Sygn. akt: KIO 156/19

WYROK

z dnia 14 lutego 2019 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: **Luiza Łamejko**

Jolanta Markowska

Małgorzata Matecka

Protokolant: Piotr Cegłowski

po rozpoznaniu na rozprawie w dniu 11 lutego 2019 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 28 stycznia 2019 r. przez wykonawcę **Meritum Grupa Budowlana spółka z ograniczoną odpowiedzialnością spółka komandytowa, ul. Jugowicka 8A, 30-443 Kraków** w postępowaniu prowadzonym przez **Gminę Mikołów, ul. Rynek 16, 43-190 Mikołów**

orzeka:

1. **Uwzględnia odwołanie i nakazuje zamawiającemu Gminie Mikołów unieważnienie czynności unieważnienia postępowania oraz unieważnienie czynności odrzucenia oferty złożonej przez Meritum Grupa Budowlana spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Krakowie i dokonanie powtórnej czynności oceny oferty,**

2. kosztami postępowania obciąża **Gminę Mikołów, ul. Rynek 16, 43-190 Mikołów** i:

2.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **20 000 zł 00 gr** (słownie: dwadzieścia tysięcy złotych zero groszy) uiszczoną przez wykonawcę **Meritum Grupa Budowlana spółka z ograniczoną odpowiedzialnością spółka komandytowa, ul. Jugowicka 8A, 30-443 Kraków** tytułem wpisu od odwołania,

2.2. zasądza od **Gminę Mikołów, ul. Rynek 16, 43-190 Mikołów** na rzecz **Meritum Grupa Budowlana spółka z ograniczoną odpowiedzialnością spółka komandytowa, ul. Jugowicka 8A, 30-443 Kraków** kwotę **23 600 zł 00 gr** (słownie: dwadzieścia trzy tysiące sześćset złotych zero groszy) poniesioną tytułem wpisu od odwołania oraz wynagrodzenia pełnomocnika.

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2018 poz. 1986 ze zm.) na niniejszy wyrok - w terminie 7 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Katowicach.

Przewodniczący : **……**

……

……

Sygn. akt: KIO 156/19

U z a s a d n i e n i e

Gmina Mikołów (dalej: „Zamawiający”) prowadzi w trybie przetargu nieograniczonego postępowanie o udzielenie zamówienia publicznego pn. „Roboty budowlane w budynku przy ul. Jana Pawła II 4 w Mikołowie. Postępowanie to prowadzone jest na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 poz. 1986 ze zm.), zwanej dalej: „ustawa Pzp”. Ogłoszenie o zamówieniu zostało opublikowane w dniu 30 października 2018 r. w Dzienniku Urzędowym Unii Europejskiej pod pozycją 2018/S 209-476346.

W dniu 28 stycznia 2019 r. wykonawca Meritum Grupa Budowlana spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Krakowie (dalej: „Odwołujący”) wniósł do Prezesa Krajowej Izby Odwoławczej odwołanie wobec czynności Zamawiającego polegających na odrzuceniu oferty Odwołującego oraz unieważnieniu postępowania o udzielenie zamówienia publicznego.

Odwołujący zarzucił Zamawiającemu naruszenie:

• art. 89 ust. 1 pkt 7 ustawy Pzp w zw. z art. 10a ust. 5 ustawy Pzp w zw. z art. 7 ust. 1 ustawy Pzp poprzez niezasadne odrzucenie oferty Odwołującego w związku z bezpodstawnym przyjęciem, że oferta Odwołującego jest nieważna na podstawie odrębnych przepisów, tj. art. 137 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2016.1579 (dalej jako: uzoie), z uwagi na (rzekome) opatrzenie dokumentów dołączonych do oferty podpisem kwalifikowanym wykorzystującym algorytm skrótu SHA-1, który w ocenie Zamawiającego, skutkuje nieważnością złożonego podpisu,

• art. 10a ust. 5 ustawy Pzp w zw. z art. 22 Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (dalej: dyrektywa klasyczna) poprzez niezasadne przyjęcie, że dla skutecznego złożenia oferty w postępowaniu niezbędnym jest opatrzenie jej kwalifikowanym podpisem elektronicznym wykorzystującym algorytm skrótu inny aniżeli SHA-1, kiedy to obwiązek ten nie wynika z przepisów obowiązującego prawa,

a w konsekwencji również art. 93 ust. 1 pkt 1 ustawy Pzp poprzez niezasadne unieważnienie postępowania z uwagi przyjęcie, że w postępowaniu nie złożono żadnej oferty

niepodlegającej odrzuceniu,

- art. 7 ust. 1 ustawy Pzp poprzez naruszenie zasady uczciwej konkurencji oraz równego traktowania wykonawców przejawiającej się w przerzuceniu na Odwołującego konsekwencji związanych z niewykorzystywaniem przez portal smartpzp kwalifikowanego podpisu elektronicznego z algorytmem SHA-256,

- art. 7 ust. 1 ustawy Pzp w zw. z art 10a ust. 5 ustawy Pzp poprzez niezasadne przyjęcie, że algorytm skrótu kwalifikowanego podpisu elektronicznego Odwołującego to SHA-1, kiedy to weryfikacja ww. okoliczności wykazuje, że algorytm ten to SHA-256.

Uzasadniając postawione zarzuty Odwołujący wskazał, że składanie ofert w postępowaniu odbywało się za pośrednictwem komercyjnego portalu smartpzp.pl. Zgodnie z instrukcją korzystania z tego portalu, złożenie oferty polegało na wypełnieniu formularza oferty zamieszczonego bezpośrednio na portalu. W postępowaniu jako treść oferty Zamawiający żądał złożenia m.in. kosztorysu ofertowego, jednolitego dokumentu oraz oświadczenia o ochronie danych osobowych, które należało opatrzyć kwalifikowanym podpisem elektronicznym i dołączyć do dokumentów składanych wraz z ofertą. Odwołujący stwierdził, że złożył ofertę zgodnie z instrukcją korzystania z portalu smartpzp, oraz zgodnie z instrukcją Zamawiającego.

Odwołujący podał, że Zamawiający w dniu 18 stycznia 2018 r. poinformował Odwołującego o odrzuceniu jego oferty. W uzasadnieniu decyzji Zamawiający wskazał, że w trakcie badania i oceny oferty Zamawiający natrafił na trudności z weryfikacją kwalifikowanego podpisu elektronicznego złożonego za pośrednictwem aplikacji zaimplementowanej w funkcjonalności portalu smartpzp.pl, czego skutkiem było wystąpienie do podmiotu zarządzającego portalem o wyjaśnienie kwestii weryfikacji złożonego podpisu. Weryfikacja podpisów dokumentów i oświadczeń złożonych wraz z ofertą (JEDZ, kosztorysy ofertowe) wykazała ich prawidłowość. Zamawiający wskazał, że przedstawiciel portalu smartpzp w dniu 18 grudnia 2018 r. jednoznacznie stwierdził że „nie ma możliwości aby Wykonawca złożył ofertę w trybie przetargu nieograniczonego, bez potwierdzenia jej podpisem elektronicznym”. O prawidłowości złożonego podpisu miał świadczyć również raport z czynności złożenia oferty wygenerowany przez portal - plik 00006PN1E2018.pdf. Bazując na tym oświadczeniu, Zamawiający w dniu 9 stycznia 2019 r. dokonał czynności wyboru oferty Odwołującego.

Jak zauważył Odwołujący, w tym samym dniu, zgodnie z ww. uzasadnieniem,

Zamawiający powziął informację o wyroku Krajowej Izby Odwoławczej z dnia 10 grudnia 2018 r., sygn. akt KIO 2428/18, który zinterpretował w ten sposób, że za wadliwy i skutkujący obowiązkiem odrzucenia oferty uznać należy kwalifikowany podpis elektroniczny złożony przy zastosowaniu algorytmu skrótu podpisu SHA-1. Zamawiający wystąpił więc ponownie do podmiotu zarządzającego portalem smartpzp o przekazanie oświadczenia, jakiego rodzaju algorytmu skrótu podpisu użyto przy składaniu podpisu kwalifikowanego dla oferty Meritum Grupa Budowlana Sp. z o.o. Sp.k.

W dniu 14 stycznia 2019 r. Prezes Zarządu podmiotu zarządzającego portalem Portal PZP Sp. z o.o. jednoznacznie oświadczyła, że na dzień składania ofert (6 grudnia 2018 r.) portal wykorzystywał podpis z funkcjonalnością skrótu SHA-1. Dodatkowo, 16 stycznia 2019 r. podmiot zarządzający portalem poinformował, że dopiero od 20 grudnia 2018 r. portal wykorzystuje podpis z funkcjonalnością skrótu SHA-256.

Odwołujący wskazał, że zdaniem Zamawiającego, kwestia prawidłowości wykorzystywanych skrótów podpisów elektronicznych została uregulowana w art 137 uzoie. W przepisie tym, w ocenie Zamawiającego, ustawodawca jednoznacznie wskazał, że do składania zaawansowanych podpisów elektronicznym można stosować funkcję skrótu SHA-1 tylko do 1 lipca 2018 r. i w ust. 2 tego artykułu nałożył na producentów oprogramowania obowiązek dostosowania oferowanych przez nich produktów do wskazanego powyżej terminu i wymagań. Zamawiający w uzasadnieniu odrzucenia oferty Odwołującego zauważył, że podmiot zarządzający portalem smartpzp wypełnił ten wskazany obowiązek ustawowy dopiero 20 grudnia 2018 r., czego konsekwencją było złożenie podpisu elektronicznego w dniu 6 grudnia 2018 r. za pośrednictwem portalu z wykorzystaniem niedozwolonej funkcji skrótu SHA-1. Zamawiający przyjął, że Odwołujący składając podpis za pośrednictwem portalu, nie miał wpływu na to, jakiej funkcji skrótu podpisu używa portal, miał jednak świadomość, że od 2 lipca 2018 r. powinna być to funkcja skrótu SHA-256, gdyż takiej użył przy składaniu podpisów na dokumentach dołączonych do oferty, które podpisał bez pośrednictwa portalu. Zamawiający przyjął, że w świetle wyroku Krajowej Izby Odwoławczej o sygn. akt KIO 2428/18, Zamawiający nie może uznać prawidłowości podpisu oferty, pomimo że nieprawidłowość była konsekwencją wadliwego działania portalu. Zamawiający odrzucił ofertę złożoną przez Odwołującego.

Odwołujący nie zgodził się z ww. decyzją Zamawiającego stwierdzając, że narusza ona dyspozycję przepisów prawa.

Odwołujący zwrócił uwagę, że przepisy prawa krajowego, w tym uzoie oraz ustawy

Pzp, nie normują definicji kwalifikowanego podpisu elektronicznego, definicji tego pojęcia należy zatem poszukiwać w regulacjach prawa wspólnotowego. Jak podał Odwołujący, zgodnie z rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (dalej: eIDAS lub rozporządzenie 910/2014) „kwalifikowany podpis elektroniczny" oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. Natomiast „kwalifikowany certyfikat podpisu elektronicznego" oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I".

Odwołujący stwierdził, że certyfikat jest to zaświadczenie elektroniczne (dokument elektroniczny) stanowiący zaświadczenie elektroniczne o określonym terminie ważności, które zawiera dane identyfikujące podpisującego oraz klucz publiczny, czyli dane służące do sprawdzenia autentyczności podpisu elektronicznego złożonego za pomocą klucza prywatnego, czyli danych, nad którymi wyłącznie podpisujący ma kontrolę.

Dalej Odwołujący wskazał, że dokument elektroniczny, który powstaje jako udokumentowanie czynności prawnej, jest podpisywany podpisem elektronicznym (analogicznie do dokumentu papierowego podpisanego piórem). Podczas podpisywania dokumentu (tworzenia podpisu) wyliczany jest skrót na podstawie treści tego dokumentu (SHA) - robi to aplikacja (system) podpisująca, niemająca najczęściej powiązania z wystawcą certyfikatu i samym tworzeniem certyfikatu.

Odwołujący wyjaśnił, że SHA (Secure Hash Algorithm) to rodzina powiązanych ze sobą kryptograficznych funkcji skrótu zaprojektowanych przez NSA [National Security Agency] i publikowanych przez National Institute of Standards and Technology.

Odwołujący podał, że w podpisie (w dużym uproszczeniu) są zawarte dwa skróty: jeden dotyczący treści dokumentu, drugi - treści certyfikatu (zawarty w pieczęci tego certyfikatu). Za ten pierwszy odpowiada aplikacja podpisująca (dostawca tej aplikacji), a za ten drugi wystawca certyfikatu.

Odwołujący zauważył, że żaden z przepisów obowiązującego prawa nie wskazuje, że kwalifikowane podpisy elektroniczne wykorzystujące algorytm skrótu SHA-1 winny być od dnia 1 lipca 2018 r. uznawane za nieważne. W przekonaniu Odwołującego, tego rodzaju

wniosków nie sposób przede wszystkim wywieść z art. 137 uzoie. Jak stwierdził Odwołujący, przepis ten nie wprowadził rygoru nieważności podpisu elektronicznego złożonego za pomocą funkcji skrótu SHA-1. Co więcej, nie można z niego wyinterpretować pozbawienia podpisu elektronicznego cech kwalifikowalności w przypadku nie skorzystania z nowszej funkcji SHA -2.

Odwołujący zwrócił uwagę, że potwierdzeniem zasadności przyjętych przez Odwołującego twierdzeń jest uzasadnienie do rządowego projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej (druk 715], gdzie wskazano, że: „Ważnym przepisem dla zapewnienia ciągłości usług zaufania w Polsce jest art. 134^2, wskazujący na możliwość stosowania skrótu SHA-1 do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych. Dotychczasowe przepisy wymagały wprost stosowania tego algorytmu, co spowodowało, że oprogramowanie stosowane do składania i weryfikacji podpisów, nie było dostosowywane do innych skrótów rekomendowanych w standardzie ETSI TS 119 312 dotyczącej wymagań w zakresie stosowania algorytmów kryptograficznych w infrastrukturze podpisu elektronicznego. Mając na uwadze, że norma ta wprost nie rekomenduje dalszego używania skrótu SHA-1 ze względu na możliwe naruszenia bezpieczeństwa, należało wprowadzić przepisy przejściowe umożliwiające stopniowe odejście od stosowania tego skrótu. Nie można było jednak wprost zrezygnować ze wskazywania algorytmu technicznego w przepisach prawa, opierając się jedynie na normach, ponieważ zgodnie z normą ETSI EN 319 412-2 dotyczącą profili certyfikatów wydawanych osobom fizycznym, stosowanie wymagań określonych w standardzie ETSI TS 119 312 może być zastąpione krajowymi zaleceniami. Brak stosownego przepisu skutkowałby wykazywaniem niezgodności z elDAS w raportach oceny zgodności, co mogłoby powodować negatywne postrzeganie krajowych dostawców usług zaufania i co za tym idzie znaczące zmniejszenie ich szans w konkurowaniu z dostawcami zagranicznymi na wspólnym rynku.”.

Jak zauważył Odwołujący, niezbędności użycia algorytmu skrótu SHA-256 dla kwalifikowanego podpisu elektronicznego nie dostrzega również Urząd Zamówień Publicznych - np. w opinii pn. „Czy podpis profilem zaufanym e-PUAP może być uznany za równoważny podpisowi kwalifikowanemu (w kontekście składania JEDZa po 18.04.2018 r.)” czy też publikacji „Podpis elektroniczny - regulacje i praktyka”.

Odwołujący zwrócił również uwagę na Komunikat Ministra Cyfryzacji z dnia 1 marca 2018 r. w sprawie wycofania algorytmu SHA-1 w zastosowaniach związanych

z zaawansowanym podpisem i pieczęcią elektroniczną, w którym zostało wyraźnie wskazane, że „Niezbędne jest jednak dostosowanie wszystkich systemów strony ufającej, tak aby z dniem 1 lipca br. było możliwe odejście od stosowania funkcji SHA-1 przy składaniu podpisu elektronicznego i pieczęci elektronicznej. Algorytm SHA-1 będzie mógł być nadal używany przy weryfikacji.”. Odwołujący zaznaczył, że ww. komunikat ma charakter zaleceń, a nie powszechnie obowiązującej reguły. Świadczy o tym także zakończenie komunikatu: „Odchodzenie od przestarzałych algorytmów i korzystanie z konserwacji za pomocą znaczników czasu pozwala minimalizować zagrożenia dla e-podpisu w przyszłości. Zarówno nadzór, jak i dostawcy usług zaufania śledzą i analizują wszystkie aspekty technologiczne, które mogą mieć wpływ na bezpieczeństwo usług zaufania. W interesie bezpieczeństwa i wygody odbiorców usług zaufania przypominamy, aby również inne podmioty dostosowały terminowo swoje systemy informatyczne.”.

Zdaniem Odwołującego, art. 137 uzoie należy intepretować w ten sposób, że ustawodawca zdecydował się narzucić administracji publicznej oraz dostawcom usług zaufania przejście na wyższy poziom bezpieczeństwa podpisu, ale powyższe nie oznacza, że którykolwiek obowiązujący przepis prawa pozwala kwestionować ważność podpisu z algorytmem SHA-1. Odwołujący podkreślił, że zaprzestanie stosowania funkcji SHA-1 przez administrację publiczną w Polsce nie oznacza, że nie wolno jej uznawać podpisów elektronicznych utworzonych przy zastosowaniu SHA-1 również po wejściu w życie art. 137. Jak zaznaczył Odwołujący, przeciwna interpretacja tego przepisu doprowadziłaby do konieczności nieuznawania statusu kwalifikowanych wszystkich podpisów wykorzystujących SHA-1, którymi opatrzone mogą być dokumenty przekazywane do polskich instytucji także z innych państw UE.

Odwołujący zwrócił uwagę, że w momencie walidacji kwalifikowanego podpisu elektronicznego nie ma możliwości ustalenia, na podstawie którego państwa przepisów powstał dany podpis. Podpis należy weryfikować zawsze na zgodność podpisu z wymaganiami Artykułu 32 rozporządzenia eIDAS i przepisami wykonawczymi obowiązującymi jednolicie w całej Unii Europejskiej. Tylko w ten sposób, w ocenie Odwołującego, można zapewnić interoperacyjność kwalifikowanego podpisu elektronicznego i szerzej wszystkich kwalifikowanych usług zaufania, co było celem i jest celem całego procesu legislacyjnego prowadzonego w UE w ostatnich latach.

Odwołujący wyjaśnił, że algorytm SHA-1 nie jest rekomendowany do stosowania przy tworzeniu podpisów zaawansowanych ze względu na możliwość w nieodległej perspektywie

czasowej skutecznego i niewykrywalnego dokonania manipulacji w treści dokumentu opatrzonego takim podpisem. Odwołujący dodał, że mimo sygnalizowanego ryzyka, nadal poziom bezpieczeństwa kryptograficznego jest na tyle wysoki, że przy obecnej wiedzy i możliwościach technicznych, gwarantuje bezpieczeństwo prawne i faktyczne podpisowi elektronicznemu, dlatego algorytm SHA-1 nie został wprost zakazany żadną decyzją lub innym unijnym prawnym aktem wykonawczym.

Odwołujący podkreślił, że algorytm skrótu SHA-1 jest nadal wykorzystywany tak w Polsce, jak i w Unii Europejskiej, o czym świadczy oświadczenie złożone przez smartpzp. Co więcej, wiele firm, w tym Google nadal jest w fazie wycofywania SHA-1 z wykorzystywanych podpisów i rozwiązań informatycznych (tj. po 1 lipca 2018 r.). Odwołujący podał, że pierwsze postulaty związane z potrzebą poszukiwania bezpieczniejszych rozwiązań kryptograficznych pojawiły się już w 2011 r. Od 2020 r. powszechnie stosowanym algorytmem skrótu ma być SHA-3, który - jak wynika z przeprowadzonych badań i testów - jest aktualnie najbezpieczniejszym rozwiązaniem szyfrującym.

Odwołujący wskazał, że nawet jeśli przyjąć odmienne zapatrywanie w przedmiotowej sprawie aniżeli przedstawione powyżej, to o niezasadności decyzji Zamawiającego świadczy fakt, że uzoie, która pośrednio reguluje kwestie związane z algorytmem SHA-1, jest aktem prawnym o randze krajowej. Odwołujący stwierdził, że aktualnie obowiązujące przepisy prawa wspólnotowego, które winny być respektowane na gruncie prawa polskiego jako akty nadrzędne względem krajowych ustaw, zawierają szereg regulacji zakazujących wprowadzania przez państwa członkowskie zapisów, które ustanawiają dodatkowe wymogi związane z posługiwaniem się i weryfikacją kwalifikowanych podpisów elektronicznych.

Jak wywodził Odwołujący, akty prawne wyznaczają wskazanym podmiotom (instytucjom, firmom, osobom) określone postępowanie. Akty prawne tworzą w państwie określoną strukturę hierarchiczną i z tego powodu moc prawna zawarta w jednym akcie może być wyższa niż w innym, może też być niższa lub równa. Powiązania, jakie z tego powodu występują między aktami prawnymi o różnej mocy, mają charakter kompetencyjny, np. akt wyższego rzędu może zawierać upoważnienie dla organu państwa lub innego podmiotu, aby wydał akt niższego rzędu, o niższej mocy prawnej. Akty niższego rzędu obowiązują na podstawie aktów zajmujących w tej hierarchii stanowisko nadrzędne. Akt wyższego rzędu ma więc wpływ na treść aktu niższego rzędu. Z kolei akt niższego rzędu nie może być sprzeczny z postanowieniami aktów nadrzędnych. Akty prawne równorzędne

mogą się wzajemnie uchylać, akt nadrzędny może uchylić akt o niższej mocy prawnej, natomiast akt o niższej mocy prawnej nie może uchylić postanowień zawartych w akcie nadrzędnym.

Odwołujący podał, że hierarchię polskich aktów prawnych reguluje Konstytucja Rzeczypospolitej Polskiej, według jej zapisów przedstawia się ona następująco:

1. Konstytucja,
2. Ratyfikowane umowy międzynarodowe, wymagające zgody wyrażonej w ustawie,
3. Rozporządzenia, decyzje i dyrektywy Unii Europejskiej,
4. Ustawy i rozporządzenia z mocą ustawy (dekrety),
5. Uchwały (akty wewnętrzne wiążące), rozporządzenia, zarządzenia,
6. Akty prawa miejscowego.

W świetle powyższego, jak zauważył Odwołujący, nie można uznać, że art. 137 uzoie ma moc nadrzędną względem art. 22 Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE:

„1. Państwa członkowskie zapewniają, że wszelka komunikacja i wymiana informacji odbywająca się na mocy mniejszej dyrektywy; w szczególności elektroniczne składanie ofert, przeprowadzane są z wykorzystaniem elektronicznych środków komunikacji zgodnie z wymogami niniejszego artykułu. Narzędzia i urządzenia wykorzystywane do celów komunikacji za pomocą środków elektronicznych, jak również ich właściwości techniczne, muszą być niedyskryminujące, ogólnie dostępne i interoperacyjne z produktami ICT będącymi w powszechnym użyciu oraz nie mogą ograniczać dostępu wykonawców do postępowania o udzielenie zamówienia,

(...)

6. Oprócz wymogów przedstawionych w załączniku IV następujące zasady mają zastosowanie do narzędzi i urządzeń służących do elektronicznego przesyłania i odbioru ofert oraz elektronicznego odbioru wniosków o dopuszczenie do udziału:

a) informacje na temat specyfikacji dotyczących elektronicznego składania ofert oraz wniosków o dopuszczenie do udziału, w tym kodowania oraz oznaczania czasu odbioru, są dostępne dla zainteresowanych stron;

b) państwa członkowskie, lub instytucje zamawiające działające zgodnie z ogólnymi ramami ustanowionymi przez dane państwo członkowskie, określają poziom bezpieczeństwa wymagany dla elektronicznych środków komunikacji stosowanych na poszczególnych etapach danego postępowania o udzielenie zamówienia; poziom ten jest proporcjonalny do powiązanego ryzyka;

c) w przypadku gdy państwa członkowskie, lub instytucje zamawiające działające zgodnie z ogólnymi ramami ustanowionymi przez dane państwo członkowskie, stwierdzą, że poziom ryzyka oceniony zgodnie z lit b) niniejszego ustępu sprawia, że wymagane są zaawansowane podpisy elektroniczne określone w dyrektywie Parlamentu Europejskiego i Rady 1999/93/WE, instytucje zamawiające akceptują zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie, uwzględniając czy te certyfikaty są wystawione przez podmiot świadczący usługi certyfikacyjne wymieniony na zaufanej liście przewidzianej w decyzji Komisji 2009/767/WE, składane za pomocą bezpiecznego urządzenia służącego do składania podpisów lub bez takiego urządzenia, o ile spełnione są następujące warunki:

b. instytucje zamawiające ustanawiają wymagany format zaawansowanego podpisu w oparciu o formaty ustanowione decyzją Komisji 2011/130/UE oraz wprowadzają niezbędne środki umożliwiające techniczne przetwarzanie tych formatów; w przypadku gdy stosowany jest inny format podpisu elektronicznego, taki podpis lub elektroniczny nośnik dokumentu muszą zawierać informację o istniejących metodach weryfikacji odpowiadają za to państwa członkowskie. Metody weryfikacji umożliwiają instytucji zamawiającej weryfikację - w trybie online. nieodpłatnie i w sposób zrozumiały dla osób niebędących rodzimymi użytkownikami danego języka - otrzymanego podpisu elektronicznego jako zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie.

b. Państwa członkowskie przekazują Komisji informacje na temat podmiotu świadczącego usługi weryfikacji a Komisja podaje informacje otrzymane od państw członkowskich do wiadomości publicznej w internecie;

a. jeżeli oferta jest podpisywana z wykorzystaniem kwalifikowanego certyfikatu, który jest umieszczony na zaufanej liście, instytucje zamawiające nie mogą stosować dodatkowych wymogów mogących utrudnić oferentom korzystanie z tych podpisów.

(....) Aby zapewnić interoperacyjność formatów technicznych, a także standardów dotyczących procesów i przesyłania komunikatów, zwłaszcza w kontekście transgranicznym, Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 87 w celu

ustanowienia obowiązku stosowania takich określonych standardów technicznych, w szczególności w zakresie stosowania elektronicznego składania ofert, katalogów elektronicznych i środków uwierzytelniania elektronicznego wyłącznie wtedy, gdy standardy techniczne zostały dokładnie przetestowane i została udowodniona ich przydatność w praktyce. Komisja, zanim nałoży obowiązek stosowania jakiegokolwiek standardu technicznego, także starannie przeanalizuje ewentualne koszty z tym związane, zwłaszcza pod kątem dostosowania do istniejących rozwiązań z zakresu elektronicznych zamówień publicznych, w tym koszty infrastruktury, procesów lub oprogramowania.”.

Odwołujący stwierdził, że analogiczne regulacje znajdują się w eIDAS. Przykładowo Odwołujący przywołał motyw 48, gdzie wskazano, że: „mimo, iż w celu zapewnienia wzajemnego uznawania podpisów elektronicznych konieczny jest wysoki poziom bezpieczeństwa, w niektórych przypadkach, akceptowane powinny być również podpisy elektroniczne o niższym poziomie bezpieczeństwa.”, motyw 50, zgodnie z którym „Ponieważ właściwe organy w państwach członkowskich używają obecnie różnych formatów zaawansowanych podpisów elektronicznych do elektronicznego podpisywania swoich dokumentów, państwa członkowskie powinny zapewnić możliwość obsługi pod względem technicznym co najmniej kilku formatów zaawansowanego podpisu elektronicznego przy odbiorze dokumentów podpisanych elektronicznie.:, jak też motyw 54, gdzie stwierdzono, że „Transgraniczna interoperacyjność i transgraniczne uznawanie kwalifikowanych certyfikatów stanowią warunek wstępny transgranicznego uznawania kwalifikowanych podpisów elektronicznych. Dlatego kwalifikowane certyfikaty nie powinny podlegać żadnym obowiązkowym wymogom przekraczającym wymogi określone w niniejszym rozporządzeniu, jednak na szczeblu krajowym należy dopuścić zawieranie w kwalifikowanych certyfikatach szczególnych atrybutów, takich jak unikalne identyfikatory, pod warunkiem że takie szczególne atrybuty nie utrudniają transgranicznej interoperacyjności i transgranicznego uznawania kwalifikowanych certyfikatów i podpisów elektronicznych.”. Odwołujący wskazał ponadto, że na podstawie art. 25 eIDAS „podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów kwalifikowanych podmiotów elektronicznych.”.

Odwołujący wskazał ponadto, że Komisja wydała w dniu 8 września 2015 r. decyzję wykonawczą do ww. ustawy ustanawiającą specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego, zgodnie z art.

27 ust. 5 i art. 37 ust. 5 elDAS. Zgodnie z brzmieniem ww. decyzji (vide: załącznik I):

„Wykaz specyfikacji technicznych w odniesieniu do zaawansowanych podpisów elektronicznych w formatach XML, CMS lub PDF oraz ASiC (Associated Signature Container)

Zaawansowane podpisy elektroniczne, o których mowa w art. 1 niniejszej decyzji, muszą być zgodne z jedną z następujących specyfikacji technicznych ETSl:

Podstawowy profil XAdES ETSl TS 103171 v.2.1.1

Podstawowy profil CAdES ETSl TS 103173 v.2.2.1

Podstawowy profil PAdES ETSl TS 103172 v.2.2.2

Format ASiC podpisu, o którym mowa w art 1 niniejszej decyzji, musi być zgodny z następującą specyfikacją techniczną ETSl:

Podstawowy profil ASiC ETSI TS 103174 v.2.2.1.

Odwołujący podkreślił, że ww. standardy dopuszczają zastosowanie algorytmu skrótu SHA-1.

Jak zauważył Odwołujący, ustawodawca jako podstawę wprowadzenia art. 137 uzoie upatruje zalecenie wynikające ze standardu ETSl TS 119 312, który nie został wyspecyfikowany w ww. decyzji. Odwołujący podkreślił, że nawet jeśli ETSl TS 119 312 zastąpił jeden z ww. standardów to brak jest w tym zakresie stosownych zmian prawnych w przywołanych powyżej aktach prawnych pozwalających na stwierdzenie, że zastosowanie algorytmu SHA-1 powoduje nieważność kwalifikowanego podpisu. Odwołujący zaznaczył, że sam standard ETSl TS 119 312 pełni funkcję rekomendacji i zaleceń, brak jest w nim wyraźnej dyspozycji odnośnie zaprzestania zastosowania SHA-1. Jak podkreślił Odwołujący, zgodnie z wytycznymi zawartymi w dokumencie „SHA-1 nie jest rekomendowany”, co nie oznacza niedopuszczalności jego wykorzystywania.

Odwołujący stwierdził, że jedynym dopuszczonym przez elDAS uzasadnieniem odrzucenia przez administrację publiczną dokumentu podpisanego ważnym kwalifikowanym podpisem elektronicznym może być powołanie się na ograniczenia techniczne, które nie pozwoliły urzędowi (zamawiającemu} dokonania prawidłowej analizy dokumentu ze względu na zastosowany w podpisie specyficzny, nieobsługiwany powszechnie algorytm

kryptograficzny. Odwołujący zaznaczył, że ww. okoliczność nie miała miejsca w stanie faktycznym przedmiotowej sprawy.

W świetle powyższego, zdaniem Odwołującego, nie sposób przyjąć, że art. 137 uzoie określający datę graniczną wykorzystywania algorytmu skrótu SHA-1 ma moc prawną nadrzędną względem regulacji prawa unijnego, które nakładają na Państwa Członkowskie obowiązek stanowienia prawa, które nie określa żadnych wymagań w tym zakresie, a dodatkowo zakazują stosowania środków, które utrudniałyby wykonawcom udział w postępowaniach o udzielenie zamówienia publicznego.

Odwołujący zwrócił uwagę, że na terenie Unii Europejskiej obowiązują jednolite przepisy dotyczące usług zaufania i uznawania kwalifikowanego podpisu elektronicznego. Jak wskazał Odwołujący, nie jest możliwym wprowadzanie do krajowego porządku prawnego regulacji, które powodowałyby, że ten sam podpis elektroniczny byłby uznawany za nieważny w Polsce, natomiast ustawodawstwa zagraniczne traktowałyby taki podpis jako skuteczny. Odwołujący zwrócił uwagę, że zgodnie z zasadą neutralności technologicznej, eIDAS nie wyklucza zastosowania dowolnego sposobu tworzenia podpisów zaawansowanych, pod warunkiem, że utworzony podpis elektroniczny spełnia wymogi art. 32 eIDAS.

W przekonaniu Odwołującego, uznać należy, że dyspozycja płynąca z art. 137 uzoie nie określa nieważności podpisów kwalifikowanych wykorzystujących algorytm SHA-1, ale stanowi zalecenie do odejścia przez adresatów tejże ustawy ze stosowania ww. algorytmu. Odwołujący argumentował, że uzoie w art. 137 narzuca obowiązek zaprzestania stosowania algorytmu SHA-1 przez administrację publiczną i dostawców usług zaufania (podkreślić należy, że adresatami ustawy nie są podmioty wykorzystujące kwalifikowane podpisy elektroniczne), co ma mitygować ryzyko ewentualnych manipulacji oraz ma spowodować przygotowanie krajowej infrastruktury wykorzystującej usługi zaufania do sytuacji, gdy przepisy nadrzędne wprowadzone przez unijnego prawodawcę zakażą wprost stosowania SHA-1 pod rygorem nieuznawania podpisu elektronicznego za podpis zaawansowany (szacowana data to styczeń 2020).

Odwołujący stwierdził, że konsekwencje za nieprzestrzeganie wymogów art. 137 uzoie mają inny charakter, aniżeli wywodzi to Zamawiający, gdyż skutki nieprzestrzegania przepisów nie obejmują odpowiedzialności podmiotów wykorzystujący podpis. Odpowiedzialność ponieść może np. dostawca kwalifikowanych usług zaufania, np. poprzez utratę kwalifikowanego statusu (wykreślenie przez nadzór z rejestru kwalifikowanych

dostawców) czy też osoba, która odpowiedzialna za dostosowanie do wymogów ustawy infrastruktury w danym urzędzie zaniedba swoich obowiązków (odpowiedzialność zawodowa lub służbowa).

Odwołujący wskazał, że przenoszenie na wykonawcę ciężarów związanych z wykorzystywaniem na potrzeby prowadzonych postępowań portalu komercyjnego wykorzystującego jedynie algorytm skrótu SHA-1 stanowi rażące naruszenie art 7 ust. 1 ustawy Pzp.

Jak stwierdził Odwołujący, w przypadku podjęcia przez Izbę decyzji o oddaleniu odwołania pojawia się pytanie czy Zamawiający (jak również inni zamawiający korzystający z portalu smartpzp) są zobowiązani unieważnić wszystkie postępowania wszczęte po 1 lipca 2018 r. a przed 20 grudnia 2018 r.? Co z postępowaniami, które zostały zakończone? Odwołujący wskazał, że zgodnie ze złożonym przez dostawcę systemu oświadczeniem, portal w ogóle nie wykorzystywał algorytmu SHA-256, a nie jedynie na potrzeby przedmiotowego postępowania.

Odwołujący przywołał także wyrok Trybunał Sprawiedliwości Unii Europejskiej z 13 lipca 2017 r. wydany w sprawie C-35/17 Saferoad Grawil sp. z o.o. and Saferoad Kabex sp. z.o.o. Generalna Dyrekcja Dróg Krajowych i Autostrad Oddział w Poznaniu, w którym Trybunał stwierdził, że „zasadę równego traktowania i obowiązek przejrzystości należy interpretować w ten sposób, iż stoją one na przeszkodzie wykluczeniu wykonawcy z przetargu publicznego wskutek niedopełnienia przez niego obowiązku, który nie wynika wyraźnie z dokumentacji przetargowej lub obowiązującej krajowej ustawy, lecz z wykładni tej ustawy i tej dokumentacji, a także z uzupełniania przez krajowe organy administracji lub sądownictwa administracyjnego występujących w tej dokumentacji luk (podobnie wyrok z dnia 2 czerwca 2016 r., Pizzo, C-27/15, EU:C:2016:404, pkt 51). W świetle powyższego odpowiedź na przedstawione pytania powinna brzmieć następująco: art. 2 dyrektywy 2004/18, zasadę równego traktowania i obowiązek przejrzystości należy interpretować w ten sposób, że stoją one na przeszkodzie wykluczeniu wykonawcy z postępowania o udzielenie zamówienia publicznego wskutek niespełnienia przez tego wykonawcę obowiązku, który nie wynika wyraźnie z dokumentacji przetargowej.”. Odwołujący przywołał też wyrok Krajowej Izby Odwoławczej z dnia 11 grudnia 2017 r., sygn. akt KIO 2479/17.

W świetle powyższego, Odwołujący wyraził przekonanie, że przedstawiona argumentacja, że wykonawca winien przewidzieć jakiego rodzaju algorytmu skrótu podpisu kwalifikowanego winien użyć na potrzeby złożenia oferty jest twierdzeniem niezasadnym

oraz prowadzi do zmiany zapisów SIWZ po terminie składania ofert.

Dodatkowo, Odwołujący zwrócił uwagę, że Zamawiający w Specyfikacji Istotnych Warunków w sposób szczegółowy opisał zasady złożenia oferty za pośrednictwem ww. portalu, w tym również zasady opatrywania dokumentów kwalifikowanym podpisem elektronicznym. Odwołujący przywołał pkt 7.3, 7.5, 7.4, 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3 SIWZ. Odwołujący zaznaczył, że wszystkie dokumenty złożone wraz z ofertą (kosztorysy ofertowe, JEDZ etc.) zostały opatrzone podpisem kwalifikowanym z algorytmem skrótu SHA-256. Niezrozumiałym jest dla Odwołującego przyjęcie, że Odwołujący nie sprostał wymaganiom, które zdaniem Zamawiającego, wynikają z art. 137 uzoie. Odwołujący stwierdził, że ww. dokumenty zostały załączone i są dostępne na portalu: https://portal.smartpzp,pl/mikolow/public/postepowanie?postepowanie=140144. Pliki mogą zostać pobrane na dysk komputera, a otwarcie pobranych plików za pomocą programu dedykowanego do opatrywania dokumentów kwalifikowanym podpisem elektronicznym i ich weryfikacji wykazuje, że wykorzystywany algorytm to SHA-256.

W ocenie Odwołującego, Zamawiający dokonał pobieżnej i niedokładnej oceny złożonych dokumentów, w tym weryfikacji kwalifikowanych podpisów elektronicznych, bazując jedynie na oświadczeniu dostawcy portalu, na którym było prowadzone postępowanie przetargowe. Wskazania wymaga, że z treści oświadczenia ww. dostawcy nie wynika, jakoby to Odwołujący wykorzystywał niewłaściwy podpis („portal wykorzystywał podpis z funkcjonalnością skrótu SHA-1"). Zdaniem Odwołującego, Zamawiający błędnie zinterpretował uzyskane oświadczenie, co skutkował przyjęciem, że oferta Odwołującego podlega odrzuceniu.

Odwołujący wyraził przekonanie, że w świetle przedstawionej przez Odwołującego argumentacji, nie powinno budzić żadnych wątpliwości, że odwołanie zasługuje w całości na uwzględnienie. Odwołujący zauważył, że Izba w orzeczeniu o sygn. akt KIO 2428/18 w sposób ogólny odniosła się do charakteru art. 137 uzoie z uwagi na okoliczność, że na kanwie ww. sprawy oferta wykonawcy, który posłużył się kwalifikowanym podpisem elektronicznym z algorytmem skrótu SHA-1, podlegała odrzuceniu z uwagi na inne okoliczności (niezgodność z SIWZ). Z uwagi na powyższe, Izba nie dokonała pogłębionej analizy przepisów w tym zakresie, przyjmując w całości zasadność zarzutów odwołania. Odwołujący zaznaczył również, że orzeczenie KIO wydane w konkretnej sprawie, nie stanowi źródła prawa w Polsce, zatem organy orzecznicze nie są zobowiązane niejako z automatu przyjmować zasadności stanowiska Izby wydanego w ww. sprawie.

Izba ustaliła, że podstawą odrzucenia oferty złożonej przez Odwołującego było stwierdzenie przez Zamawiającego w piśmie z dnia 18 stycznia 2019 r., że złożona przez Odwołującego oferta jest nieważna na podstawie odrębnych przepisów, a zatem podlega odrzuceniu na podstawie art. 89 ust. 1 pkt 8 ustawy Pzp. Zamawiający uzasadniając swoją decyzję wskazał, że zgodnie z art. 10a ust. 5 ustawy Pzp, ofertę sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym pod rygorem nieważności. Zamawiający podał, że składanie ofert odbywało się za pośrednictwem komercyjnego portalu smartpzp.pl. Zgodnie z instrukcją korzystania z tego portalu, złożenie oferty polegało na wypełnieniu formularza oferty zamieszczonego bezpośrednio na portalu i opatrzenie go kwalifikowanym podpisem elektronicznym. Zamawiający wskazał, że w postępowaniu jako treść oferty Zamawiający żądał złożenie również kosztorysu ofertowego, który należało opatrzyć kwalifikowanym podpisem elektronicznym i dołączyć do dokumentów składanych wraz z ofertą. Zamawiający stwierdził, że Odwołujący złożył ofertę zgodnie z instrukcją korzystania z portalu smartpzp.pl. Zamawiający wskazał także, że w trakcie badania i oceny oferty natrafił na trudności z weryfikacją kwalifikowanego podpisu elektronicznego złożonego za pośrednictwem aplikacji zaimplementowanej w funkcjonalności portalu smartpzp.pl, czego skutkiem było wystąpienie do podmiotu zarządzającego portalem o wyjaśnienie kwestii weryfikacji złożonego podpisu. Jednocześnie Zamawiający podał, że weryfikacja podpisów dokumentów i oświadczeń złożonych wraz z ofertą (JEDZ, kosztorysy ofertowe) wykazała ich prawidłowość.

Zamawiający wskazał również, że w dniu 18 stycznia 2018 r. przedstawiciel portalu smartpzp stwierdził, że „nie ma możliwości aby Wykonawca złożył ofertę w trybie przetargu nieograniczonego, bez potwierdzenia jej podpisem elektronicznym”, powołując się również na treść instrukcji składania oferty dla wykonawców. O prawidłowości złożonego podpisu miał świadczyć również raport z czynności złożenia oferty wygenerowany przez portal – plik 00006PN1E2018.pdf. Zamawiający poinformował, że bazując na tym oświadczeniu w dniu 9 stycznia 2019 r. dokonał czynności wyboru oferty Odwołującego.

Zamawiający poinformował ponadto, że w tym samym dniu Zamawiający powziął wiedzę o wyroku Krajowej Izby Odwoławczej z dnia 10 grudnia 2018 r., sygn. akt KIO 2428/18, w którym za wadliwy i skutkujący obowiązkiem odrzucenia oferty uznano kwalifikowany podpis elektroniczny złożony przy zastosowaniu algorytmu skrótu podpisu SHA-1. Z uwagi na powyższe, Zamawiający wystąpił ponownie do podmiotu zarządzającego portalem smartpzp o przekazanie oświadczenia, jakiego rodzaju algorytmu skrótu podpisu użyto przy składaniu podpisu kwalifikowanego dla oferty Odwołującego. W dniu 14 stycznia

2019 r. Prezes Zarządu podmiotu zarządzającego portalem (Portal PZP Sp. z o.o.) jednoznacznie oświadczyła, że na dzień składania ofert)6 grudnia 2018 r.) portal wykorzystywał podpis z funkcjonalnością skrótu SHA-1. Dodatkowo 16 stycznia 2019 r. podmiot zarządzający portalem poinformował, że dopiero od 20 grudnia 2018 r. portal wykorzystuje podpis z funkcjonalnością skrótu SHA-256.

Zamawiający podniósł, że kwestia prawidłowości wykorzystywanych skrótów podpisów elektronicznych została uregulowana w art. 137 uzoie. We wskazanym przepisie ustawodawca jednoznacznie wskazał, zdaniem Zamawiającego, że do składania zaawansowanych podpisów elektronicznych można stosować funkcję skrótu SHA-1 tylko do 1 lipca 2018 r. i w ust. 2 tego artykułu nałożył na producentów oprogramowania obowiązek dostosowania oferowanych przez nich produktów do wskazanego powyżej terminu i wymagań. Jak zauważył Odwołujący, podmiot zarządzający portalem smartpzp wypełnił ten obowiązek ustawowy dopiero 20 grudnia 2018 r., czego konsekwencją było złożenie podpisu elektronicznego w dniu 6 grudnia 2018 r. za pośrednictwem portalu z wykorzystaniem niedozwolonej funkcji skrótu SHA-1.

Zamawiający podkreślił, że Odwołujący składając podpis za pośrednictwem portalu nie miał wpływu na to, jakiej funkcji skrótu podpisu używa portal, miał jednak świadomość, że od 2 lipca 2018 r. powinna być to funkcja skrótu SHA-256, gdyż takiej użył przy składaniu podpisów na dokumentach dołączonych do oferty, które podpisał bez pośrednictwa portalu. Zamawiający stwierdził, że w świetle wyroku Izby o sygn. akt KIO 2428/18 nie może uznać prawidłowości podpisu oferty, pomimo że nieprawidłowość była konsekwencją wadliwego działania portalu i zobowiązany jest do odrzucenia oferty.

Krajowa Izba Odwoławcza, rozpoznając złożone odwołanie na rozprawie i uwzględniając zgromadzony materiał dowodowy wymieniony w treści uzasadnienia, jak również stanowiska stron postępowania zaprezentowane na piśmie i ustnie do protokołu posiedzenia i rozprawy, ustaliła i zważyła co następuje.

Izba stwierdziła, że odwołujący legitymuje się interesem we wniesieniu środka ochrony prawnej, o którym mowa w art. 179 ust. 1 ustawy Pzp. Zakres zarzutów, w sytuacji ich potwierdzenia się, wskazuje na pozbawienie Odwołującego możliwości uzyskania

zamówienia i jego realizacji, narażając go tym samym na poniesienie w tym zakresie wymiernej szkody.

Rozpoznając odwołanie w granicach podniesionych zarzutów Izba uznała, że podlega ono uwzględnieniu.

Izba stwierdziła, że żaden z przepisów prawa nie wskazuje, że kwalifikowane podpisy elektroniczne wykorzystujące algorytm skrótu SHA-1 powinny być od dnia 1 lipca 2018 r. uznawane za nieważne.

Sankcji nieważności na podpisy złożone po dniu 1 lipca 2018 r. z ich uwierzytelnieniem przy użyciu algorytmu SHA-1 nie nakłada art. 137 uzoie. Zgodnie z ust. 1 art. 137 uzoie, do dnia 1 lipca 2018 r. do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych można stosować funkcję skrótu SHA-1, chyba że wymagania techniczne wynikające z aktów wykonawczych wydanych na podstawie rozporządzenia 910/2014 wyłączą możliwość stosowania tej funkcji skrótu. Ust. 2 tego przepisu stanowi, że dostawcy usług zaufania, producenci oprogramowania oraz podmioty publiczne obowiązani są do odpowiedniego dostosowania oprogramowania oraz systemów teleinformatycznych do zmian i terminu określonych w ust 1. Izba zgodziła się ze stanowiskiem, że przepis ten należy interpretować jako dyspozycję skierowaną do dostawców usług zaufania, producentów oprogramowania oraz podmiotów publicznych zobowiązanych do odpowiedniego dostosowania oprogramowania oraz systemów teleinformatycznych do przejścia na wyższy poziom bezpieczeństwa podpisu. Z przepisu tego nie można jednak wywieść, że tego typu zobowiązanie skierowane do ww. podmiotów skutkuje odpowiedzialnością po stronie uczestników obrotu, wykorzystujących podpis z algorytmem SHA-1, w postaci nieważności podpisu. Izba miała również na uwadze dyspozycję art. 18 ust. 1 uzoie, który stanowi, że: „Podpis elektroniczny lub pieczęć elektroniczna weryfikowane za pomocą certyfikatu wywołują skutki prawne, jeżeli zostały złożone w okresie ważności tego certyfikatu”. Co za tym idzie, nie można odmówić podpisowi elektronicznemu statusu kwalifikowanego podpisu elektronicznego, ani jego ważności, w sytuacji, gdy taki podpis został złożony w okresie ważności certyfikatu.

Wprowadzenie rygoru nieważności podpisu w polskim prawie powodowałoby powstanie sprzeczności z Rozporządzeniem 910/2014, które nie przewiduje negatywnych skutków dla kwalifikowanych podpisów elektronicznych wytworzonych z wykorzystaniem funkcji skrótu SHA-1. Podobnie, dyrektywa 2014/24/UE art. 22 ust. 6 lit. c) pkt (ii) wskazuje, że jeżeli oferta jest podpisywana z wykorzystaniem kwalifikowanego certyfikatu, który jest

umieszczony na zaufanej liście, instytucje zamawiające nie mogą stosować dodatkowych wymogów mogących utrudniać oferentom korzystanie z tych podpisów. Z przepisów przywołanych aktów wspólnotowych należy wywieść, że nie można odmówić ważności kwalifikowanemu podpisowi elektronicznemu złożonemu z zastosowaniem skrótu SHA-1, skoro spełnia on przesłanki Rozporządzenia 910/2014, a stwierdzenie nieważności takiego podpisu stanowiłoby nieuprawnione tworzenie wymogów utrudniające składanie ofert w formie elektronicznej.

W przedmiotowej sprawie za istotną Izba uznała również okoliczność, że Odwołujący składając ofertę działał zarówno w zgodzie z postanowieniami Specyfikacji Istotnych Warunków Zamówienia, jak również zgodnie z instrukcją korzystania z portalu smartpzp.pl. Wszystkie dokumenty załączone do oferty zostały opatrzone przez Odwołującego kwalifikowanym podpisem elektronicznym wykorzystującym algorytm skrótu SHA-256, co stanowiło okoliczność bezsporną. Jedynie formularz oferty zamieszczony bezpośrednio na portalu, za pośrednictwem którego odbywało się składanie ofert, został opatrzony podpisem wykorzystującym algorytm skrótu SHA-1. Przyczyną tego było nie działanie wykonawcy, a funkcjonowanie portalu, który nie umożliwiał wykorzystania podpisu z funkcjonalnością SHA-256. Jednocześnie, złożone pod dokumentami i oświadczeniami podpisy zostały zweryfikowane pozytywnie, co stwierdził Zamawiający w piśmie z dnia 18 stycznia 2019 r. Powyższe potwierdził także przedstawiciel portalu smartpzp stwierdzając w piśmie z dnia 18 grudnia 2018 r., że nie ma możliwości, aby wykonawca złożył ofertę w trybie przetargu nieograniczonego bez potwierdzenia jej podpisem elektronicznym.

Mając powyższe na uwadze, Izba zgodziła się z Odwołującym, że uznanie przez Zamawiającego za nieprawidłowy podpisu użytego przy podpisywaniu oferty, stanowiło czynność nieuprawnioną, bowiem dokument ten został opatrzony ważnym podpisem kwalifikowanym, zgodnie z wymogami prawa. W konsekwencji, potwierdzenie znalazł także zarzut niezasadnego unieważnienia przez Zamawiającego postępowania z uwagi na przyjęcie, że w postępowaniu nie złożono żadnej oferty niepodlegającej odrzuceniu. Tym samym, potwierdziły się zarzuty naruszenia przez Zamawiającego przepisów wskazanych w odwołaniu.

Z uwagi na powyższe, na podstawie art. 192 ust. 1 i 2 ustawy Pzp, orzeczono jak w sentencji.

O kosztach postępowania orzeczono na podstawie art. 192 ust. 9 i 10 ustawy Pzp oraz § 5 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 15 marca 2010 r. w sprawie wysokości wpisu od odwołania oraz rodzajów kosztów w postępowaniu odwoławczym i sposobu ich rozliczania (Dz. U. Nr 41, poz. 238 ze zm.).

Przewodniczący : **……**

……

……