Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 18.08.2017 r.
KIGEiT/1018/08/2017

Sz. P. Marcin Cichy
Prezes Urzędu Komunikacji Elektronicznej
ul. Kasprzaka 18/20
01-211 Warszawa

Działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***"), w związku z ogłoszeniem o społecznych konsultacjach dokumentacji konkursowej (dalej „***Dokumentacja***") na wybór podmiotu, który zapewni system pomiarowy do celów certyfikowanego mechanizmu monitorowania usług dostępu do Internetu, Izba przedstawia stanowisko w ww. sprawie.

I. KWALIFIKACJA DZIAŁALNOŚCI PROWADZONEJ PRZEZ PODMIOT ZAPEWNIAJĄCY MECHANIZM MONITOROWANIA JAKOŚCI USŁUGI DOSTĘPU DO INTERNETU

(1.) Na samym wstępie należy zauważyć, że Dokumentacja nie porusza w ogóle wątku wymagań dotyczących wpisu podmiotu zapewniającego mechanizm do rejestru przedsiębiorców telekomunikacyjnych. Tymczasem nie budzi wątpliwości, że **świadczone przez taki podmiot usługi kwalifikują się jako usługi telekomunikacyjne** w rozumieniu art. 2 pkt 48 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tj. Dz. U. z 2016 r., poz. 1489, dalej „***PT***").

(2.) Oczywistym jest bowiem, że na potrzeby testu podmiot dostarczający mechanizm będzie przekazywał sygnały w sieci telekomunikacyjnej. Należy również zaznaczyć, że monitorowanie jakości usług jest niewątpliwie działalnością gospodarczą, tzn. jest prowadzone w celu zarobkowym. O ile sami odbiorcy usługi (czyli abonenci/użytkownicy oraz dostawcy usług) nie ponoszą z tytułu korzystania żadnych opłat na rzecz tego podmiotu, to zapewnienie mechanizmu będzie oznaczało możliwość uzyskania przychodów np. z tytułu reklam.

(3.) Uwzględnienie powyższej kwestii jest o tyle istotne, że **prowadzenie działalności telekomunikacyjnej wiąże się z szeregiem obowiązków wynikających z PT** (obowiązki te zostaną omówione w dalszej części stanowiska) **oraz pozwala na kontrolę takiej działalności przez Prezesa UKE**.
Zgodnie z art. 199 ust. 1 PT „*Prezes UKE jest uprawniony do kontroli przestrzegania przepisów, decyzji oraz postanowień z zakresu telekomunikacji, gospodarki częstotliwościami lub spełniania wymagań dotyczących kompatybilności elektromagnetycznej*".

(4.) Brak wpisu podmiotu zapewniającego mechanizm monitorowania mógłby oznaczać brak możliwości kontroli, z uwagi na to, że poszczególne obowiązki wynikające z PT są adresowane do przedsiębiorców telekomunikacyjnych. Z uwagi na znaczenie wyników pomiarów dla rynku telekomunikacyjnego, zapewnienie możliwości takiej kontroli jest absolutnie kluczowe.

II. KONSTRUKCJA KONKURSU

(5.) Izba zwraca również uwagę, że **idea konkursu budzi zastrzeżenia w zakresie roli Prezesa UKE w monitorowaniu jakości usług**.

(6.) Sam **konkurs skonstruowany jest w ten sposób, że prowadzi on do wyłonienia podmiotu odpowiedzialnego za monitorowanie jakości usług na podstawie wyłącznie zapewnień**.

(7.) Tymczasem dostarczane narzędzie będzie miało istotny wpływ na prowadzenie działalności przez dostawców usług dostępu do Internetu z uwagi na roszczenia za nienależytą jakość usług.

(8.) Niedopuszczalna jest sytuacja, w której rola Prezesa UKE ograniczona jest do wyboru takiego podmiotu na podstawie deklaracji, przy czym pojawiają się również wątpliwości co do etapu certyfikowania dostarczanego narzędzia (o czym szerzej w dalszej części stanowiska).

(9.) W pkt 6.3.2. Dokumentacji przewidziano, że *„Jeżeli w wyniku realizacji porozumienia zostanie przygotowany system pomiarowy, którego wymogi zostały określone w załączniku nr 2 do dokumentacji, Prezes UKE certyfikuje mechanizm monitorowania usługi dostępu do Internetu na okres 12 miesięcy*".
Oznacza to, że możliwe jest wyłonienie w konkursie podmiotu, który zapewni narzędzie niespełniające wymagań Prezesa UKE, przy czym narzędzie takie nie zostanie certyfikowane. Pytaniem otwartym pozostaje w jaki sposób zostanie zbadane, czy narzędzie to spełnia te wymagania oraz czemu może służyć narzędzie niespełniające takich wymagań?

(10.) W kontekście weryfikacji spełnienia wymogów Izba zwraca również uwagę, że Dokumentacja powinna szczegółowo określać sposób weryfikacji, przy czym powinna być ona dokonana przez Prezesa UKE, a nie *„zewnętrznego eksperta*", o którym mowa w pkt 3.24 Załącznika nr 2 do Dokumentacji.

(11.) Niezależnie od powyższego Izba ponownie zwraca uwagę, na **konieczność wskazania wymogu wpisu do rejestru przedsiębiorców telekomunikacyjnych celem zapewnienia Prezesowi UKE możliwości ciągłej weryfikacji mechanizmu monitorowania, m.in. poprzez kompetencje organu w ramach postępowania kontrolnego**.

III. WERYFIKACJA OFERTY

(12.) Niezależnie od uwag dotyczących wadliwości konstrukcji konkursu, polegającej na tym, że wybór dokonywany jest wyłącznie w oparciu o zapewnienia składane w ofercie, Izba wskazuje na **konieczność uzupełnienia postanowień porozumienia zawieranego z podmiotem wyłonionym o kary umowne na wypadek niespełnienia deklarowanych funkcjonalności**.

(13.) Jednocześnie sama **procedura testów, zastrzeżona dla *„zewnętrznego eksperta"*, powinna umożliwiać wzięcie udziału w testach dostawców usług dostępu do Internetu, którzy jako jedyni mogą dokonać porównania wyników otrzymywanych przez testowany mechanizm monitorowania z innymi mechanizmami, w tym takimi, które są stosowane przez samych dostawców**.

(14.) Ocena punktowa ofert w trakcie konkursu przewiduje otrzymanie jednakowej liczby punktów za każdą część oceny natomiast Izba proponuje wprowadzenie oceny ważonej dla bardziej precyzyjnej oceny oferty.

IV. PRZETWARZANIE DANYCH

(15.) Izba wskazuje, że w związku z zapewnieniem mechanizmu monitorowania jakości usług, **podmiot dostarczający to narzędzie będzie dysponował i przetwarzał cały szereg danych, z którymi obowiązujące przepisy wiążą szereg obowiązków**.

(16.) Warto w tym zakresie wspomnieć o danych osobowych i reżimie ustawy o ochronie danych osobowych (a od maja 2018 r. Rozporządzenia Ogólnego o Ochronie Danych), oraz przetwarzaniu danych teletransmisyjnych (por. obowiązki wynikające z art. 165 PT), adresów IP należących do dostawców usług oraz danych lokalizacyjnych, w szczególności w przypadku dostawców usług mobilnych (por. obowiązki wynikające z art. 166 PT).

(17.) W ocenie Izby Dokumentacja oraz treść porozumienia powinny zapewniać spełnienie przez dostawcę narzędzia wszelkich obowiązków wynikających z obowiązujących przepisów prawa w zakresie przetwarzania ww. kategorii danych.

V. DANE WRAŻLIWE

(18.) Niezależnie od uwag przedstawionych w pkt IV powyżej Izba wskazuje na ryzyka związane z dostępem podmiotu wyłonionego w konkursie do danych wrażliwych, mogących stanowić tajemnicę różnych przedsiębiorstw. Do tego rodzaju danych należy bowiem zaliczyć dane o przepływnościach zapewnianych przez poszczególnych dostawców usług, czy też o stosowanych przez użytkowników systemach operacyjnych. W szczególności nie sprecyzowano obowiązków wyłonionego podmiotu co do postępowania z wrażliwymi danymi w przypadku zakończenia i nieprzedłużenia 12 miesięcznego okresu certyfikowania lub odebrania certyfikacji.

(19.) W przypadku pierwszej wskazanej kategorii informacji posiadane dane pozwolą oszacować np. jaki odsetek abonentów danego dostawcy korzysta z danej przepływności. Do kategorii informacji stanowiących tajemnicę przedsiębiorstwa należy zaliczyć również adresację IP oraz dane abonentów konkretnego dostawcy usług. Również wynikający z kierowanych przez abonentów zapytań poziom świadczonych usług czy też sama liczba zapytań są danymi wrażliwymi, które mogą zostać wykorzystane przez konkurentów danego dostawcy usług.

(20.) Takie informacje, w przypadku udostępnienia ich konkurencji, pozwoliły np. na stworzeniu dedykowanej, konkurencyjnej oferty detalicznej (np. na podobnym poziomie cenowym przy lepszych parametrach jakościowych).

(21.) Z tego względu, niezależnie od konieczności nałożenia na podmiot wyłoniony szczególnych obowiązków związanych z potrzebą zapewnienia ochrony takich danych (pod rygorem zapłaty wysokich kar umownych) Prezes UKE powinien przewidzieć w Dokumentacji, że w związku z zapewnieniem mechanizmu monitorowania (czy to w formie aplikacji czy z poziomu strony internetowej) **podmiot wyłoniony nie może reklamować w jakiejkolwiek formie usług telekomunikacyjnych, w szczególności zaś związanych z usługą dostępu do Internetu** (co jest obecnie nagminne, np. w przypadku speedtest.pl).

VI. WYMOGI DOTYCZĄCE MECHANIZMU MONITOROWANIA

a. System operacyjny

(22.) W pkt 3.1 Załącznika nr 2 do Dokumentacji wskazano, że „*Aplikacja powinna działać pod kontrolą systemów operacyjnych dla komputerów stacjonarnych (typu desktop/laptop), posiadających co najmniej 10% udział w rynku konsumenckim w Polsce*". W ocenie Izby **brak jest rzetelnych danych pozwalających na weryfikację tego wymogu**. Jedyne dostępne dane pochodzą z ciągów identyfikacyjnych przeglądarek internetowych, jednak nie są one w pełni wiarygodne. Nie uwzględniają one również podziału na rynek konsumencki i niekonsumencki.

(23.) Wymóg ten budzi również wątpliwości w zakresie tego, jak należy rozumieć system operacyjny. Wydaje się bowiem, że np. system Windows XP jest innym systemem operacyjnym niż Windows 10. Przy takim rozumieniu tego pojęcia, według danych za 2017 roku są tylko dwa systemy operacyjne, które posiadają udział większy niż 10%.

b. Czynniki wpływające na wynik

(24.) Pkt 3.11 Załącznika nr 2 do Dokumentacji przewiduje katalog czynników, które mogą być uwzględniane w badaniu jakości. W katalogu tym wymienia się:

- datę i godzinę pomiaru z dokładnością do 1 sekundy,
- adres IP przydzielony przez operatora sieci,
- nazwę operatora sieci,

- wykorzystany interfejs sieciowy komputera użytkownika (WiFi, Ethernet itp.),
- kartę sieciową i prędkość połączenia sieciowego komputera użytkownika,
- parametry radiowe w przypadku wykorzystania interfejsu radiowego,
- obciążenie interfejsu sieciowego, procesora i pamięci operacyjnej komputera użytkownika,
- podstawowe dane o komputerze (CPU/RAM, obciążenie CPU),
- rodzaj i wersja systemu operacyjnego zainstalowanego na komputerze użytkownika,
- równoczesny ruch w tle (cross-traffic).

(25.) **Za zupełnie niezrozumiałe należy uznać dopuszczenie możliwości (a nie konieczności), by mechanizm monitorowania nie zapewniał ww. funkcjonalności**.

(26.) Dopuszczenie narzędzia, które nie uwzględnia np. równoczesnego ruchu w tle oznacza z samego założenia, że otrzymany wynik będzie niemiarodajny, a może być on podstawą do dochodzenia przez abonenta roszczeń z tytułu nienależytej jakości usługi. Brakuje również mechanizmów identyfikowania, czy pomiar jest dokonywany przy użytkowaniu jednego komputera czy w trakcie pomiaru w usługi korzysta jednocześnie więcej urządzeń istotnie zaburzających pomiar.

(27.) Tym samym **Izba postuluje, by wszystkie wymienione funkcjonalności były wymagane dla dopuszczenia danej oferty do etapu II konkursu**. Jakikolwiek bowiem brak oznaczać będzie bowiem stworzenie narzędzia, które nie będzie przydatne w kontekście realizacji przewidzianych celów.

c. Weryfikacja adresu IP

(28.) Izba dostrzega również potrzebę zapewnienia przez podmiot wyłoniony możliwości **weryfikacji adresu IP pod kątem przypisania do konkretnego dostawcy usług**. Chodzi tu o zapewnienie uniknięcia sytuacji, w której pomiar będzie dokonywany przy pomocy innego łącza niż to, które jest przedmiotem umowy pomiędzy danym abonentem a dostawcą.

d. Dostarczenie wyników pomiaru do dostawcy usług

(29.) W ocenie Izby **podmiot wyłoniony powinien być również zobligowany do przesyłania online wyników pomiaru do danego dostawcy usług tak, aby zapewnić mu możliwość weryfikacji pomiaru**.

(30.) Zwracamy uwagę na ryzyko sytuacji, w której dany abonent dokona pomiaru, który wykaże nienależytą jakość usługi a następnie skieruje roszczenia z tym związane np. po upływie 11 miesięcy od daty pomiaru. W takiej sytuacji **dostawca usług nie będzie miał żadnej możliwości weryfikacji rzetelności takiego pomiaru, a co za tym idzie - zasadności kierowanych roszczeń (innymi słowy nie będzie miał żadnych możliwości obalenia domniemania związanego z wynikami pomiaru)**.

e. Wymogi dotyczące serwerów

(31.) Załącznik nr 2 do Dokumentacji przewiduje wymóg (pkt 3.20 i 3.21), by serwery testowe zlokalizowane były w min. dwóch największych punktach wymiany ruchu internetowego i były podłączone interfejsami o przepływności min. 1 Gb/s w każdym kierunku. Izba zwraca uwagę, że wymagania te są zdecydowanie zbyt niskie w kontekście potencjalnej, wielomilionowej grupy abonentów usług stacjonarnego dostępu do Internetu.

(32.) **Izba postuluje konieczność zapewnienia min. 100 serwerów o większej przepływności**.

(33.) Istotne jest również to, aby podmiot wyłoniony zapewnił backup dla każdego z serwerów (min. dwa serwery podłączone niezależnymi drogami) oraz SLA na poziomie 100% pod rygorem zapłaty wysokich kar umownych za każdą rozpoczęta godzinę braku dostępności serwera.
Bez takiego zastrzeżenia mechanizm będzie miał charakter iluzoryczny.

f. Wymogi pod kątem bezpieczeństwa

(34.) Zarówno **aplikacja, jak i oprogramowanie wykorzystywane do pomiaru z poziomu strony internetowej powinny być zweryfikowane pod kątem bezpieczeństwa**. Weryfikacja powinna być prowadzona okresowo w postaci zewnętrznego audytu przez firmy niezależne.

(35.) Należy wziąć pod uwagę ryzyko wykorzystania zaufania do systemu (system certyfikowany) do przeprowadzania ataków phishingowych, dystrybucji złośliwego oprogramowania, fałszowania pomiarów czy innego rodzaju cyberataków. W związku z powyższym:

- system powinien spełniać wymagania bezpieczeństwa (zdefiniowane w zapytaniu oraz potwierdzone zewnętrznym, niezależnym audytem podczas odbioru). Wymagania bezpieczeństwa powinny obejmować również zapewnienie braku możliwości podszycia się pod system lub jego elementy zarówno po stronie klienckiej jak i serwerowej,
- system powinien być monitorowany w zakresie bezpieczeństwa w okresie eksploatacji, w tym poddawany okresowym audytom bezpieczeństwa. Dostawca powinien zapewnić brak podatności systemu na ww. ryzyka, ich usunięcie w zdefiniowanym czasie (w przypadku ewentualnego wykrycia błędów bezpieczeństwa lub zidentyfikowania incydentów) pod rygorem kar finansowych.

(36.) Jak wspomniano powyżej, podmiot wyłoniony będzie miał dostęp do szeregu kategorii danych wrażliwych, co samo w sobie powinno oznaczać obowiązek zapewnienia należytej ich ochrony. Nie można również lekceważyć ryzyka cyberataków. Trzeba przecież pamiętać, że przy proponowanym rozwiązaniu jedna aplikacja może stać się „furtką" do zasobów informatycznych milionów abonentów.

(37.) Oznacza to, że **zapewnienie bezpieczeństwa powinno mieć istotne znaczenie przy ocenie wyboru podmiotu certyfikowanego**.

g. Wymogi dotyczące warunków transmisji

(38.) Zapewnienie wysycenia pojemności łącza w trakcie dokonywania pomiaru jest w opinii Izby warunkiem bezzasadnym ze względu na konieczność zapewnienia świadczenia prędkości maksymalnej usług, co koliduje z wcześniejszymi wytycznymi UKE co do świadczenia usług dostępu do Internetu.

VII. PODSTAWA PRAWNA CERTYFIKACJI

(39.) **Wątpliwości KIGEiT budzi również forma, w jakiej miałaby zostać dokonana ewentualna certyfikacja mechanizmu** (z zastrzeżeniem uwag, zgodnie z którymi sam mechanizm, bez certyfikacji, nie będzie spełniał swojej funkcji).
Dziwi fakt, że certyfikacja nie będzie miała formy decyzji administracyjnej.

(40.) W ocenie Izby takie stanowisko oznacza, że Prezes UKE, w obowiązującym stanie prawnym, nie posiada w ogóle kompetencji do certyfikacji.

(41.) Należy bowiem wskazać, że zgodnie z art. 7 Konstytucji RP *„Organy władzy publicznej działają na podstawie i w granicach prawa"*. Oznacza to, że Prezes UKE **może działać wyłącznie w określonych formach prawnych**. Nie można przy tym zapominać, że zgodnie z art. 206 ust. 1 Pt, postępowanie przed Prezesem UKE toczy się na podstawie przepisów kpa.

(42.) **Każda z prawnych form działania musi być wyznaczona przepisami obowiązującego prawa. Innymi słowy, przepisy prawa muszą przewidywać daną formę, niezależnie od tego, czy jest to decyzja czy czynność natury materialno-technicznej.**

(43.) Powracając do wątku stosowania kpa do postępowania przed Prezesem UKE należy wskazać, że zgodnie art. 1 kpa: *„Kodeks postępowania administracyjnego normuje postępowanie: 1) przed organami administracji publicznej w należących do właściwości tych organów sprawach indywidualnych rozstrzyganych w drodze decyzji administracyjnych"*. Innymi słowy, w każdej sprawie, **w której organ administracji publicznej dokonuje władczej konkretyzacji uprawnień lub obowiązków jednostki, rozstrzygnięcie następuje w drodze decyzji administracyjnej**. W ocenie Izby kryteria przewidziane w art. 1 kpa w kontekście certyfikacji narzędzia są spełnione. Skoro Prezes UKE wychodzi z założenia, że nie ma podstaw do wydania decyzji, to musi tym samym przyjmować, że dopuszczalne jest certyfikowanie narzędzia w formie materialno-technicznej. Tymczasem w odpowiednich przepisach prawa brak jest przepisu uprawniającego Prezesa UKE do dokonania zatwierdzenia w takiej właśnie formie. Przyjęciu formy czynności materialno-technicznej sprzeciwia się również art. 4 Dyrektywy Ramowej. Gdyby bowiem uznać, że certyfikacja mechanizmu monitorowania następuje w formie czynności materialno-technicznej, to naruszona zostałaby zasada przyznająca m.in. przedsiębiorcom telekomunikacyjnym prawo odwołania się od środka regulacyjnego, który takiego przedsiębiorcy dotyczy. Nie ulega wątpliwości, że z uwagi na konsekwencje certyfikowania mechanizmu monitorowania, środek taki dotyczy przedsiębiorcy telekomunikacyjnego, gdyż jego funkcjonowanie będzie miało istotne znaczenie dla oceny ewentualnych roszczeń kierowanych do takiego przedsiębiorcy przez abonentów.

(44.) Ponadto w sposób oczywisty certyfikacja daje podmiotowi, który zapewnia certyfikowany mechanizm oraz dostawcom usług określone prawa i obowiązki.

(45.) Również w doktrynie wskazuje się (prof. S. Piątek), że:

„Rozstrzygnięcie organu regulacyjnego przyznające certyfikat na wniosek podmiotu zainteresowanego eksploatowaniem takiego mechanizmu ma wszelkie cechy decyzji administracyjnej w rozumieniu KPA. Zgodnie z art. 1 pkt 1 KPA, Kodeks normuje postępowanie przed organami administracji publicznej w należących do właściwości tych organów sprawach indywidualnych rozstrzyganych w drodze decyzji administracyjnych. Prezes UKE jest centralnym organem administracji państwowej, rozporządzenie przyznaje mu kompetencję do podejmowania rozstrzygnięć w sprawie certyfikacji mechanizmów monitorowania jakości usług dostępu do internetu, a rozstrzygnięcie w sprawie certyfikacji dotyczy sprawy indywidualnej związanej z ustanowieniem mechanizmu monitorowania jakości usługi".

(46.) Konkludując, **certyfikowanie narzędzia musi nastąpić w formie decyzji administracyjnej**.

(47.) Wskazujemy również, że **tylko taka forma rozstrzygnięcia pozwoli na dokonanie ewentualnych zmian rozstrzygnięcia, stwierdzenie jej wygaśnięcia czy też nieważności, w sytuacji wystąpienia poszczególnych przesłanek wskazanych w k.p.a.**

VIII. METODA POMIARU

(48.) Załącznik nr 2 do Dokumentacji odsyła w kontekście metody pomiaru do dokumentu IETF RFC 6349. Izba pragnie zwrócić uwagę na szereg wątpliwości związanych z adekwatnością tej metody do celów mechanizmu monitorowania.

(49.) W samym dokumencie wskazuje się m.in., że **metoda ta nie jest przewidziana dla celów porównywania usług różnych dostawców**.

(50.) Niezależnie od tego Izba pragnie zwrócić uwagę, że również w świetle Rozporządzenia certyfikowany mechanizm monitorowania ma służyć wyłącznie weryfikacji jakości usługi, a nie jej porównaniu z usługami zapewnianymi przez innych dostawców. Izba zwraca również uwagę na fakt deklaracji odmiennych wartości prędkości minimalnej, zwykle dostępnej i maksymalnej przez różnych dostawców usług, co uniemożliwia porównywanie wyników pomiarów.

(51.) W powołanym dokumencie wskazuje się również na kwestie związane z bezpieczeństwem danych, co koresponduje z uwagami przedstawionymi przez Izbę w pkt 6 lit. f powyżej.

(52.) W tym samym dokumencie wskazuje się również, że **w celu uzyskania rzetelnego pomiaru wskazana jest współpraca pomiędzy odbiorcą usługi, a jej dostawcą**.

Potwierdza to prezentowane wcześniej stanowisko Izby, zgodnie z którym rozwiązaniem najpełniej realizującym cele Rozporządzenia byłoby zapewnienie mechanizmów monitorowania przez dostawców usług.

(53.) Dokument wskazuje również na **szereg czynników, które mogą zaburzać wynik pomiaru**.
Wskazuje się tu m.in. na to, że wszystkie systemy operacyjne posiadają globalny mechanizm ograniczania pamięci systemowej używanej dla połączeń TCP. Systemy operacyjne przewidują również różne ograniczenia w zakresie buforów dla przesyłania danych.

Wreszcie, powołany przez Prezesa UKE dokument zastrzega, że przewidziany jest on raczej dla usług biznesowych, o wyższych parametrach.

(54.) Powyższe zastrzeżenia budzą wątpliwości co do tego, czy pomiary dokonywane przy wykorzystaniu tej metody będą rzetelne, co w kontekście roszczeń powstających na ich podstawie jest kwestią niezwykle istotną. Rolą Prezesa UKE powinno być bowiem również wzięcie pod uwagę interesów dostawców usług.

IX. POZOSTAŁE UWAGI

(55.) Izba zastrzega sobie możliwość zgłoszenia dalszych uwag po przedstawieniu finalnej wersji Dokumentacji. Jednocześnie zwracamy uwagę, że możliwość kierowania pytań o wyjaśnienie treści Dokumentacji została zastrzeżona wyłącznie dla podmiotów zainteresowanych przedstawieniem oferty (por. pkt 2.5.1. Dokumentacji).

(56.) Z uwagi na to, że konkurs dotyczy kwestii mających niewątpliwy wpływ na dostawców usług Prezes UKE powinien zapewnić również możliwość przedstawienia pytań przez tych dostawców oraz zrzeszające ich izby gospodarcze.

Z poważaniem

Prezes Zarządu

Stefan Kamiński