

Warszawa, 31 stycznia 2023 r.

ZDG/DAiL/0039/01.23/JP

**Pan
Jacek Oko
Prezes Urzędu Komunikacji
Elektronicznej**

Szanowny Panie Prezesie,

w związku z prowadzonymi konsultacjami publicznymi dokumentacji aukcyjnej na cztery rezerwacje częstotliwości z pasma 3,6 GHz, Pracodawcy RP proszą o przyjęcie poniższych uwag. Wyrażamy jednocześnie zadowolenie z uruchomienia procedury aukcyjnej, która – jak mamy nadzieję – zostanie skutecznie zakończona stabilnymi rozstrzygnięciami.

I. Brak podstawy dla Procedury DWR w obecnie obowiązujących przepisach prawa

Pracodawcy RP podnoszą, że w obowiązującym stanie prawnym nie znajdują się jakiegokolwiek podstawy dla obecnie proponowanego brzmienia pkt 11 Załącznika nr 3 do projektów decyzji w sprawie rezerwacji częstotliwości pn. „Wymagania dotyczące bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług” („Procedura DWR”). Treść tego punktu wywołuje niepewność co do obecnego i przyszłego stanu prawnego. W pierwszej kolejności niejasne jest, czy Procedura DWR miałaby stanowić samoistną procedurę, w której to Prezes UKE byłoby organem uprawnionym do wydania decyzji, czy zapis ten ma referować do kompetencji innego organu.

Zgodnie z Procedurą DWR Prezes UKE przekazuje¹ dysponentowi rezerwacji częstotliwości informację o uznaniu dostawcy za dostawcę wysokiego ryzyka. Analiza przepisów Prawa telekomunikacyjnego², czy ustawy o krajowym systemie

¹ Analogicznie, konstrukcja przekazania stosowana jest w Prawie telekomunikacyjnym, gdy mowa o transferze pewnych informacji lub rozstrzygnięć (por. odpowiednio art. 9 ust. 4, art. 19 ust. 2b, art. 175a ust. 1a, art. 175b ust. 3, art. 179, art. 190 ust. 2c, art. 192a ust. 2 Prawa telekomunikacyjnego).

² Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.

cyberbezpieczeństwa³, nie prowadzi do wniosku, aby Prezes UKE posiadał kompetencje do uznania dostawcy za dostawcę wysokiego ryzyka⁴. Brak także przepisów powszechnie obowiązujących, z których wynika uprawnienie Prezesa UKE do przekazywania takich informacji tj. o uznaniu danego dostawcy za dostawcę wysokiego ryzyka dysponentowi rezerwacji częstotliwości, co uruchamiałoby Procedurę DWR. Jakiegokolwiek decyzje lub orzeczenia organów innych państw, w tym państw członkowskich Unii Europejskiej, w tym zakresie nie mogą skutkować uznaniem dostawcy za dostawcę wysokiego ryzyka na gruncie prawa polskiego. W obecnym stanie prawnym nie ma także podstaw, aby decyzję o wykluczeniu dostawcy mógł podjąć jakiegokolwiek inny organ. Opisana w dalszej części punktu 11 załącznika nr 3 procedura wycofania sprzętu, prowadzona z udziałem Prezesa UKE, ze wskazaniem konkretnych czynności i terminów ich realizacji przez operatora także nie znajduje żadnego umocowania w obowiązujących przepisach prawa. Taka samoistna procedura oparta jedynie o rozstrzygnięcie decyzji rezerwacyjnej pozbawiona byłaby ram kluczowych dla możliwości uznawania jej za posiadającą znamiona legalności. W szczególności rodziłaby poważne wątpliwości co do swojej zgodności z art. 22 Konstytucji RP wyrażającym zasadę wolności gospodarczej, która podlega ograniczeniu jedynie w drodze ustawy i tylko ze względu na ważny interes publiczny. W konsekwencji treść punktu 11 ograniczałaby swobodę wolności gospodarczej na podstawie aktu pozaustawowego.

Próbując natomiast odnosić tę Procedurę DWR do projektowanej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa podkreślamy, że Procedura DWR nie tylko w sposób nieuprawniony odnosi się do stanu prawnego, który nie istnieje i niekoniecznie będzie istniał, ale nawet próbuje go zmieniać (program wycofania, uzgodnienia terminu wycofania). Co do samego skutku ewentualnego uznania jakiegokolwiek podmiotu za DWR zupełnie niezrozumiałe jest odwołanie się do takiej hipotetycznej sytuacji w projekcie decyzji rezerwacyjnej. Należy bowiem przyjąć, że jeśli taka decyzja zostanie wydana na gruncie polskich przepisów prawa powszechnie obowiązującego, będzie wówczas obejmować wszystkie określone w niej istniejące już zasoby i szczególne odwołanie w decyzji rezerwacyjnej nie jest konieczne, ani nawet słuszne.

W konsekwencji projektowany pkt 11 wydaje się wykraczać poza dyspozycję Prezesa UKE do określenia wymagań dotyczących bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług, o których mowa w art. 115 ust. 1 pkt 10 Prawa telekomunikacyjnego.

³ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

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

II. Proponowane rozwiązanie

Pracodawcy RP apelują o usunięcie Procedury DWR (pkt 11 z załącznika nr 3 do projektów decyzji w sprawie rezerwacji częstotliwości).

Jedynym słusznym w naszej ocenie kierunkiem jest przyjęcie, że decyzje uznające jakiegokolwiek dostawcę za dostawcę wysokiego ryzyka będą mogły być podejmowane na podstawie obowiązujących przepisów – kiedy takie zostaną wprowadzone. Ich skutki zaś będą się rozciągać w zakresie wynikającym z tychże przepisów oraz w wydawanej na ich podstawie decyzji administracyjnej. Nie istnieją przy tym istotne przesłanki, które uniemożliwiłyby objęcie zakresem takiej decyzji zasobów, które tworzą sieć wykorzystującą zasoby częstotliwości, dla których decyzja rezerwacyjna nie wskazywała na taką ewentualność.

Odwoływanie się do tej nieistniejącej jeszcze procedury, jak również nadawanie projektowi decyzji rezerwacyjnej mocy prawotwórczej w zakresie kompetencji Prezesa UKE Pracodawcy RP uważają za działanie przede wszystkim niepotrzebne, a także potencjalnie rodzące skutki odwrotne od zamierzonych.

Należy podkreślić, że organy administracji publicznej w kontekście wymagań bezpieczeństwa i samej Procedury DWR w obowiązującym stanie prawnym mogą sięgnąć po mechanizmy umożliwiające wykluczenie dostawców z budowy i rozbudowy sieci 5G w Polsce. Są one zawarte w rozporządzeniu 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim⁵. Na podstawie tych bezpośrednio stosowanych przepisów możliwe jest zamrożenie zasobów dostawcy, co jest równoznaczne z wykluczeniem z rynku.

Z poważaniem



⁵ Rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim.