „powinna być oferowana" jest również wymaganie zawarte w Rozdziale I, podrozdział 1.1 pkt. 26, co do którego Wykonawca nie wskazał żadnych wątpliwości interpretacyjnych co do tego, czy jest ono objęte przedmiotem zamówienia. Zdaniem Zamawiającego nie sposób zgodzić się ze stanowiskiem Odwołującego wskazującym, że „Zgodnie z pkt 1.1.28 SWZ: „System powinien posiadać możliwość rozbudowy o ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS, w szczególności MS 0365 oraz Google for Business." Zamawiający wskazywał, zdaniem Odwołującego, że zakres ochrony aplikacji w chmurze, w tym pakietu Microsoft Office 365, pozostaje opcjonalnie jako możliwość rozbudowy, a zatem nie jest wymagane dostarczenie licencji w tym zakresie w ramach przedmiotowego zamówienia. Wymaganie nr 28 należy w jego ocenie zatem rozumieć jako wyłączające ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS poza zakres przedmiotowego zamówienia, stawiając jedynie wymóg zapewniania możliwości rozbudowy o taki zakres licencji.

W ocenie ARiMR powyższe stanowisko Odwołującego stanowi element taktyki procesowej, niezasadnie utożsamiając usługę i aplikację jako tożsamy produkt (nawet sam producent na swoich stronach www stosuje podział). Odwołujący mianowicie pomija fakt, iż Zamawiający w pkt 20 zdanie 2 wymieniał bardzo konkretnie usługi obecnie używane przez Zamawiającego z Microsoft Office 365, których obsługi wymaga od zamawianego systemu DLP (foldery Exchange, Exchange Online, Sharepoint, Sharepoint Online) nie wskazując całego szeregu pozostałych aplikacji wchodzących w skład tego pakietu. Natomiast w punkcie 28 zakładał możliwość rozbudowy o ochronę aplikacji, w szczególności MS 0365 oraz Google for Business. Innymi słowy zdaniem Zamawiającego Odwołujący dokonuje

zabiegu niezasadnego z punktu widzenia zapisów SWZ oraz z punktu widzenia zawartości Microsoft Office 365. Zabieg ten skutkuje wywołaniem wrażenia utożsamienia jako jednego produktu różnych usług oraz aplikacji wchodzących w skład MS 0365. Utożsamienie to jest bezzasadne. Zamawiający stwierdził, że wykładnia proponowana przez Odwołującego prowadzi do absurdalnego wniosku. Zgodnie z nią Zamawiający w jednym miejscu wskazać by miał, iż oczekuje możliwości rozbudowy o niektóre elementy pakietu MS 0365, tylko po to, żeby w innym miejscu wskazać na potrzebę zapewnienia rozbudowy uwzględniającej cały pakiet MS 0365. Takie sformułowanie wymagań należałoby zaś uznać za oczywiście niedorzeczne. Tym samym należy uznać, że wykładnia taka, jako prowadząca do wniosków niedorzecznych, absurdalnych jest nie do zaakceptowania jako poprawna z punktu widzenia podstawowych zasad dokonywania wykładni językowej. Stanowisko Odwołującego powoduje, że Zamawiający kupując system DLP, który miał objąć ochroną wszystkie komponenty obecnie wykorzystywane (enumeratywnie wyszczególnione w zapisie w Rozdziale I, podrozdział 1.1 pkt 20) de facto nie zapewniałby kompleksowej ochrony o usługi w chmurze. Koniunkturalność i sztuczność wykładni stworzonej przez Odwołującego na potrzeby postępowania i odwołania jawi się szczególnie wyraźnie w treści jego własnych wyjaśnień z dnia 28 czerwca 2021 r. złożonych w odpowiedzi na wezwanie Zamawiającego. Unaocznia ona w sposób jasny różnicę pomiędzy naturalnym rozumieniem pojęcia oferowania czegoś w przypadku wszelkich innych wymagań SWZ w postępowaniu przyjmowanym przez samego Odwołującego, a zupełnie sztuczną wykładnią wytworzoną przez niego na potrzeby zanegowania znaczenia spornego wymagania. A więc kolejno:

W ostatnim wersie na str. 1 wyjaśnień Odwołujący pisze o „modelu licencyjnym oferowanego pakietu (...)" w pkt 3 na str. 2 wyjaśnień Odwołujący wskazuje: „Potwierdzamy, że oferowane rozwiązanie spełnia wymagania pkt 1.1 pkt 5 SWZ(...)", a następnie: „potwierdzamy, iż oferowane rozwiązanie spełnia wymagania", w pkt 3 na str. 3 ponownie wskazuje na: „Oferowane rozwiązanie w pkt 4 na str. 3: „Okoliczność, iż oferowane jest (...)", w zd. 1 ostatniego akapitu punktu 5 na str. 4: „Innymi słowy, oferowane przez Wykonawcę rozwiązanie spełnia wymagania",

Zamawiający stwierdził, że nie ulega jakiejkolwiek wątpliwości, że w każdym z tych przypadków Odwołujący pisząc o czymś co jest „oferowane" ma na myśli to co zaoferował w swojej ofercie, a nie to co „jest oferowane na rynku". Dopiero w pkt 2 na str. 5 wyjaśnień Odwołujący dokonuje (podobnie jak obecnie w odwołaniu) całkowicie odmiennej wykładni znaczenia słowa „oferować". Wskazuje tamże, iż „ta funkcjonalność jest oferowana (dostępna w ofercie producenta), jednak nie jest elementem oferowanej licencji, gdyż Zamawiający nie wymagał jej dostarczenia w ramach obecnego postępowania". Co szczególnie widoczne, Odwołujący w tym samym zdaniu używa słowa „oferowana" w dwóch

zupełnie odmiennych znaczeniach. Twierdzi zarazem, że funkcjonalność jest oferowana (w ofercie producenta) i nie jest oferowana (w ofercie złożonej w postępowaniu). Zamawiający stwierdził, że sposób sformułowania tego zdania uwidacznia już sam w sobie sztuczność dokonywanej przez Odwołującego na potrzeby postępowania wykładni znaczenia słowa „oferowana" w świetle pkt 20 SWZ. Sam Odwołujący dokonać musiał tu bowiem koniecznych dodatkowych oznaczeń, dopełnień, dla nadania takiego, zupełnie odmiennego od przyjmowanego w zarówno w SWZ jak i zupełnie naturalnie w jego własnych wyjaśnieniach znaczenia. W jednym przypadku dodaje, że oferowana „w ofercie producenta", w drugim dodaje do oferowana „w ofercie złożonej w, postępowaniu". Nie ulega wątpliwości, że tego rodzaju dodatkowych elementów istotnie zmieniających znaczenie samodzielnie występującego słowa „oferowana" nie zawiera SWZ. Bez tego rodzaju zabiegów nie sposób z SWZ wywodzić znaczenia, jakie usiłuje mu nadawać Odwołujący w przypadku treści zd. 2 pkt 20.

Co więcej, proponowana przez Odwołującego interpretacja postanowień SWZ prowadziłaby do absurdalnych wniosków. Wystarczy tu wskazać na treść formularza ofertowego stanowiącego załącznik nr 1 do SWZ. W formularzu tym w drugiej kolumnie wpisane zostały „wymagane minimalne parametry systemu DLP". W kolumnie trzeciej zaś wskazano do zaznaczenia przez wykonawców TAK lub NIE „oferowany parametr". Zgodnie z wykładnią proponowaną przez Odwołującego należałoby więc uznać, że złożył on ofertę nie obejmującą żadnego z parametrów wymaganych, a jedynie informującą o ich dostępności w ofercie producenta.

Co znamienne w dalszej części wyjaśnień z 28 czerwca 2021 r. Odwołujący powraca do naturalnego znaczenia pojęcia „oferowany":

w ostatnim akapicie punktu 1 na str. 6 „wezwanie ma charakter wezwania dot. treści złożonej oferty i parametrów oferowanego rozwiązania", podobnie w pkt 2 wielokrotnie mowa o „oferowanym rozwiązaniu", w pkt 3 na str. 6 pisze: „potwierdzając i oświadczając o spełnianiu przez oferowane rozwiązanie", również w pkt 4na str. 7 mowa o „oferowanym rozwiązaniu"

Podobnie w innych elementach SWZ Wykonawca nie dopatruje się znaczenia jakie usiłuje nadać sformułowaniu wymagania z pkt 20.

Przykładowo w pkt 25 zostało ustanowione wymaganie zgodnie z którym „system powinien umożliwiać rozpoznawanie tekstu zawartego w plikach graficznych (OCR) i jego analizę pod względem wrażliwości informacji. Ta funkcjonalność powinna być oferowana co najmniej dla dokumentów graficznych wysyłanych poprzez styk z internetem (smtp, http, https)".

Zdaniem ARiMR zwraca tu uwagę szczególnie to, iż podobnie jak w wymaganiu w pkt 20 w dwóch zdaniach składających się na opis wymagania posłużono się innymi zwrotami (w zdaniach pierwszych mowa jest o tym, że system ma coś umożliwiać, a w obu zdaniach drugich mowa jest o tym, że coś ma być oferowane). Wykonawca nie twierdzi zaś w przypadku wymagania opisanego w pkt 25, iż część wyspecyfikowana w zdaniu drugim nie jest objęta przedmiotem zamówienia, lecz ma pozostawać jedynie „w ofercie producenta" i w tym sensie „być oferowana". Jest to więc kolejny element wskazujący na całkowitą sztuczność wykładni dokonywanej przez Odwołującego w stosunku do treści wymagania z pkt 20.

Kolejno Zamawiający podniósł, że w Rozdziale I, podrozdział 1.1 SWZ w wymaganiach dotyczących zakresu ochrony informacji określonych w pkt. 30 w pkt. 17 wskazano, iż system powinien posiadać funkcjonalność wymuszania szyfrowania poczty elektronicznej. Wymaganie to, w odpowiedzi na pytanie nr 12 zadane przez Wykonawcę, zostało doprecyzowane w piśmie z dnia 5 maja 2020 r. znak: ZP.103.DPiZP.2610.30.2020.KaMa w sprawie wyjaśnienia SWZ, w następujący sposób „Zamawiający potwierdza, że oczekuje, aby narzędzie klasyfikacji było elementem oznaczania wiadomości email do zaszyfrowania". Odwołujący wskazywał w uzasadnieniu zarzutu, że „nigdzie w SWZ nie wskazano, aby takie narzędzie do szyfrowania (czy też funkcjonalność szyfrowania) miało zostać dostarczone w ramach zamawianej usług". W ocenie Zamawiającego teza powyższa jest niezgodna ze stanem faktycznym. Odwołujący dokonuje wykładni wymagania opisanego w pkt I.1.30.17 SWZ w oderwaniu od pozostałych wymagań opisanych w tejże SWZ. W szczególności należy więc tu wskazać na konieczność wykładania powyższego wymagania bez pomijania treści wymagania opisanego w pkt 12.4 SWZ, zgodnie z którym „system DLP musi umożliwiać tworzenie polityk uwzględniających takiej akcje jak szyfrowanie informacji". Tworzenie polityk przez system DLP nie jest samo w sobie celem a jedynie środkiem do osiągnięcia celu jakim jest opisana w pkt.12.4 możliwość zaszyfrowania emaila/informacji. Należy wyraźnie zaznaczyć, że pozostałe podpunkty tj. 12.1 -12.2- 12.3 są analogicznie opisane i tu Odwołujący nie miał wątpliwości co do intencji Zamawiającego, tzn., że Zamawiający oczekiwał od systemu wykonania konkretnej akcji przez system na podstawie zdefiniowanych polityk a nie stworzenie samych polityk. Poczta elektroniczna o której mowa w pkt I.1.30.17 jest jednym z nośników informacji o których mowa w pkt 12.4 SWZ. Szyfrowanie informacji w systemach DLP jest stosowane nie tylko do wiadomości email, ale również w przypadku zapisywania chronionych danych na nośniki USB, dyski twarde i nośniki zewnętrzne. Mowa tu o szyfrowaniu wszelkich informacji jako takich, także tych przekazywanych pocztą elektroniczną. Wymaganie wymuszania szyfrowania poczty elektronicznej w połączeniu z wymaganiem umożliwiania przez system

tworzenia polityk uwzględniających w szczególności szyfrowanie informacji (wszelkich, a więc także tych przekazywanych pocztą elektroniczną), prowadzi do wniosku, zgodnie z którym, aby system spełniał łącznie te ww. wymagania SWZ musi on posiadać narzędzie, które zapewni również realizację funkcjonalności szyfrowania poczty elektronicznej.

W toku postępowania odwoławczego również Przystępujący złożył pismo procesowe, w którym wnosił o oddalenie odwołania i na poparcie swojego stanowiska przestawił stosowną argumentację.

Uwzględniając dokumentację postępowania o udzielenie zamówienia przedstawioną przez Zamawiającego, dowody oraz oświadczenia i stanowiska Stron i Przystępującego wyrażone w pismach procesowych oraz na rozprawie Izba ustaliła, co następuje.

Przedmiotem zamówienia jest zakup przez ARiMR usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (ang. DLP - Data Loss Protection, dalej „system DLP") i 300 godzin konsultacji.

W Rozdziale I. „Przedmiot zamówienia" podrozdziale I.1. „Opis przedmiotu zamówienia" Zamawiający sprecyzował m. in.:

„9. System musi umożliwiać monitorowanie i ochronę wielu typowych kanałów komunikacyjnych, w szczególności:

9.1. http oraz https,

9.2. email,

9.3. komunikatory internetowe. (…).

12. System musi umożliwiać tworzenie polityk uwzględniających takie akcje jak: (…)

12.4. szyfrowanie informacji, (…).

14. System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:

14.1. kto wysyła informacje,

14.2. gdzie informacje są wysyłane,

14.3. w jaki sposób informacje są wysyłane,

14.4. co jest wysyłane, czyli właściwa identyfikacja treści. (…).

20. System musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego (funkcjonalność Discovery). Funkcjonalność ta powinna być również oferowana dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online. (…).

28. System powinien posiadać możliwość rozbudowy o ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS, w szczególności MS O365 oraz Google for Business.

30. System musi posiadać funkcjonalność klasyfikowania informacji (w tym plików oraz wiadomości pocztowych email), lub w pełni integrować się z takim rozwiązaniem.

W zakresie klasyfikacji informacji, o której mowa w pkt. 30 powyżej, system powinien posiadać następujące funkcje: (…)

17. Wymuszanie szyfrowania poczty elektronicznej. (…)".

Z ustaleń Izby wynika, że Zamawiający pismem z dnia 1 czerwca 2021 r. wezwał Odwołującego do złożenia wyjaśnień dotyczących podejrzenia występowania w jego ofercie ceny rażąco niskiej. Pismem z dnia 9 czerwca 2021 r. Wykonawca złożył stosowne wyjaśnienia. W wyniku wyjaśnień złożonych przez Wykonawcę Zamawiający doszedł do wniosku, że wystąpiła konieczność uzyskania dodatkowych wyjaśnień, o które wystąpił do Konsorcjum Comp pismem z dnia 21 czerwca 2021 r. W odpowiedzi na to wezwanie Odwołujący złożył wyjaśnienia w piśmie z dnia 28 czerwca 2021 r.

Zamawiający pismem z dnia 26 lipca 2021 r. poinformował Odwołującego o odrzuceniu jego oferty jako niezgodnej z warunkami zamówienia.

W toku rozprawy zostały złożone następujące dowody:

1. oświadczenie producenta z dnia 8 września 2021 r. na okoliczności wskazane na stronie 1 złożonego dowodu wraz z dokumentem potwierdzającym, że wystawca oświadczenia, jest przedstawicielem producenta w Polsce.
2. wydruk ze strony Microsoft, w treści którego dla produktu Microsoft 365 Business Standard w zakresie dostępnych usług wymieniono foldery wskazane przez zamawiającego w pkt 20 SWZ.

Izba zważyła, co następuje.

Krajowa Izba Odwoławcza stwierdza, że Odwołujący legitymuje się uprawnieniem do korzystania ze środków ochrony prawnej, o którym stanowi przepis art. 505 ust. 1 Pzp, według którego środki ochrony prawnej określone w ustawie przysługują wykonawcy, uczestnikowi konkursu, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów niniejszej ustawy.

Izba za konieczne uznała przytoczenie przepisów Pzp, których naruszenie Zamawiającemu zarzucał Odwołujący, które zostały powołane poniżej.

Art. 16 Pzp Zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób:

1) zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie wykonawców;

2) przejrzysty;

3) proporcjonalny.

Art. 226 ust. 1 pkt 5 Pzp Zamawiający odrzuca ofertę, jeżeli: treść jest niezgodna z warunkami zamówienia;

W oparciu o ustalony stan faktyczny sprawy Izba stwierdziła, że zarzuty odwołania w części okazały się zasadne.

Na wstępie Izba wskazuje, że chybione są twierdzenia Odwołującego zasadzające się na tym, że Zamawiający dokonując odrzucenia oferty Odwołującego dopuścił się naruszenia zasad równego traktowania wykonawców i uczciwej konkurencji, ponieważ jedynie względem Konsorcjum Comp przeprowadził szczegółową procedurę badania złożonej przez tego wykonawcę oferty. Z ustaleń dokonanych przez Izbę wynika, że procedurę badania oferty pod kątem występowania w niej ceny rażąco niskiej Zamawiający prowadził nie tylko względem wykonawcy Comp, ale również w stosunku do Przystępującego. Natomiast w tym względzie treść wyjaśnień złożonych przez Odwołującego spowodowała konieczność wystąpienia przez Zamawiającego o dalsze wyjaśnienia w aspekcie stwierdzenia, czy oferta ta jest zgodna z warunkami zamówienia ustalonymi przez Zamawiającego w ramach prowadzonego postępowania. W związku z tym nie sposób czynić Zamawiającemu zarzutu, że dążył do wyjaśnienia wszelkich wątpliwości związanych z

rozwiązaniem zaoferowanym przez Konsorcjum Comp. Wręcz przeciwnie. Izba ocenia tego rodzaju postępowanie Zamawiającego jako wzorcowe i zmierzające do ustalenia jego zgodności z ustalonymi warunkami zamówienia, co ma bezpośrednie przełożenie na otrzymanie przez Zamawiającego produktu zgodnego z postawionymi wymaganiami.

Wszechstronna i wyczerpująca analiza zarzutów zgłoszonych w odwołaniu przeprowadzona przez Izbę doprowadziła do wniosku, że z trzech zarzutów dwa uznała za nieuzasadnione, tj. zarzuty dotyczący niezasadnego odrzucenia oferty Odwołującego z powodu niespełnienia wymagań Zamawiającego odnoszących się do:

- budowanie polityk ochrony informacji z uwzględnieniem kierunku przepływu informacji (Rozdział I podrozdział I.1. pkt 14.2 SWZ)
- zaoferowania funkcjonalności Discovery dla aplikacji typu SaaS (Rozdział I podrozdział I.1. pkt 20 SWZ).

W omawianym zakresie Izba nie stwierdziła naruszenia przepisu art. 226 ust. 1 pkt 5 Pzp w zw. z art. 16 ust. 1-3 Pzp polegającego na niezasadnym odrzuceniu oferty Odwołującego.

W tym miejscu zasadnym jest odniesienie się przez Izbę do zastrzeżeń Odwołującego zgłoszonych podczas rozprawy, który stwierdził, że argumentacja zaprezentowana przez Zamawiającego wykracza poza podstawy odrzucenia jego oferty zawarte w informacji przekazanej Odwołującemu w piśmie z dnia 26 lipca 2021 r. W omawianym zakresie Izba przyznała rację Odwołującemu, ale jedynie w odniesieniu do podstawy odrzucenia związanej z zapewnieniem funkcjonalności wymuszania szyfrowania poczty elektronicznej.

Zwrócić uwagę należy, że w ww. piśmie Zamawiający czynność odrzucenia oferty Odwołującego powiązał z niespełnieniem wymogu zawartego w SWZ do Rozdziale I podrozdziału I.1.30 pkt 17, w którym wskazano, że system powinien posiadać funkcjonalność wymuszania szyfrowania poczty elektronicznej. Ponadto Zamawiający wskazał, że jeden z dokumentów, który został złożony przez Odwołującego wraz z wyjaśnieniami z dnia 28 czerwca 2021 r. został sporządzony i przedstawiony w języku obcym bez tłumaczenia na język polski. Natomiast w odpowiedzi na odwołanie oraz w toku rozprawy Zamawiający odwoływał się do wymogu zawartego w SWZ w Rozdziale I podrozdziale I.1. w pkt 12.4, w którym stwierdzono, że „System musi umożliwiać tworzenie polityk uwzględniających takie akcje jak: szyfrowanie informacji”. Z tym że, tego rodzaju argumentacji wpierającej się o pkt 12.4 SWZ Zamawiający nie uczynił podstawą odrzucenia oferty Odwołującego. Z tych

względów Izba uznała ww. argumentację Zamawiającego za niedopuszczalne rozszerzenie podstaw odrzucenia oferty Odwołującego. W toku rozprawy Odwołujący oświadczył, że rozwiązanie, które zaoferował spełnia wymóg zawarty w Rozdziale I podrozdziału I.1.30 pkt 17 dotyczący posiadania funkcjonalności wymuszania szyfrowania poczty elektronicznej. Zamawiający nie zaprzeczył temu, a jedynie powołując się na treść Rozdziału I podrozdziału I.1. pkt 12.4 twierdził, że nie spełnia ono wymogu szyfrowania poczty elektronicznej. Z tych względów Izba uznała zgłoszony zarzut za uzasadniony.

W pozostałym zakresie Izba uznała zastrzeżenia Odwołującego za bezzasadne, a stanowisko Zamawiającego za konsekwentne i spójne z treścią pisma z dnia 26 lipca 2021 r. Wobec tego Izba nie doszukała się nowych okoliczności ponad te wskazane w ww. piśmie zawierającym podstawy i uzasadnienie odrzucenia oferty Odwołującego. I tak. W przypadku zarzutu Odwołującego, że argumentacja o kierunku przesyłania informacji nie została zawarta w piśmie z dnia 26 lipca 2021 r. Izba przytacza jej stosowną część (str.1): „Do spełnienia wskazanych funkcjonalności systemu DLP niezbędne jest posiadanie przez zaoferowany produkt komponentu Cloud Access Security Broker (CASB), który zapewni spełnienie wymagań dla pkt 20, oraz uwzględni kontekst np. dla punktu 14.2 (przykładowo: czy pracownik A może przez komunikator Teams wysłać dane informacje do pracownika B)". Do podobnego przykładu Zamawiający odwołał się w piśmie z dnia 21 czerwca 2021 r. zawierającym prośbę o złożenie wyjaśnień przez Odwołującego.

Następnie wskazać należy, że w piśmie z dnia 26 lipca 2021 r. (str. 2) Zamawiający podał również: „Zamawiający wskazuje, iż przywołany przez Wykonawcę kontekst słowa „gdzie" odnosi się do wskazania lokalizacji aplikacji, w której przesyłane są informacje. Biorąc pod uwagę całościowy zapis wymagania określonego w Rozdziale I, podrozdział 1.1 pkt. 14 określenie „gdzie" oznacza kierunek przepływu informacji, czyli, „do kogo" informacje są wysyłane".

Wobec tego Izba w omawianym zakresie (pkt. 14.2 oraz 20) nie stwierdziła, aby Zamawiający rozszerzył podstawy odrzucenia ponad te wskazane w piśmie z dnia 26 lipca 2021 r. Natomiast stanowisko zawarte w odpowiedzi na odwołanie oraz prezentowane na rozprawie Izba uznała za argumentację wspierającą podstawy odrzucenia, które zostały opisane przez Zamawiającego w piśmie powołanym wyżej.

Powracając do analizy pozostałych zarzutów odwołania, które nie zostały przez Izbę uznane za uzasadnione Izba prezentuje następujące stanowisko, które zostało wyrażone poniżej.

1. Budowanie polityk ochrony informacji z uwzględnieniem kierunku przepływu informacji (Rozdział I podrozdział I.1. pkt 14.2 SWZ).

Nie było sporne między stronami, że Zamawiający w Rozdziale I podrozdziale I.1. pkt 14 SWZ sprecyzował, że system musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak: gdzie informacje są wysyłane.

W treści odwołania Odwołujący podniósł, że Zamawiający posługując się określeniem „gdzie informacje są wysyłane" sformułował wymaganie, aby system umożliwiał budowanie polityk ochrony informacji uwzględniając wyłącznie lokalizację lub miejsce przepływu informacji.

W rozpoznawanym zakresie Izba stanęła na stanowisku, że wymaganie postawione przez Zamawiającego w pkt 14.2, należy odczytywać literalnie nie pomijając przy tym kontekstu w jakim informacje są używane, tj., gdzie informacje są wysyłane. Izba stwierdziła, że przez takie ukształtowanie omawianego wymagania Zamawiający chciał sobie zapewnić kontrolę nad kierunkiem przesyłania informacji. Zatem słusznie Zamawiający oczekiwał od wykonawców składających oferty w tym postępowaniu, mającym służyć ochronie zasobów informacyjnych i danych przed wyciekiem, iż zaoferowane systemy będą potrafiły rozróżniać kierunki przepływu informacji. Z tych względów niezbędnym było zaoferowanie komponentu CASB, który w przypadku przesyłania informacji przez komunikatory internetowe potrafi rozpoznać kierunek przesyłania informacji. Podkreślić należy przy tym, że nie budziło żadnych wątpliwości, że wymóg z pkt 14 SWZ dotyczył nie tylko kanałów komunikacyjne takich jak: e-mail czy też http lub też https, ale również komunikatorów internetowych (pkt 9 w Rozdziale I podrozdziale I.1 SWZ).

Izba podziela zapatrywania Przystępującego, że posłużenie się w tym przypadku stwierdzeniem „do kogo" nie byłoby do końca trafne, ponieważ dotyczyłoby danych ściśle związane z konkretnym podmiotem, np. dane o IP odbiorcy. Zresztą sam Odwołujący w treści złożonego odwołania wskazuje, że *„Kierunek wysyłania informacji cyfrowych nie jest powiązany bezpośrednio z użytkownikiem, a wynika ze sposobu działania całej infrastruktury, np. kierunkiem może być firma/aplikacja/serwer, do którego jest informacja wysyłana a konkretny użytkownik definiowany jest jako odbiorca informacji".* Powyższy wywód wydaje się potwierdzać słuszność użycia w pkt 14.2 przez Zamawiającego określenia „gdzie", a nie „do kogo" skoro kierunek wysłania informacji nie jest powiązany bezpośrednio z użytkownikiem. Wobec tego Izba stwierdziła, że Zamawiający odnosząc się do kierunku przesyłu informacji użył więc odpowiedniego określenia „gdzie". W omawianym zakresie Izba

nie dopatrzyła się ze strony Zamawiającego nadinterpretacji wymogu opisanego w pkt 14.2 SWZ.

Jednocześnie dostrzec należy, że Zamawiający posługując się słowem „gdzie" zamiast „do kogo" przesądził, że jego celem było zapewnić sobie możliwość kontroli kierunku przepływu danych a nie informacji o IP odbiorcy. Powyższe zostało również potwierdzone przez Zamawiającego w toku rozprawy, który w odpowiedzi na pytanie Przewodniczącej potwierdził ww. interpretację postanowień pkt 14.2 SWZ.

Podkreślenia wymaga, że w toku rozprawy Odwołujący potwierdził, że rozwiązanie, które zaoferował nie zapewnia omawianej funkcjonalności (w tym nie obejmuje komponentu CASB), co w ocenie izby przesądza o tym, że jego oferta jest niezgodna z warunkami zamówienia, w konsekwencji podlega odrzuceniu na podstawie art. 226 ust. 1 pkt 5 Pzp. Konsekwencją takiego zapatrywania jest stwierdzenie prawidłowości czynności Zamawiającego polegającej na odrzuceniu oferty Konsorcjum Comp.

2. <u>Zaoferowania funkcjonalności Discovery dla aplikacji typu SaaS (pkt I.1.20 SWZ).</u>

Po dokonaniu wnikliwej i dogłębnej analizy materiału dowodowego zgromadzonego w sprawie Izba nie podziela zapatrywań Odwołującego, że oferowany przez niego system musi posiadać funkcjonalność Discovery wyłącznie w zakresie informacji zawartych na serwerach i stacjach końcowych w sieci Zamawiającego. Natomiast funkcjonalność Discovery nie musi być zapewniona w stosunku do folderów Exchange, Exchange Online, Serwera SharePoint, SharePont Online (które są usługami SaaS).

Nie budzi żadnych wątpliwości Izby, że treścią pkt 20 SWZ Zamawiający nałożył na wykonawców ubiegających się o udzielenie zamówienia obowiązek zaoferowania systemu, który będzie posiadał funkcjonalność Discovery nie tylko w wyłącznie w zakresie informacji zawartych na serwerach i stacjach końcowych w sieci Zamawiającego, ale również w stosunku do folderów Exchange, Exchange Online, Serwera SharePoint, SharePont Online. Wynika to wprost ze zdania drugiego pkt 20 SWZ, w którym Zamawiający jednoznacznie podał, że funkcjonalność ta powinna być również oferowana dla poszczególnych ww. folderów. Nie było sporne między stronami, że foldery te są w posiadaniu i funkcjonują już u Zamawiającego, jak również to, że mieszczą się w ramach rozwiązania Microsoft 365. Tym samym należy uznać za chybioną argumentację Odwołującego, który twierdził, że stwierdzenie, iż funkcjonalność Discovery powinna być również oferowana dla folderów

Exchange, Exchange Online, serwera SharePoint, Sharepoint Online należy odczytywać niejako „na przyszłość”.

Powyższego rozumienia nie zmienia również treść pkt 28 SWZ, ponieważ należy go odczytywać z uwzględnieniem pkt 20, którego treść jest jednoznaczna. W tym kontekście za racjonalne i przekonywujące należy uznać wyjaśnienia Zamawiającego, który stwierdził, że intencjonalnie rozdzielił treść obu tych wymagań. Zgodzić się należy z Przystępującym, który stwierdził, że „pkt I.1.20 zd. 1 swz wymaga ściśle - zautomatyzowanego wykrywania informacji objętych politykami ochrony, co wyraża się w opisywanej szeroko w niniejszym piśmie funkcji Discovery. Natomiast pkt I.1.28 swz stanowi o ochronie informacji przechowywanych w aplikacjach oferowanych jako SaaS. Z porównania treści obu pkt swz wynika ewidentny wniosek, że zakres wymogów określonych w tych punktach nie jest tożsamy. Zamawiający w pkt I.1.20 zd. 2 swz wymaga funkcjonalności Discovery dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online. Natomiast w pkt I.1.28 zamawiający odnosi się do dalszej ochrony informacji przechowywanej w aplikacjach oferowanych jako SaaS. O ile funkcja Discovery dla aplikacji SaaS powinna zostać zaoferowana bazowo przez wykonawcę, to w odniesieniu do dalszej ochrony informacji przechowywanych w aplikacjach oferowanych jako SaaS zamawiający wymaga jedynie możliwości rozbudowy”.

Izba za chybioną uznała argumentację Odwołującego wspierającą się na postanowieniach wzoru umowy, ponieważ z ich treści nie płyną wnioski na które powołuje się Wykonawca, a co najwyżej należy dokonywać interpretacji w aspekcie lokalizacji realizacji prac, co zresztą słusznie zauważył zarówno Zamawiający jak i Przystępujący.

Względy opisane powyżej doprowadziły Izbę do wniosku, że wskazana w pkt 28 możliwość rozbudowy systemu nie dotyczy wymagania funkcjonalności Discovery dla folderów wskazanych w pkt 20, tj. Exchange, Exchange Online, Serwera SharePoint, SharePont Online, która zawiera się w ramach obecnego zamówienia i nie może być odczytywana jako taka, mam być oferowana dopiero w przyszłości. Tym samym system, który jedynie zapewnia możliwość rozbudowy na przyszłości należy uznać za taki który nie spełnia wymagań Zamawiającego, a zatem oferta ofertę zawierającą takie rozwiązanie należy uznać za podlegającą odrzuceniu na podstawie art. 226 ust. 1 pkt 5 Pzp, jako nie niezgodną z warunkami zamówienia.

Odnosząc się do dowodu złożonego przez Odwołującego w postaci oświadczenia pochodzącego od dystrybutora producenta systemu zaoferowanego przez Odwołującego w zakresie interpretacji spornych postanowień SWZ Izba stwierdziła, że stanowisko ww.

podmiotu należy traktować z dużą ostrożnością z uwagi na to, że podmiot ten jako oferujący rozwiązanie zawarte w ofercie Odwołującego jest zainteresowany tym, aby to właśnie Odwołujący uzyskał zamówienie, ponieważ w takim przypadku nabędzie o określone produkty tego właśnie producenta. Z tych względu za uzasadnione należy uznać stwierdzenie zarówno Zamawiającego jak i Przystępującego, że ww. oświadczenie powinno być traktowane nie jako dowód pochodzący od bezstronnego podmiotu a raczej jako stanowisko własne Odwołującego.

Biorąc pod uwagę powyższe Izba stwierdziła, że w sytuacji, gdy nie potwierdziły się dwa zarzuty naruszenia art. 226 ust. 1 pkt 5 Pzp to powoduje to, że w mocy pozostaje czynność Zamawiającego polegająca na odrzuceniu oferty Odwołującego. Bez wpływu na wynik pozostaje okoliczność związana z uznaniem przez Izbę za zasadny jednego z zarzutów, bowiem nie spowoduje to przywrócenia oferty Odwołującego do postępowania. Skutkiem powyższego była konieczność oddalenia odwołania.

Zgodnie z art. 557 Pzp, w wyroku oraz w postanowieniu kończącym postępowanie odwoławcze Izba rozstrzyga o kosztach postępowania odwoławczego. Z kolei w świetle art. 575 Pzp strony oraz uczestnik postępowania odwoławczego wnoszący sprzeciw ponoszą koszty postępowania odwoławczego stosownie do jego wyniku. W związku z tym Izba kosztami postepowania odwoławczego w sprawie o sygn. akt KIO 2362/21 zgodnie z art. 575 Pzp oraz § 2 ust. 1 pkt 2 w zw. z § 5 ust. 1 oraz § 8 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. z 2020 r. poz. 2437) obciążyła Odwołującego. Izba wskazuje, że na koszty postępowania odwoławczego w kwocie 15 000 zł, na którą składał się koszt wpisu od odwołania uiszczony przez Odwołującego.

Mając powyższe na uwadze, orzeczono jak w sentencji.

Przewodniczący: ……..…