



HUAWEI POLSKA sp. z o.o.
ul. Domaniewska 39A,
02-672 Warszawa, Poland
Tel.: + 48 22 355 18 00,
Fax: + 48 22 355 18 86
www.huawei.com
E-mail: poland@huawei.com

Warszawa, 12 maja 2023 r.

dr Jacek Oko

Prezes Urzędu Komunikacji Elektronicznej

**STANOWISKO W DRUGIM POSTĘPOWANIU KONSULTACYJNYM DOTYCZĄCYM
PROJEKTÓW DOKUMENTACJI AUKCYJNEJ NA CZTERY REZERWACJE
CZĘSTOTLIWOŚCI Z PASMA 3,6 GHz**

Szanowny Panie Prezesie,

działając w imieniu Huawei Polska sp. z o.o. („Huawei”) na wstępie chcielibyśmy podziękować za możliwość wyrażenia stanowiska Spółki w ramach drugiej rundy konsultacji dotyczących dokumentacji aukcyjnej. Szanujemy i doceniamy wysiłek Pana Prezesa, mający na celu jak najszybsze i bezpieczne udostępnienie częstotliwości na potrzeby sieci 5G w Polsce. Wierzymy, że ponowione konsultacje są szansą na wypracowanie lepszej, bardziej sprawiedliwej i transparentnej procedury selekcyjnej. Niestety zmiany zaproponowane w obecnej wersji wymagań w zakresie bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług nie odpowiadają zgłaszanym przez rynek uwagom i sugestiom, zwiększając niepewność prawną całego procesu.

W ocenie Huawei kluczowe jest, aby aukcja odbyła się w oparciu o obowiązujące przepisy prawa, a w szczególności nakładane obowiązki i ograniczenia wynikały z przepisów rangi ustawowej. Niestety mechanizmy proponowane w ramach projektów decyzji rezerwacyjnych stwarzają bardzo poważne ryzyko dla stabilności prawnej rozstrzygnięć w postępowaniu aukcyjnym, co naszym zdaniem utrudni lub opóźni budowę infrastruktury 5G w Polsce. Taka konstatacja wynika z następujących przyczyn:

- a. w obowiązujących przepisach rangi ustawowej nie ma podstaw do nałożenia obowiązków i ograniczeń przewidzianych w punkcie 11 Załącznika nr 4 do projektów decyzji w sprawie rezerwacji częstotliwości pt. „Wymagania dotyczące bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług”;
- b. do Załącznika nr 4 wprowadzono klauzulę sprzeczną z przepisami prawa;
- c. proponowane rozwiązania nie uwzględniają wejścia w życie Dyrektywy NIS¹

¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

Brak podstaw prawnych w obowiązujących przepisach prawa dla stosowania Procedury dostawcy stanowiącego zagrożenie

W punkcie 11 załącznika nr 4 do projektów decyzji rezerwacyjnych sformułowano procedurę wyznaczania „dostawcy stanowiącego poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi” („Procedura dostawcy stanowiącego zagrożenie”). Analiza przepisów Prawa telekomunikacyjnego² oraz ustawy o krajowym systemie cyberbezpieczeństwa³ nie prowadzi do wniosku, aby Prezes Urzędu Komunikacji Elektronicznej („Prezes UKE”) posiadał kompetencje do ustanowienia procedury prowadzącej do uznania dostawcy za dostawcę stanowiącego takie zagrożenie⁴. Oznacza to, że postanowienia te nie mają oparcia w obowiązujących przepisach prawa, co stwierdzono nawet w uzasadnieniu do projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa: *obecnie nie ma żadnych środków prawnych umożliwiających nakazanie wycofywania z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce, a przez to funkcjonowaniu państwa. W szczególności dotyczy to kluczowych przedsiębiorców telekomunikacyjnych, którzy będą świadczyć usługi w oparciu o mobilne sieci 5G (zgodnie z aktualnym uzasadnieniem projektu nowelizacji uksc⁵).*

Zauważyć także należy, że jakiegokolwiek decyzje lub orzeczenia organów innych państw, także państw członkowskich Unii Europejskiej w tym zakresie, nie mogą skutkować uznaniem dostawcy za dostawcę stanowiącego takie zagrożenie na gruncie prawa polskiego. W obecnym stanie prawnym nie ma także podstaw, aby decyzję o wykluczeniu dostawcy mógł podjąć jakikolwiek inny organ. Procedura wycofania sprzętu, prowadzona z udziałem Prezesa UKE, ze wskazaniem konkretnych czynności i terminów ich realizacji przez operatora, także nie znajduje umocowania w obowiązujących przepisach prawa.

Postanowienia punktu 11 naruszają sformułowaną w art. 22 Konstytucji RP zasadę wolności gospodarczej. Zgodnie bowiem z tym przepisem Konstytucji, ograniczenie wolności działalności gospodarczej jest dopuszczalne tylko w drodze ustawy i tylko ze względu na ważny interes publiczny. Dlatego nie ma podstaw prawnych ograniczania swobody działalności gospodarczej w oparciu o dokument, który nie jest ustawą i nie ma swojego umocowania w ustawie. Proponowane rozwiązania mogą prowadzić do naruszenia konstytucyjnej zasady zaufania do państwa i prawa (art. 2, art. 7 Konstytucji). Co więcej, nakładanie tych ograniczeń wykracza poza zakres uprawnienia Prezesa UKE do określenia wymagań dotyczących bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług (por. art. 115 ust. 1 pkt 10 Prawa telekomunikacyjnego).

W obecnej sytuacji prawnej wydanie decyzji rezerwacyjnych zawierających postanowienia niemające podstawy prawnej (punkt 11 załącznika nr 4), a także wykraczające poza kompetencje Prezesa UKE powoduje, że decyzje nie będą wykonalne w przedmiotowym zakresie. Przyjęta konstrukcja punktu 11 załącznika nr 4 umożliwia dowolną zmianę wymagań w okresie rezerwacji częstotliwości, skutkując naruszeniem zasady trwałości decyzji

² Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2022 r. poz. 1648).

³ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2022 r. poz. 1863).

⁴ Por. art. 175b i 175e Prawa telekomunikacyjnego.

⁵ [Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, nr w wykazie prac legislacyjnych i programowych rady ministrów: UD68](#)

administracyjnych⁶. Opisane wady stwarzają wysokie prawdopodobieństwo uchylecia decyzji rezerwacyjnych.

Niedozwolona klauzula

W Załączniku Nr 4 sformułowana została następująca klauzula: *Poszczególne postanowienia Wymagań mają zastosowanie, o ile obowiązujące przepisy prawa nie stanowią inaczej. Postanowienia Wymagań należy tak interpretować aby je pogodzić z obowiązującymi przepisami. W przypadkach niedających się pogodzić kolizji z obowiązującymi przepisami, przepisy prawa powszechnie obowiązującego mają pierwszeństwo i wchodzi w miejsce postanowień niniejszego Załącznika, z którymi są one niezgodne. W związku z treścią tego zastrzeżenia należy stwierdzić, że organ administracyjny nie może wydać decyzji określającej wymagania w sposób odmienny aniżeli przewidują to przepisy prawa powszechnie obowiązującego. Decyzja administracyjna musi być zgodna z aktualnym porządkiem prawnym i rozstrzygać sytuację prawną jej adresata w sposób jednoznaczny. Klauzula ta może zostać uznana za sprzeczną nie tylko z zasadą praworządności, ale także z zasadą zaufania do państwa i prawa.*

Niespójność z Dyrektywą NIS2

W dniu 16 stycznia 2023 r. (już po ogłoszeniu pierwszej rundy konsultacji) weszła w życie Dyrektywa NIS2, która w sposób systemowy adresuje kwestie cyberbezpieczeństwa, także w odniesieniu do rynku telekomunikacyjnego. Polska zobligowana jest do transpozycji tej dyrektywy nie później niż do 17 października 2024 r. Powstaje zatem uzasadniona wątpliwość, czy i w jakim zakresie Procedura dostawcy stanowiącego zagrożenie jest zgodna z nową dyrektywą. Pytanie to w szczególności dotyczy zgodności Procedury dostawcy stanowiącego zagrożenie ze środkami dopuszczalnymi na podstawie Dyrektywy NIS2, w celu skoordynowanego szacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw. Środki te powinny być odpowiednie i proporcjonalne. Dopóki środki przewidziane w Dyrektywie NIS2 nie zostaną transponowane do obowiązujących w Polsce przepisów ustawowych i na ich podstawie nie zostanie uregulowana Procedura dostawcy stanowiącego zagrożenie, brak jest podstaw prawnych wprowadzenia do decyzji rezerwacyjnych postanowień punktu 11. W przeciwnym razie stanowić to będzie naruszenie wspomnianych już konstytucyjnych zasad praworządności i swobody prowadzenia działalności gospodarczej.

Proponowane rozwiązanie

Mając na uwadze powyższe, wnosimy o:

- **usunięcie w całości punktu 11 z załącznika nr 4 do projektów decyzji w sprawie rezerwacji częstotliwości oraz**

- **przywołanej wcześniej klauzuli,**

ewentualnie o:

zastąpienie treści punktu 11 i klauzuli poniższą propozycją, w celu oparcia działań Prezesa UKE na podstawie i w granicach obowiązującego prawa:

⁶ Por. art. 16 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j. Dz. U. z 2023 r. poz. 775).

11. W celu eliminacji ryzyk określonych w pkt 3 Dysponent zobowiązuje się do realizacji obowiązków w zakresie bezpieczeństwa i integralności sieci i usług telekomunikacyjnych zawartych w ustawie.

Huawei od ponad 20 lat wnosi istotny wkład w rozwój polskiej branży telekomunikacyjnej, wdrażając wspólnie z operatorami kolejne generacje łączności bezprzewodowej (od GSM/UMTS do 5G), w celu zapewnienia nieprzerwanej i bezpiecznej komunikacji. Produkty Huawei spełniają najwyższe standardy bezpieczeństwa udokumentowane międzynarodowymi certyfikatami. Wbrew nieuzasadnionym i nieobiektywnym opiniom pojawiającym się w przestrzeni publicznej, do działalności Huawei w Polsce nigdy nie było zarzutów, w szczególności w odniesieniu do bezpieczeństwa przetwarzania danych.

Będąc odpowiedzialnym dostawcą i liderem rynku, konsekwentnie podnosimy, że środki zarządzania ryzykiem w cyberbezpieczeństwie powinny być stosowane do konkretnych usług, produktów i oprogramowania, proporcjonalne i poprzedzone rzetelną analizą rzeczywistych podatności tego sprzętu i oprogramowania, a nie powinny się opierać na pozamerytorycznych cechach samego dostawcy. Nie kwestionujemy potrzeby stawiania wysokich wymagań bezpieczeństwa dostawcom rozwiązań. Wyrażamy jednak nadzieję, że wszelkie środki w zakresie cyberbezpieczeństwa będą wdrażane w sposób proporcjonalny do zidentyfikowanych ryzyk, a przede wszystkim zgodnie z obowiązującymi przepisami prawa.



Z wyrazami szacunku

Zhang Jie
Dyrektor Zarządzający
HUAWEI POLSKA sp. z o.o.