Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 02.11.2021 r.
KIGEiT/1970/11/2021

Szanowny Pan Janusz Cieszyński
Sekretarz Stanu,
Pełnomocnik ds. Cyberbezpieczeństwa
Kancelaria Prezesa Rady Ministrów

Szanowny Panie Ministrze,

projekt „ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw" z dn. 12 października 2021 r., przedstawiony w ramach uzgodnień na szczeblu Kancelarii Prezesa Rady Ministrów, **w wielu miejscach różni się od poddanej konsultacjom publicznym** wersji projektu opatrzonej datą 7 września 2020 roku. Prowadzone obecnie konsultacje robocze projektu nie powinny zastąpić rzetelnych, przewidzianych prawem ponownych konsultacji publicznych projektu ustawy. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***") sprzeciwia się takiemu trybowi prac nad projektem Ustawy oraz pragnie wyrazić w poniższym stanowisku opinię w stosunku do wersji projektu opatrzonej datą 12 października 2021

Tytułem wstępu Izba pragnie podkreślić, że proponowane zmiany przepisów dotyczące powstania strategicznej sieci bezpieczeństwa oraz jej operatora wyposażonego w szerokie uprawnienia stanowią poważne zagrożenie dla konkurencyjności rynku, powodują jego uszczuplenie o ok. 1 mld zł i będą miały negatywny wpływ na inwestycje w rozwój nowoczesnych sieci telekomunikacyjnych, a tym samym rozwój gospodarczy całego kraju. Żadne państwo nie może sobie pozwolić na ograniczenie planów rozwoju kluczowej obecnie branży zapewniającej udział społeczeństwa w wykonywaniu podstawowych czynności, jak praca czy nauka zdalna. Należy mieć na uwadze, że przeregulowany rynek telekomunikacyjny, szczególnie gdy regulacja ta niesie za sobą gigantyczne koszty funkcjonowania przedsiębiorców, nie będzie w stanie podjąć wyzwań inwestycyjnych przed nim stawianych.

Proces konsultacji

Zgłoszone w trakcie konsultacji publicznych trwających od dnia 8 września do 6 października 2020 r. uwagi, w dużej mierze zostały odrzucone, natomiast obecny projekt nowelizacji został bardzo zmieniony, uzupełniony o dużą liczbę nowych przepisów oraz podzielony pomiędzy dwa projekty ustaw. **W ocenie KIGEiT konsultacje projektu nie zostały przeprowadzone w sposób rzetelny i należy je powtórzyć.** Dodatkowo, Izba podkreśla, że w odpowiedzi na złożone rok temu uwagi dotyczące np. procedury oceny ryzyka dostawcy udzielone zostały te same odpowiedzi (ponad sto razy) z pominięciem odniesienia się do merytorycznej treści każdej z nich. Fakt dołączenia do projektu, już po zakończeniu procedury konsultacji publicznych, całego Działu III, a także rozdziału 11a dotyczącego krajowego systemu certyfikacji, które nie były w żaden sposób poddane konsultacjom z podmiotami zainteresowanymi kształtem proponowanych przepisów, pozwala uznać, że projekt został gruntownie zmieniony i wymaga ponownych konsultacji.

Wzrost kosztów działalności telekomunikacyjnej

Wejście w życie proponowanych przepisów nowelizacji Ustawy o KSC wraz z jednocześnie procedowanym projektem ustawy „Prawo Komunikacji Elektronicznej" oraz ustawy „Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej", spowodują drastyczny wzrost kosztów prowadzenia podstawowej działalności telekomunikacyjnej (wzrost maksymalnych stawek opłat za numerację, wykorzystanie częstotliwości czy opłaty telekomunikacyjnej w projekcie PKE) oraz wymuszą nieuzasadniony wzrost nakładów na zwiększenie bezpieczeństwa sieci i usług komunikacji elektronicznej, co doprowadzi do dużego spadku rentowności przedsiębiorstw telekomunikacyjnych. Przy jednoczesnym spadku przychodów spowodowanym szeregiem działań, wśród których należy wymienić: znaczną obniżkę stawek za zakończenie połączenia w sieciach telekomunikacyjnych (stacjonarnych i ruchomych), praktyczne wyeliminowanie z rynku sektora public oraz wzroście innych kosztów wynikających z podwyżki cen prądu, – może to doprowadzić do fali bankructw. Dodatkowo, duży wzrost kosztów świadczenia usług m.in. wynikający z proponowanej podwyżki opłat za pozwolenia radiowe może pozbawić wiele firm i instytucji dostępu do usług transmisji danych albo dobrego backupu z wykorzystaniem technologii radiowych, co będzie miało negatywny wpływ na bezpieczeństwo użytkowanych przez nie sieci i usług.

Projektowane przepisy zakładają wzrost kosztów m.in. związanych z certyfikacją produktów i usług ICT (rozdział 11a), obejmujących zarówno koszty samych audytów certyfikacyjnych, jak i utrzymanie niezbędnej dokumentacji i wymogów (np. audyty wewnętrzne, analizy ryzyka) oraz koszty dostosowania stosowanych rozwiązań do tych wymogów.

Regulacje wynikające z projektu nowelizacji UKSC oraz PKE i ustawy wprowadzającej PKE (w szczególności dodawany do UKSC rozdział 4a) zmierzają w kierunku objęcia normą ISO27001 wszystkich przedsiębiorców komunikacji elektronicznej, a w szczególności wszelkich usług dostarczanych klientowi i wszelkich zmian w sieci, która do tego służy. Wynika to głównie z obowiązku szacowania ryzyka. Dla każdego przedsiębiorcy komunikacji elektronicznej oznacza to co najmniej kilka dodatkowych etatów niezbędnych do realizacji samej tylko pracy dokumentacyjnej i specjalistycznej. W odniesieniu do przedsiębiorców zobowiązanych do posiadania planu działań w sytuacjach szczególnych zagrożeń zostaje dołożony kolejny obowiązek związany z faktem, że plan musi zawierać zarządzanie cyberzagrożeniami – co generuje kolejne formalności i koszty związane z zapewnieniem ich obsługi.

Wyeliminowanie małych i średnich podmiotów

Podwyżka opłat za częstotliwości i pozwolenia radiowe, za udostępnienie numeracji oraz opłaty telekomunikacyjnej jest szczególnie dotkliwa dla małych i średnich przedsiębiorców, co w efekcie oznacza, że będą oni zmuszeni ograniczyć lub zakończyć działalność ze względu na brak płynności finansowej, wynikającej z nadmiernych kosztów działalności. To z kolei będzie powodowało przyspieszenie koncentracji rynku (ich miejsce zajmą duże grupy albo operatorzy o największym udziale w rynku) i ryzyko powrotu do monopolu/oligopolu stanie się realne. Bez wątpienia efektem końcowym takiego procesu będzie podwyżka cen zarówno hurtowych, jak i detalicznych oraz ograniczenie albo zaniechanie inwestycji w sieć i nowe rozwiązania techniczne, czyli regres na polskim rynku telekomunikacyjnym. Należy również pamiętać, że wysokie opłaty stanowią barierę wejścia na rynek, co ponownie odbije się negatywnie na jego konkurencyjności.

Proponowana zmiana przepisów w zakresie Prawa Komunikacji Elektronicznej oraz Ustawy o Krajowym Systemie Cyberbezpieczeństwa, będzie uderzać zarówno w konkurencyjność rynku, jak i będzie miała negatywny wpływ na realizację celów, które w tej chwili są priorytetem, tj. cyfryzacja, rozwój e-usług, powszechny dostęp do sieci szerokopasmowych.

Bezpośredni wpływ na rynek telekomunikacyjny w Polsce

Utrata obecnych klientów z segmentu *public,* przeznaczonych do obsługi z wykorzystaniem SSB oznacza, że wartość rynku spada o ok. 1 mld złotych i może prowadzić do wyeliminowania z rynku wielu podmiotów świadczących usługi dla klientów z tego segmentu. Wielokrotnie w ciągu ostatnich lat rynek telekomunikacyjny doświadczał prób zastosowania nadmiernych regulacji, czego wynikiem było znaczne spowolnienie i ograniczenie inwestycji. Mniejsza konkurencja na rynku, to też uboższa oferta, zapaść innowacyjna, brak postępu, gorsza jakość usług i obsługi.

Ubiegłe lata pokazują, że stymulacja inwestycji w szybkie i nowoczesne sieci jest możliwa jedynie przy odpowiednim rozłożeniu kosztów danin publicznych oraz zmniejszenia obciążeń regulacyjnych czego przykładem są porozumienia zawierane przez Prezesa UKE w latach 2009 -2011.

Zakładany w projekcie model funkcjonowania OSSB, oparty na finasowaniu przez konkurentów, doprowadzi do tego, że żadne inwestycje w rozwój infrastruktury nie będą realizowane. Trudno spodziewać się, aby OSSB był zainteresowany rozbudową własnej sieci telekomunikacyjnej. Z kolei przedsiębiorcy telekomunikacyjni, zmuszeni do udostępniania infrastruktury w zamian za zwrot kosztów, również mogą nie dostrzec szansy na rozwój takiego biznesu. Należy pamiętać, że przedsiębiorcy telekomunikacyjni, aby podjąć decyzję o realizacji nowych inwestycji, muszą dostrzegać szansę na uzyskanie satysfakcjonującej marży. W przypadku współpracy z OSSB i udostępniania sieci po kosztach, marża nie będzie realizowana.

Oczekiwania wobec przedsiębiorców

Rynek telekomunikacyjny i występujące na nim podmioty są często wykorzystywane do realizacji szczytnych celów, takich jak: zapewnienie szerokopasmowego dostępu do internetu na obszarach nierentownych (nieatrakcyjnych inwestycyjnie), zapewnienie podwyższonych standardów jakości i prędkości transmisji danych, standardów obsługi klienta, czasu reakcji na awarie, obniżki cen, uproszczenia usług, wprowadzenie dodatkowych kanałów komunikacji z klientem itd. Nieustanne dokładanie obowiązków, zwiększanie kosztów oraz uszczuplanie przychodów ma kolosalny wpływ na kondycję przedsiębiorców telekomunikacyjnych i realizacja nowych obowiązków wymaga zapewnienia odpowiedniego poziomu przychodów. Sektor telekomunikacyjny w dobie pandemii przyczynił się do niezakłóconej realizacji codziennych obowiązków zarówno zwykłych obywateli, przedsiębiorców, ale też całego sektora publicznego, w tym organów władzy w państwie. Dlatego niezrozumiały dla rynku komunikacji elektronicznej jest kierunek zmian funkcjonowania proponowany zarówno w projekcie UKSC, PKE i ustawy wprowadzającej PKE. Wzrost kosztów przy jednoczesnej redukcji przychodów i finansowaniu niekonkurencyjnego tworu w postaci OSSB, może oznaczać wyłącznie regres branży. A to wszystko przed jednym z najbardziej oczekiwanych i ważnych etapów rozwoju sieci – aukcji 5G, który pociągnie za sobą gigantyczne zobowiązania finansowe i inwestycyjne operatorów sieci ruchomej oraz stanowi nie mniejsze wyzwanie dla operatorów sieci stacjonarnych, aby zapewnić odpowiednio dostosowane, nowoczesne, szybkie i niezwodne sieci światłowodowe.

Utrata budżetowych wpływów z opłat

Utrata ogromnych kwot, jakie potencjalnie mogłyby zasilić budżet Państwa z wpływów z opłat za rezerwacje częstotliwości, a przeznaczone zostaną nieodpłatnie dla spółki Polskie 5G, będzie jednym z pierwszych dotkliwych skutków wejścia w życie proponowanych przepisów. Zasoby te mogłyby być z powodzeniem rozdystrybuowane wśród podmiotów komercyjnych, zamierzających świadczyć usługi w technologii 5G, w zamian za opłaty rezerwacyjne, które według szacunków dotyczących analogicznych zasobów mogłyby przynieść budżetowi Państwa ok. 3,5 mld zł. Nie ma również żadnej pewności, że podmioty te w związku

z ograniczeniami nałożonymi na podstawie art. 76p wezmą udział w przetargu, który ma legitymizować proces dystrybucji częstotliwości oraz zapewnić udział w spółce Polskie 5G.

Należy również wspomnieć o spodziewanym uszczupleniu wpływów z podatków, związanym z okrojeniem rynku *public*.

Konflikt geopolityczny

Wykluczenie dostawcy pochodzącego z państwa spoza UE i NATO może doprowadzić nie tylko do naruszenia umów międzynarodowych, lecz również do wykluczenia producentów sprzętu bardziej zaawansowanych technicznie i korzystających z nowocześniejszych rozwiązań, które coraz częściej powstają w Azji.

Sytuacja geopolityczna uległa zmianie od chwili powstania propozycji tych przepisów i wydaje się, że rozwiązania stosowane przez dostawców z państw określanych jako zaufane mogą w niedługim czasie okazać się niewystarczająco nowoczesne oraz drogie i podatne na np. kryzys na rynku półprzewodników i związane z tym ograniczenia w przepływie surowców. To z kolei będzie mieć negatywne skutki dla zabezpieczenia łańcuchów dostaw i możliwości wytwarzania nowych urządzeń.

Bezpieczeństwo Państwa

W myśl proponowanych przepisów, Operator Strategicznej Sieci Bezpieczeństwa staje się dostawcą usług dla większości podmiotów administracji rządowej i samorządowej. Rezygnacja z nałożenia na przedsiębiorców telekomunikacyjnych obowiązków w zakresie bezpieczeństwa państwa wydaje się zatem logiczną konsekwencją przyjęcia zapisów predestynujących OSSB do realizacji zadań dotyczących obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji. Ograniczenie obciążeń nałożonych w Dziale VIII ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, oraz projektowanych w rozdziale 5 PKE pozwoliłoby na częściowe zniwelowanie kosztów realizacji obowiązków przez przedsiębiorców telekomunikacyjnych.

Decyzja o uznaniu za dostawcę wysokiego ryzyka oraz środki naprawcze

W obecnym kształcie decyzja jest podejmowana jednoosobowo przez ministra właściwego do spraw informatyzacji. Z uwagi na wpływ tej decyzji na stosunki międzynarodowe z innymi państwami czy bezpieczeństwo wewnętrzne oraz skomplikowany charakter prawny, powinny uczestniczyć w jej podejmowaniu także inni ministrowie odpowiedzialni za obszary istotne z perspektywy chronionych wartości (obronność, bezpieczeństwo i porządek publiczny, zdrowie i życie ludzi) lub za obszary właściwe merytorycznie z perspektywy sektora, którego dotyczy decyzja (rozwój i technologia). Będzie to zgodne z analogicznymi rozwiązaniami funkcjonującymi w innych krajach UE. Przykładowo decyzja taka w Niemczech jest podejmowana przy udziale federalnego ministerstwa spraw wewnętrznych, zagranicznych i gospodarki.

Pozytywną opinię powinien wyrazić także Prezes Urzędu Ochrony Konkurencji i Konsumentów. Decyzja w sprawie uznania za dostawcę wysokiego ryzyka może bowiem, poprzez ograniczenie możliwości oferowania określonych produktów lub usług przez tego dostawcę, wpływać istotnie na konkurencję na rynku oraz korzystanie z usług przez użytkowników. Konsekwencją takiego – częściowego lub całkowitego – wykluczenia z rynku dostawcy czy dostawców, może być wzrost cen infrastruktury telekomunikacyjnej, a w konsekwencji wzrost cen świadczonych dla indywidulanych klientów usług telekomunikacyjnych.

Wyłączenie możliwości prowadzenia działalności gospodarczej danego rodzaju (a do tego sprowadzałoby się dla dostawcy wydanie decyzji na podstawie projektowanego art. 66a ust. 11), nie może być przy tym w demokratycznym państwie prawnym bezterminowe. Regulacja powinna w szczególności uwzględniać wpływ bardzo szybkiego rozwoju technologicznego

i dynamicznych zmian w zakresie zagrożeń związanych z cyberbezpieczeństwem na aktualność decyzji. Z tego względu w ocenie Izby regulacja powinna wymuszać przegląd aktualnych uwarunkowań, i stosownie do przypadku – dokonanie zmian w wydanej decyzji, wydanie nowej decyzji albo uznanie, że nie zachodzi już potrzeba wydawania w omawianym zakresie kolejnej decyzji. Uregulowania takie występują w innych krajach UE, np. w Austrii.

Warto podkreślić, że obecna wersja projektu nie przewiduje możliwości podjęcia przez dostawcę uznanego za dostawcę wysokiego ryzyka podjęcia odpowiednich i proporcjonalnych środków zaradczych wraz ze stosownym planem naprawczym, umożliwiającym reakcje na stwierdzone nieprawidłowości, co właściwie oznacza, że taki dostawca pomimo podejmowanych starań właściwie nie może w żaden sposób przeciwdziałać niekorzystnym skutkom decyzji, co w przypadku działalności gospodarczej powinno być normą. Środki o charakterze ostatecznym tj. wydanie decyzji o uznaniu za dostawcę wysokiego ryzyka, powinny być stosowane dopiero w ostatecznych sytuacjach.

Obowiązek wycofania produktu/usługi/procesu ICT

Decyzja ministra właściwego do spraw informatyzacji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka powinna zostać ograniczona do produktów, usług lub procesów ICT o charakterze krytycznym, a nie do każdego rodzaju produktu, usług lub procesów, w szczególności wyłączeniu z zakresu regulacji tych urządzeń, które zapewniają odpowiednie standardy szyfrowania i komunikacji, niezależnie od rozwiązań sprzętowych.

Jednocześnie apelujemy o ograniczenie procedury wykluczenia dostawców wysokiego ryzyka jedynie w odniesieniu do produktów, usług lub procesów ICT wykorzystywanych przez operatora strategicznej sieci bezpieczeństwa, lub ewentualnie podmiotów publicznych, nie rozszerzając zakresu regulacji do całego sektora prywatnego.

Obowiązek wycofania z użytkowania produktów pochodzących od dostawcy uznanego za dostawcę wysokiego ryzyka w ciągu 5 lat, przewidziany dla przedsiębiorców telekomunikacyjnych, być może jest wystarczający dla urządzeń końcowych, tj. aparatów telefonicznych czy modemów, które ulegają szybkiemu zużyciu w normalnym procesie użytkowania. Urządzenia sieciowe mają jednak zdecydowanie dłuższy cykl życia i wydłużenie tego okresu do co najmniej 7 lat mogłoby pozwolić na ograniczenie strat spowodowanych decyzją Ministra ds. informatyzacji. Izba podkreśla, że obowiązek wycofania urządzeń powinien być jednak rekompensowany odszkodowaniem, szczególnie w przypadku skrócenia okresu przewidzianego na wycofanie z użytkowania wskazanych w decyzji typów urządzeń do 5 lat.

Proponowane w przepisach **wymagania dot. cyberbezpieczeństwa sieci telekomunikacyjnych i infrastruktury cyfrowej, odnoszące się do wykorzystywanego sprzętu lub oprogramowania** w ramach infrastruktury telekomunikacyjnej **powinny dotyczyć wyłącznie OSSB, a nie wszystkich przedsiębiorców telekomunikacyjnych** świadczących komercyjne usługi ogółowi społeczeństwa, ponieważ zastosowanie tych samych wymagań będzie nieproporcjonalne wobec potrzeb i kosztów całego rynku.

Utworzenie OSSB, tym bardziej przemawia za tym, aby regulacje w sektorze prywatnym nie były tak daleko idące i ingerujące w prowadzoną przez przedsiębiorców działalność gospodarczą.

Ze względu na skupienie obsługi całej łączności państwowej w OSSB i określenie w tym zakresie wymagań dot. bezpieczeństwa sprzętu i oprogramowania, wytyczne dotyczące innych przedsiębiorców powinny zostać proporcjonalnie zmniejszone lub pozostawione decyzji własnej przedsiębiorców co do odpowiedniego ukształtowania i oceny procesów bezpieczeństwa architektury sieciowej na styku z dostawcami rozwiązań ICT.

OSSB

Prezes Rady Ministrów wyznacza Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) spośród grona podmiotów spełniających określone w art. 76b warunki. Stanowi to jawne naruszenie konkurencyjności rynku oraz ograniczenia swobody działalności gospodarczej. Na rynku krajowym istnieje jeden podmiot spełniający wymienione kryteria. Tym samym zapis ten wprost określa, który podmiot zostanie wyznaczony i wyłącza innych uczestników rynku z procedury wyboru, co stanowi ewidentny przykład dyskryminacji pośredniej.

Izba podkreśla również, że podmiot spełniający kryteria określone w art. 76b jest jednoosobową spółką Skarbu Państwa. W ocenie KIGEiT powierzenie tak małemu podmiotowi realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji może okazać się działaniem niemożliwym, bowiem działania takie wymagają zaangażowania zarówno znacznej liczby wykwalifikowanych pracowników, jak również posiadania odpowiednich zasobów infrastruktury, których wybrany podmiot nie posiada. Oznacza to, że OSSB do realizacji powierzonych mu celów będzie wykorzystywał dostęp do nieruchomości Skarbu Państwa czy jednostek samorządu terytorialnego, a także dostęp telekomunikacyjny świadczony przez operatorów publicznych sieci telekomunikacyjnych w zakresie kolokacji i współkorzystania z infrastruktury telekomunikacyjnej. Tym samym podmiot ten będzie pełnił jedynie rolę pośrednika, czerpiącego dodatkowy przychód od wymienionych w art. 76d podmiotów.

Projekt przewiduje, że operator będący adresatem decyzji Prezesa UKE w zakresie kolokacji oraz udostępniania, w tym współkorzystania z infrastruktury telekomunikacyjnej na rzecz OSSB, otrzyma w zamian zapłatę umożliwiającą zwrot proporcjonalnej części poniesionych kosztów powstania tej infrastruktury oraz ponoszonych kosztów jej utrzymania oraz uwzględnia wpływ zapewnienia tego dostępu na plan biznesowy operatora, w szczególności na realizowane przez niego inwestycje. Co ciekawe, projekt nie przewiduje zawarcia dobrowolnej umowy pomiędzy OSSB a operatorem, co może wskazywać na przewidywaną, z góry ustaloną maksymalną wysokość opłat, niekorelującą w żaden sposób z kosztami przedsiębiorcy udostępniającego.

OSSB otrzymuje również szczególne uprawnienia do nieodpłatnego korzystania z dostępu do nieruchomości, w tym budynków, należących do Skarbu Państwa oraz jednostek samorządu terytorialnego, polegające na umożliwieniu umieszczenia na niej infrastruktury telekomunikacyjnej, a także jej eksploatacji i konserwacji. Pomijając fakt uprzywilejowania OSSB na rynku telekomunikacyjnym, nie został przytoczony żaden koszt, jaki przyjęcie przepisów będzie oznaczało dla samorządów w wyniku spadku zainteresowania analogicznymi usługami ze strony pozostałych przedsiębiorców telekomunikacyjnych.

Ograniczenia stosowania przepisów kodeksu postępowania administracyjnego oraz udział dostawców i operatorów w procesie oceny dostawcy wysokiego ryzyka

Przepisy dotyczące postępowania w sprawie wydawania decyzji dotyczącej dostawcy wysokiego ryzyka wyłączają stosowanie niektórych podstawowych zasad procedury administracyjnej, np. art. 28 kpa definiującego stronę postępowania administracyjnego, jedocześnie definiując stronę jako „podmiot wobec którego zostało wszczęte postępowanie", ograniczając udział w postępowaniu tylko do ocenianego dostawcy. Inne podmioty, jak np. przedsiębiorcy telekomunikacyjni, którzy korzystają z rozwiązań danego dostawcy nie będą mieli wiedzy na temat prowadzonego postępowania zmierzającego do wykluczenia sprzętu czy oprogramowania w ich infrastrukturze. Przedsiębiorcy ci będą objęci pod względem organizacyjnym i kosztowym skutkami wydawanej decyzji.

Wyłączenie art. 79 kpa pozbawia dostawcę, jako stronę możliwości udziału w postępowaniu dowodowym z przesłuchania świadków, biegłych i oględzin.

Wyłączenie art. 106 § 5 kpa powoduje, że nie można wnieść zażalenia do sądu na opinię wydaną przez Kolegium. Inne wyłączenia kpa utrudniają wnoszenie środków odwoławczych od decyzji o wykluczeniu dostawcy, np. skarga na decyzję o wykluczeniu dostawcy z rynku jest rozpatrywana na posiedzeniu niejawnym, a po wniesieniu ww. skargi, sąd administracyjny nie może wstrzymać jej wykonalności

Wszystkie podmioty, w tym operatorzy i oceniani dostawcy, które będą objęte skutkami wydawanych decyzji powinny mieć pełną wiedzę i prawa w zakresie prowadzonego postępowania, ponieważ wydawane decyzje będą dla nich oznaczały obowiązki w zakresie zmian dotyczących architektury sieciowej. Konieczne są więc zmiany zaproponowanych przepisów, które umożliwią prowadzenie postępowania z poszanowaniem praw wszystkich zainteresowanych podmiotów. Zmiany te polegałyby w pierwszej kolejności na wprowadzeniu możliwości udziału w postępowaniu dot. dostawcy wysokiego ryzyka wszystkim podmiotom, na których prawa wydawana decyzja będzie oddziaływała.

Nacjonalizacja 5G

Lektura projektu nowelizacji UKSC w zakresie Działu III prowadzi do konstatacji, że duża część rynku telekomunikacyjnego zostanie zawłaszczona przez spółkę Skarbu Państwa. Dodatkowo w ocenie Izby konieczne jest zbadanie, czy działanie takie nie wyczerpuje znamion nieuzasadnionej pomocy publicznej i jako takie powinno zostać zbadane przez odpowiednie organy UE, w tym TSUE. Dziwi zatem fakt, że *Projektowana ustawa nie wymaga przedstawiania organom i instytucjom Unii Europejskiej w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.*

Dystrybucja pasma 700 MHz

W ocenie Izby, plan budowy strategicznej sieci bezpieczeństwa i przyznania na ten cel 10 MHz z zakresu 700 MHz Operatorowi SSB należy uregulować odrębnie od kwestii zagospodarowania pozostałej części (20 MHz) pasma 700 MHz, przeznaczonej na potrzeby świadczenia publicznych usług telekomunikacyjnych w sieciach ruchomych. Nie jest również zasadne wprowadzanie ograniczeń w zakresie wykorzystania częstotliwości w celu świadczenia usług detalicznych przez dysponentów rezerwacji.

Należy również podkreślić, że warunki gospodarowania częstotliwościami, w tym zasady dotyczące przeprowadzania postępowań selekcyjnych, zostały kompleksowo uregulowane w Rozdziale 1 Działu IV ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Projektowany art. 76p jest więc zbędny, co przemawia za jego usunięciem.

Ponadto Izba zwraca uwagę, że nie została zaktualizowana OSR.

Jednocześnie, zgodnie z prośbą otrzymaną w toku konsultacji wewnątrz-izbowych od dwóch członków Izby, firmy Exatel S.A. oraz Motorola Solutions Polska Sp. z o.o., informuję o wyłączeniu poparcia tych firm dla treści powyższego stanowiska oraz załączonych w tabeli uwag.

Z poważaniem

Prezes Zarządu

Stefan Kamiński

Signature Not Verified
Dokument podpisany przez Stefan Kamiński; KIGEiT
Data: 2021.11.02 17:25:59 CET
Powód: Złożenie podpisu

Załącznik: *Tabela z uwagami do projektu (z dn. 12 października 2021 r.) ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*

Załącznik do pisma: KIGEiT/1970/11/2021

Uwagi Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
1.	**Art. 1**	KIGEiT	Przyjęta technika prowadzenia procesu legislacyjnego, w szczególności konsultacji publicznych, wyklucza możliwość szczegółowego zapoznania się z projektem oraz zgłoszenia opinii i uwag. Fakt przeprowadzenia konsultacji publicznych wersji projektu opatrzonej datą 7 września 2020 r. oraz procedowanie kolejnych wersji bez zebrania o nich uwag przeczy chęci szczegółowego poznania opinii rynku oraz wskazuje na fasadowy charakter tego etapu.	
2.	**Art 1**	KIGEiT	Izba podtrzymuje zgłaszane w toku prac, poza konsultacjami, uwagi zawarte m.in. w stanowisku z dn. 2 lutego 2021 r. (KIGEiT/365/02/2021) w zakresie wymienionych w nim punktów: 1-7.	
3.	**Art. 1 pkt 2) lit. c)**	KIGEiT	Izba zgłasza, że jednocześnie procedowany projekt ustawy PKE oraz ustawy „Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej" stanowi, że „Ustawa o Krajowym Systemie Cyberbezpieczeństwa" (dalej UKSC) obejmie przedsiębiorców telekomunikacyjnych w dacie wejścia w życie tych przepisów. Występuje zatem sprzeczność postanowień dwóch odrębnie procedowanych projektów aktów prawnych.	
4.	**Art. 1 pkt 2) lit. c)**	KIGEiT	Pomimo podtrzymanego (tymczasowo) wyłączenia przedsiębiorców telekomunikacyjnych spod zakresu obowiązywania UKSC, podlegają oni przepisom: dot. obowiązku wycofania produktów ICT, usług ICT, procesów ICT pochodzących od dostawcy wysokiego ryzyka, dotyczącym ostrzeżenia i polecenia zabezpieczającego oraz karach pieniężnych. Objęcie KSC przedsiębiorców telekomunikacyjnych oznacza dla nich dodatkowe obowiązki i koszty (jak wskazuje uzasadnienie), co może być bardzo trudne do realizacji zwłaszcza przez małych przedsiębiorców. Obowiązek wycofania konkretnego sprzętu, usług, procesów konkretnego dostawcy bez odszkodowania powoduje wymierne koszty dla każdego podmiotu. Obowiązek wycofania urządzeń powinien być rekompensowany odszkodowaniem, szczególnie w przypadku skrócenia okresu przewidzianego na wycofanie z użytkowania wskazanych w decyzji typów urządzeń do 5 lat.	
5.	**Art. 1 pkt 3 lit d**	KIGEiT	**W art. 1 pkt 3 lit d po pkt 4b dodaje się pkt 4c w brzmieniu następującym:** „*funkcje krytyczne – oznaczają funkcje zawarte w wykazie funkcji krytycznych dla bezpieczeństwa sieci i usług, o którym mowa w art. 66f, które są krytyczne dla bezpieczeństwa produktów ICT, usług ICT i procesów ICT*;" **Uzasadnienie:** Projekt nie przewiduje definicji „funkcji krytycznych", podczas gdy to pojęcie jest istotne z perspektywy wprowadzanych instytucji prawnych, w szczególności postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Z tego względu proponuje się zdefiniowanie tego pojęcia w art. 2 ustawy, poprzez odwołanie do szczegółowego postanowienia odnoszącego się do trybu określania wykazu funkcji krytycznych w proponowanym art. 66f (pkt 37 poniżej). W przypadku braku uwzględnienia uwagi dotyczącej art. 66f (pkt 37 poniżej), proponuje się dodanie pkt 4c w brzmieniu następującym:	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			„funkcje krytyczne – oznaczają funkcje zawarte w wykazie funkcji krytycznych dla bezpieczeństwa sieci i usług, stanowiącym załącznik nr 3 do ustawy, które są krytyczne dla bezpieczeństwa produktów ICT, usług ICT i procesów ICT zgodnie z wykazem krytycznych aktywów zawartym w 5G Toolbox;"	
6.	**Art. 1 pkt 3 lit d**	KIGEiT	**W art. 1 pkt 3 lit d po pkt 4c dodaje się pkt 4d w brzmieniu następującym:** *„5G Toolbox* – oznacza dokument „Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G" opublikowany w styczniu 2020 roku i jego kolejne wersje. **Uzasadnienie:** Definicja jest skorelowana z propozycją wprowadzenia definicji dla pojęcia funkcji krytycznych w pkt 5 powyżej.	
7.	**Art. 1 pkt. 11** (dotyczy Art. 9 ust. 1 pkt 1 UKSC)	KIGEiT	Wydaje się, że właściwym rozwiązaniem byłoby określenie „co najmniej dwie osoby", nie ograniczając górnego limitu, co w przypadku dużych przedsiębiorców może ułatwić zapewnienie całodobowej dostępności upoważnionych osób.	
8.	**Art. 1 pkt. 43** (Rozdział 11a)	KIGEiT	Ogromne koszty certyfikacji produktów i usług ICT, obejmujące zarówno koszty samych audytów certyfikacyjnych, jak i utrzymanie niezbędnej dokumentacji i wymogów (np. audyty wewnętrzne, analizy ryzyka) a przede wszystkim koszty dostosowania rozwiązań do tych wymogów. Powoduje to dodatkowe koszty działalności przedsiębiorców, które powinny zostać zrekompensowane.	
9.	**Art. 1 pkt 47 lit a**	KIGEiT	**W art. 1 pkt 47 lit a dodany do art. 65 ust. 1 pkt 7 otrzymuje brzmienie następujące:** *„7) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania o funkcjach krytycznych, za dostawcę wysokiego ryzyka;"* **Uzasadnienie:** Decyzja w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka powinna uwzględniać kategorie funkcji krytycznych dla bezpieczeństwa sieci i usług (por. w tym zakresie argumentację zawartą w pkt 12 poniżej). W konsekwencji projektowany przepis art. 65 ust. 1 pkt 7 powinien być uzupełniony poprzez wskazanie, że przepis ten dotyczy dostawcy sprzętu lub oprogramowania o funkcjach krytycznych. Zmiana skorelowana jest ze zmianą proponowaną w pkt 5 (definicja funkcji krytycznych).	
10.	**Art. 1 pkt 49 lit b**	KIGEiT	**W art. 1 pkt 49 lit b w art. 66 ust. 4 dodaje się pkt 8 w następującym brzmieniu:** *„8) w sprawach określonych w art. 66a ust. 7 – przedstawiciele operatora strategicznej sieci bezpieczeństwa który nabywa lub posiada produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie"* Alternatywnie – w razie braku uwzględnienia uwagi zawartej w pkt 12 w zakresie odniesienia decyzji wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB: *„8) w sprawach określonych w art. 66a ust. 7 – przedstawiciele podmiotów wskazanych w art. 66a pkt 1) – 4), które nabywają lub posiadają produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie"*	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Uzasadnienie: Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka prowadzone jest w specyficznym trybie, a skutki decyzji daleko wybiegają poza bezpośrednie konsekwencje dla dostawcy, którego sprzęt lub oprogramowanie podlega ocenie. Prace Kolegium w zakresie opracowania opinii mają kluczowe znaczenie dla tego postępowania. Opinia ta w praktyce będzie stanowić podstawowe uzasadnienie merytoryczne dla decyzji podejmowanej przez organ. Z tego względu kluczowe jest zapewnienie odpowiednio wysokiej jakości merytorycznej analizy. Skład Kolegium ma co do zasady charakter polityczny (art. 66 ust. 1 ustawy). Z tego względu zasadne jest, by udział w procesie analizy – poza członkami Kolegium – zapewniony został także podmiotom eksperckich, aktywnym na rynku i najlepiej znających bieżące uwarunkowania techniczne i rynkowe. Z perspektywy ekonomiki postępowania, zasadne jest także uwzględnienie w składzie zespołu pracującego nad opinią, także samego dostawcy, którego postępowanie dotyczy. Umożliwi to bieżące udzielanie wyjaśnień, przedstawianie dokumentów czy dodatkowych informacji. Udział dostawcy umożliwi mu bieżącą korektę w obszarach wiążących się z ryzykiem zakwestionowania oraz przygotowanie się z wyprzedzeniem na ewentualną konieczność podjęcia kroków naprawczych (w razie wydania decyzji o uznaniu za dostawcę wysokiego ryzyka). Proponowana zmiana skorelowana jest z propozycją opisaną w pkt 37.	
11.	**Art. 1 pkt. 50** (dot. art. 66a)	KIGEiT	Wykluczenie dostawcy pochodzącego z państwa spoza UE i NATO może doprowadzić nie tylko do naruszenia umów międzynarodowych, lecz również do wykluczenia producentów sprzętu bardziej zaawansowanego technicznie i korzystających z nowocześniejszych rozwiązań w przyszłości. Sytuacja geopolityczna uległa zmianie od chwili powstania propozycji tych przepisów i wydaje się, że rozwiązania stosowane przez dostawców z państw określanych jako zaufanych mogą w niedługim czasie okazać się niewystarczająco nowoczesne, drogie i podatne na np. kryzys na rynku półprzewodników. Dodatkowo, w art. 66a ust. 1 powinien być wymieniony Operator strategicznej sieci bezpieczeństwa – Izba podtrzymuje argumentację przytoczoną w piśmie z dn. 2 lutego 2021 r. (sygn. KIGEiT/365/02/2021).	
12.	**Art. 1 pkt 50** (dot. art. 66a ust. 1 i 2)	KIGEiT	**W art. 1 pkt 50 przepis art. 66a ust. 1 i 2 otrzymuje brzmienie:** *„Art. 66a.* 1. *Minister właściwy do spraw informatyzacji, w celu ochrony ważnego interesu państwowego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium, gdy istnieją konkretne dowody lub uzasadnione podejrzenia, że sprzęt lub oprogramowanie określonego dostawcy zagraża bezpieczeństwu narodowemu, postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania o którym mowa w ust. 2, wykorzystywanych przez operatora strategicznej sieci bezpieczeństwa, za dostawcę wysokiego ryzyka, zwane dalej „postępowaniem w sprawie uznania za dostawcę wysokiego ryzyka”.* 2. *Dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT o funkcjach krytycznych”* **Uzasadnienie:** Proponowane zmiany odnoszą się do trzech zagadnień – przesłanek wszczęcia postępowania w sprawie uznania za dostawcę wysokiego ryzyka, doprecyzowania rodzaju sprzętu lub oprogramowania, które może być przedmiotem	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			takiego postępowania oraz wskazania podmiotu, w odniesieniu, do którego korzystanie ze sprzętu lub oprogramowania może skutkować zagrożeniem uzasadniającym wszczęcie postępowania. [**przesłanki postępowania**] Proponuje się, by postępowanie wszczynane było, jeśli zaistnieją konkretne dowody lub uzasadnione podejrzenia, że określony dostawca zagraża bezpieczeństwu narodowemu. Aktualnie projektowane brzmienie przepisu nie określa przesłanek wszczęcia postępowania, pozostawiając organowi bardzo dużą dowolność w tym obszarze. W konsekwencji może pojawić się ryzyko wszczynania postępowań bezpodstawnych (nieuzasadnionych) i ponoszenia w związku z tym kosztów obciążających budżet. Przede wszystkim jednak tak szerokie ujęcie będzie negatywnie wpływać na poziom zaufania do właściwego organu przez uczestników rynku – zarówno po stronie producentów sprzętu lub oprogramowania jak i podmiotów je nabywających. Proponowana zmiana zapewni, że prowadzone będą postępowania uzasadnione konkretnymi dowodami na zagrożenia bezpieczeństwa narodowego lub uzasadnionymi (a więc znajdującymi poparcie w danych okolicznościach) podejrzeniami, co zniweluje opisane wyżej ryzyka. [**sprzęt lub oprogramowanie o funkcjach krytycznych**] Ponadto postuluje się, by postępowanie w sprawie uznania za dostawcę wysokiego ryzyka dotyczyło dostawcy, który dostarcza sprzęt lub oprogramowanie o funkcjach krytycznych, a nie każdy rodzaj sprzętu. Obecne brzmienie przepisu umożliwia bowiem prowadzenie postępowania także w kontekście sprzętu lub oprogramowania, które nie mają i nie mogą mieć znaczenia dla ochrony bezpieczeństwa. Aktualnie projektowany zakres możliwego postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest niezwykle szeroki i obejmuje w praktyce każdego producenta, dystrybutora lub importera produktów, usług lub procesów ICT lub produktów i usług dla infrastruktury telekomunikacyjnej. W raporcie Grupy Współpracy ds. Bezpieczeństwa Sieci i Informacji z postępów państw członkowskich we wdrażaniu zestawu narzędzi UE w zakresie cyberbezpieczeństwa 5G z lipca 2020 r. wskazano, że zdefiniowanie kluczowych aktywów podlegających ograniczeniom jest jednym z głównych wyznaczników skutecznej realizacji działania strategicznego SM03[1]. W skoordynowanej ocenie ryzyka UE zidentyfikowane zostały najbardziej wrażliwe aktywa (np. funkcje sieci bazowej, funkcje zarządzania siecią i orkiestracji oraz funkcje sieci dostępu) oraz główne kryteria, które należy wziąć pod uwagę przy ocenie wrażliwości różnych aktywów[2]. W myśl powyższego proponowana zmiana doprecyzowuje, że postępowanie powinno dotyczyć sprzętu lub oprogramowania o funkcjach krytycznych – co jest spójne z wytycznymi zawartymi w EU 5G Toolbox[3]. Pozwoli także uchronić się przed zarzutem naruszenia zasady proporcjonalności, którego ryzyko generuje aktualnie projektowane brzmienie przepisu. W kontekście sposobu identyfikowania funkcji krytycznych – por. uzasadnienie do pkt 26. [**podmioty korzystające z rozwiązań ICT o funkcjach krytycznych**]	

[1] https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, s. 11 i 16.
[2] Zob. raport NIS Cooperation Group z 9 października 2019 r. *EU coordinated risk assessment of the cybersecurity of 5G networks*, pkt. 2.20 i 2.21, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.
[3] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, styczeń 2020

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Zgodnie z projektowanym brzmieniem, katalog podmiotów, korzystających ze sprzętu i oprogramowania potencjalnie objętego postępowaniem, obejmować będzie tysiące podmiotów prawa prywatnego i publicznego (operatorzy usług kluczowych, dostawcy usług cyfrowych, jednostki sektora finansów publicznych wymienione w ustawie – w tym jednostki samorządu terytorialnego, itd.). Także w tym zakresie projekt stwarza ryzyko zarzutu naruszenia zasady proporcjonalności. Skoro bowiem ustawodawca zakłada utworzenie operatora strategicznej sieci bezpieczeństwa – OSSB – i powierza mu niezwykle szeroko zdefiniowane zadania, kluczowe dla bezpieczeństwa Państwa (art. 76a ust. 2). – uzasadnione jest, by omawiana regulacja w sprawie uznania za dostawcę wysokiego ryzyka odnosiła się właśnie do OSSB, bez generowana dodatkowych obciążeń dla innych uczestników rynku. Strategiczna sieć bezpieczeństwa jest bowiem stworzona właśnie w celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji (art. 76a ust. 1). Odniesienie postępowania w sprawie uznania za dostawcę wysokiego ryzyka do sprzętu lub oprogramowania, z którego korzysta OSSB, w świetle obszernego katalogu zadań przypisanych OSSB, będzie wystarczające dla zapewnienia podstawowego celu regulacji jakim jest wzmacnianie bezpieczeństwa państwa.	
13.	**Art. 1 pkt 50** (dot. art. 66a ust. 3)	KIGEiT	**W art. 1 pkt 50 w dodanym art. 66a ust. 3 skreśla się następujący fragment:** *„z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy”.* **Uzasadnienie:** Obecna wersja Projektu ogranicza możliwość udziału na prawach strony innych podmiotów, np. operatorów telekomunikacyjnych (art. 28 k.p.a.), wyklucza możliwość dopuszczenia do udziału w postępowaniu zainteresowanych organizacji społecznych (art. 31 k.p.a.), czy wreszcie uprawnienia strony w zakresie przeprowadzenia czynności dowodowych (art. 79 k.p.a.). Poprzednie wersje Projektu nie przewidywały tak daleko idących ograniczeń dla uczestników postępowania. Proponowane rozwiązanie stanowi daleko idące ograniczenie podstawowych praw przewidzianych dla uczestników postępowania w przepisach powszechnie obowiązujących i może skutkować naruszeniem podstawowych zasad rzetelnego postępowania. W szczególności niepokojący jest projekt wyłączenia stosowania art. 28, 31 i 79 KPA. **Wyłączenie stosowania art. 28 i 31 KPA** Zgodnie z uzasadnieniem Projektu: „*Zawężenie przymiotu strony oraz udziału organizacji społecznej jest koniecznej w celu uniknięcia obstrukcji postępowania i wzmocnić trwałość rozstrzygnięć, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania”.* Takie uzasadnienie nie przekonuje i stwarza bardzo duże ryzyka w kontekście ograniczania sprawiedliwości proceduralnej podmiotów rynku. Powyższa argumentacja może być bowiem zastosowana dla wyłączenia wskazanych przepisów w każdej sprawie, wskazując na konieczność zapewnienia trwałości rozstrzygnięcia i uniknięcia obstrukcji. Tymczasem w szczególności z uwagi na szczególną wagę postępowania w sprawie uznawania za dostawcę wysokiego ryzyka – i jego bardzo daleko idące skutki rynkowe i potencjalnie społeczne, niezbędne jest zapewnienie udziału w postępowaniu podmiotów, na których prawa i obowiązki oddziaływać będzie decyzja, jak również zapewnić udział strony społecznej. Nie sposób nie zauważyć, iż wyłączenie stosowania art. 28 k.p.a. oraz zdefiniowanie nowego pojęcia „strony” w myśl proponowanego brzmienia art. 66a ust. 4 (wskazane w art. 1 pkt 50 projektu) implikuje ryzyko nie tylko zbyt skrajnego	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			ograniczenia, ale także całkowitego wyłączenia możliwości ochrony praw przez podmioty związane decyzją w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka, ale niemieszczące się w pojęciu „strony" w brzmieniu proponowanym przez projektodawcę w art. 1 pkt 50 niniejszego projektu. O ile stosowanie szczególnych względem k.p.a. definicji strony w aktach prawnych regulujących szczegółowe obszary gospodarki jest zjawiskiem występującym w systemie postępowania administracyjnego, o tyle należy zwrócić uwagę na daleko idące, *de facto*, zrównanie pojęcia strony z „podmiotem wobec którego zostało wszczęte postępowanie", które uniemożliwia udział w postępowaniu podmiotom, których prawa i obowiązki będą kształtowane przez wydaną w toku takiego postępowania decyzję. Wbrew zatem stanowi faktycznemu, stroną postępowania będzie tylko podmiot formalnie wskazany jako strona przez organ wszczynający postępowanie, a więc tylko od woli organu wszczynającego postępowanie będzie zależeć, kto będzie stroną postępowania – ze wszystkimi tego procesowymi konsekwencjami, w tym możliwością lub brakiem możliwości ochrony swoich praw. Prawo do rzetelnego postępowania administracyjnego (w szczególności – prawo do przedstawienia swojej argumentacji, do obrony oraz do uczestnictwa w postępowaniu, którego wynik decyduje o prawach bądź obowiązkach) należy wywodzić z wartości konstytucyjnych oraz międzynarodowych – w szczególności z prawa do sądu oraz zasady demokratycznego państwa prawa[4]. Ograniczanie praw podmiotów powinno być każdorazowo badane z perspektywy art. 31 ust. 3 Konstytucji RP, który wskazuje wprost, iż ograniczenia konstytucyjnych wolności i praw nie mogą naruszać samej istoty tych wolności i praw. Proponowane w Projekcie wyłączenie stosowania art. 28 k.p.a. naruszy istotę prawa do korzystania z uprawnień strony oraz prawa do czynnego uczestnictwa w postępowaniu względem podmiotu lub podmiotów będących adresatami obowiązków wynikających z przedmiotowej decyzji. Redukcja tak głębokiej ingerencji w uprawnienia podmiotów posiadających interes prawny w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka byłaby również możliwa przez rozszerzenie statusu strony postępowania także o podmioty wskazane w art. 66b ust. 1 w związki z objęciem ich konsekwencjami wydania decyzji, które projektodawca przedstawia w pkt 1 i 2 powyższego przepisu. Rozwiązanie to również wydaje się słuszne z punktu widzenia ochrony interesów stron oraz chęci uniknięcia obstrukcji postępowania przez projektodawcę, wskazanego w uzasadnieniu projektu. **Wyłączenie stosowania art. 79 kpa** Projekt wyłącza regulację KPA gwarantującą stronie możliwość udziału w postępowaniu dowodowym w odniesieniu do przesłuchania świadków i biegłych czy przeprowadzania oględzin. W połączeniu z pozostałymi ograniczeniami praw proceduralnych (por. uwagi powyżej oraz pkt 7-8, 17-18), strona zostanie faktycznie pozbawiona realnego wpływu na postępowanie i przedstawienie swojej argumentacji. Proponowane rozwiązanie stanowi zaprzeczenie zasad ogólnych postępowania administracyjnego, które mają **umocowanie konstytucyjne**, zwłaszcza przy uwzględnieniu potencjalnej możliwości wyłączenia jawności niektórych dokumentów na podstawie art. 74 kpa. Tak daleko idące ograniczenia nie mają żadnego uzasadnienia – nawet bowiem powołanie się na względy bezpieczeństwa narodowego nie pozwalają na odebranie stronie konstytucyjnego prawa do obrony. **Z tego względu wskazane wyłączenie powinno zostać usunięte.**	

[4] J. Szremski, Prawo do postępowania administracyjnego i jego elementy jako wartości wynikające z uregulowań konstytucyjnych, międzynarodowych oraz europejskich, Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury, Zeszyt 2 (42)/2021, s. 38.

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			W praktyce mogą wystąpić okoliczności uzasadniające wyłączenie jawności określonych czynności – w przypadku, gdy takie ujawnienie byłoby sprzeczne z obowiązującym prawem (w szczególności w zakresie informacji niejawnych) lub z prawem międzynarodowym. W żadnym jednak wypadku ograniczenie udziału strony w postępowaniu dowodowym nie powinno być zasadą, a rozstrzygnięcie organu o wyłączeniu możliwości udziału w czynnościach powinno mieć charakter zaskarżalnego postanowienia na zasadach ogólnych.	
14.	**Art. 1 pkt 50** (dot. art. 66a ust.4)	KIGEiT	**W art. 1 pkt 50 w art. 66a skreśla się projektowany ust. 4.** **Uzasadnienie:** Proponowana zmiana jest skorelowana z postulatem wykreślenia wyłączenia stosowania art. 28 KPA (por. pkt 8 powyżej). Usunięcie ust. 4 umożliwi bezpośrednie stosowanie przepisów KPA odnoszących się do pojęcia „strony postępowania". Obecna treść art. 66a ust. 4 zawęża pojęcie strony tylko do tego wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Przyjęcie takiej definicji względem art. 28 k.p.a. zawierającego znacznie szersze znaczenie strony może nieść ze sobą wyłączenie możliwości ochrony praw podmiotów, których obowiązki zostaną ukształtowane w wyniku wydania decyzji w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. W tym kontekście por. uwagi do pkt 8 powyżej.	
15.	**Art. 1 pkt 50** (dot. art. 66a ust.6)	KIGEiT	**W art. 1 pkt 50 w projektowanym art. 66a skreśla się ust. 6** **Uzasadnienie:** Projekt przewiduje we wskazanym punkcie brak obowiązku doręczenia zawiadomienia o wszczęciu postępowania podmiotom spoza UE / EFTA/ Konfederacji Szwajcarskiej, co stanowi istotne odstępstwo od zasad ogólnych kpa. W uzasadnieniu Projektu brak w tym zakresie wyjaśnienia przyczyn przyjętego podejścia. Obecne brzmienie stwarza ryzyko dyskryminacji podmiotów spoza wskazanych regionów (w tym w szczególności podmiotów położonych w Ameryce Północnej lub Azji, w których działa cały szereg dostawców rozwiązań ICT, potencjalnie objętych regulacją). Zważywszy, że projekt przewiduje względem takich podmiotów opublikowanie informacji o postępowaniu jedynie na stronie podmiotowej BIP organu (potencjalnie – wyłącznie w języku polskim), występuje bardzo wysokie ryzyko braku realnej możliwości uzyskania informacji o prowadzanym postępowaniu przez zainteresowany podmiot. Stanowi to zaprzeczenie podstawowej zasady postępowania administracyjnego polegającej na zapewnieniu stronie czynnego udziału w postępowaniu. Może być także sprzeczne z umowami międzynarodowymi, których stroną jest Rzeczpospolita Polska (w szczególności umów popieraniu i wzajemnej ochronie inwestycji, a potencjalnie także Porozumienia o Wolnym Handlu GATT).	
16.	**Art. 1 pkt 50** (dot. art. 66a ust. 7)	KIGEiT	W art. 1 pkt 50 w art. 66a ust. 7 nadaje się następujące brzmienie: *„W przypadku wszczęcia postępowania w sprawie uznania za dostawcę wysokiego ryzyka, minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Terminu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy."* **Uzasadnienie:**	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Wbrew treści uzasadnienia ustawy, zgodnie z obecnym brzmieniem projektu opinia Kolegium nie będzie sporządzana „każdorazowo", a jedynie w przypadku, w którym postępowanie w sprawie uznania za dostawcę wysokiego ryzyka zostało wszczęte z urzędu. W przypadku wszczęcia postępowania na wniosek przewodniczącego Kolegium, brak jest ustawowej gwarancji zapewniającej, że także w tym wypadku rozstrzygnięcie zostanie poprzedzone pogłębioną analizą wszystkich mających znaczenie okoliczności. Potencjalnie takie rozwiązanie stwarza też ryzyko wykorzystywania wskazanego ograniczenia jako furtki pozwalającej na pominięcie kroku w postaci uzyskania opinii Kolegium. Opinia ta ma tymczasem kluczowe znaczenie z perspektywy rozstrzygnięcia i kształtowania podejścia do cyberzagrożeń. W naszej ocenie, sam fakt wszczęcia postępowania na wniosek przewodniczącego Kolegium nie oznacza jeszcze, że taka analiza została sporządzana, a nawet jeśli tak – nie gwarantuje jej zawartości ani formy sporządzenia, nie wywołuje też żadnych skutków w postępowaniu (teoretycznie – nie musi nawet zostać uwzględniona przez organ wydający decyzję). W odniesieniu do propozycji usunięcia wyłączenia stosowania art. 106 § 5 kpa, to należy przypomnieć, że zgodnie z tym przepisem, zajęcie stanowiska przez ten organ następuje w drodze postanowienia, na które służy stronie zażalenie. Efektem wyłączenia art. 106 § 5 będzie także brak możliwości wniesienia zażalenia na opinię – jej kwestionowanie będzie więc możliwe dopiero na etapie wnoszenia skargi do sądu administracyjnego. Negatywnie wpływać to będzie na ekonomikę procesową i zwiększy ryzyko uchylania decyzji, opartych na opiniach niespełniających wymogów określonych w ustawie, których nie można było zakwestionować na wcześniejszym etapie, bez angażowania drogi sądowej. Wyłączenie w obecnej wersji Projektu stosowania art. 106 § 5 k.p.a. oznacza także brak określenia formy prawnej wydawanej opinii – a w konsekwencji brak możliwości jasnego określenia jej statusu. Niewątpliwie opinia będzie mieć faktyczną wartość dowodową – kluczową dla wydania decyzji, nie jest jednak jasne, czy będą stosować się do niej pozostałe przepisy kpa odnoszące się do stanowisk organów wydawanych w toku postępowania administracyjnego. Takie rozwiązanie będzie powodować duże wątpliwości praktyczne w zakresie skutków wydania opinii (lub braku jej wydania w terminie) na przebieg postępowania.	
17.	**Art. 1 pkt. 50** (dot. art. 66a ust. 8)	KIGEiT	Niejasne kryteria oceny, na której oparta będzie analiza służąca opinii Kolegium. Izba podtrzymuje uwagi złożone w piśmie z dn. 2 lutego 2021 r. (sygn. KIGEiT/365/02/2021) pkt 3 - 4.	
18.	**Art. 1 pkt 50** (dot. art. 66a ust. 8 pkt 2)	KIGEiT	**W art. 1 pkt 50 w art. 66a ust. 8 punkt 2 otrzymuje brzmienie:** *„2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:* *a) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności tam gdzie nie zostały zawarte umowy międzynarodowe w zakresie ochrony tych danych między Unią Europejską i tym państwem, lub czy dostawca sprzętu lub oprogramowania przestrzega postanowień rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* *b) struktury własnościowej dostawcy sprzętu lub oprogramowania, w tym z uwzględnieniem informacji o dostawcy z Centralnego Rejestru Beneficjentów Rzeczywistych, zgodnie z przepisami prawa polskiego lub odpowiedniego właściwego rejestru prowadzonego przez państwo członkowskie Unii Europejskiej.*	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Uzasadnienie: Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci telekomunikacyjnych, pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci telekomunikacyjnych, w oparciu o niedookreślone kryteria, które nie zawierają rzeczywistych elementów analizy technicznej. Projekt w art. 66a ust. 8 wśród kryteriów oceny wymienia kryteria ocenne i niezwykle szerokie, w szczególności ocenę przepisów prawa regulujących stosunki pomiędzy dostawcą a państwem oraz praktyki stosowania prawa w tym zakresie (art. 66a ust. 8 pkt 2 lit a Projektu). Brak jest wskazówek co do standardu dowodu wymaganego do oceny zagrożeń, wpływu państwa trzeciego, wagi podatności na zagrożenia i incydentów oraz stopnia kontroli procesu produkcji i dostawy (art. 66a ust. 4 Projektu). W naszej ocenie proponowane podejście nie będzie w praktyce możliwe do poddania merytorycznej kontroli. Z uwagi na brak precyzji sformułowań, zakres swobody pozostawiony Kolegium nie znajduje uzasadnienia w świetle celu jakim jest zapewnienie bezpieczeństwa publicznego. Nie daje też wystarczających gwarancji ograniczenia ryzyka dyskryminacji, co będzie wpływało negatywnie na poziom zaufania adresatów regulacji do organów państwa. Proponowane zmiany (wraz ze zmianami opisanymi w pkt 12) ograniczają arbitralność regulacji w tym zakresie, jednocześnie zapewniając Kolegium odpowiednio szerokie możliwości weryfikacji. Propozycje są skorelowane ze zmianami proponowanymi w pkt 23 w zakresie włączenia w proces analizy podmiotów eksperckich oraz samego zainteresowanego.	
19.	**Art. 1 pkt 50 (**66a ust. 8, pkt 6)	KIGEiT	**W art. 1 pkt 50 w art. 66a ust. 8 po punkcie 6** dodaje się następujące postanowienia: „7) *treści deklaracji wiarygodności od producentów i dostawców infrastruktury telekomunikacyjnej, przedkładanej operatorom telekomunikacyjnym oraz aktualizowanej nie rzadziej niż co dwa lata, która powinna w szczególności zawierać:* *a) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do współpracy z przedsiębiorcą w zakresie techniki bezpieczeństwa, a w szczególności do wczesnego informowania o nowych produktach, technologiach i aktualizacjach istniejących linii produktów;* *b) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej, że żadne informacje pochodzące z jego relacji umownych z przedsiębiorcą nie zostaną przekazane osobom trzecim;* *c) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej polegające na niezwłocznym poinformowaniu przedsiębiorcy, że nie może już zagwarantować dotrzymania zadeklarowanego zobowiązania;* *d) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do posługiwania się wyłącznie godnymi zaufania pracownikami przy opracowywaniu i produkcji krytycznych pod względem bezpieczeństwa części infrastruktury telekomunikacyjnej;* *e) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie;* *f) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej, że produkt, którego dotyczy składana deklaracja, nie posiada celowo wdrożonych wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie;* *g) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa;*	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			8) zobowiązania do zapewnienia integralności dostarczanych krytycznych składników infrastruktury, a w szczególności w zakresie: *a) możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu;* *b) sprawdzenia w czasie odbioru, czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione;* *9) zobowiązania prowadzenia monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;* *10) zobowiązania zatrudniania tylko przeszkolonych specjalistów w obszarach związanych z bezpieczeństwem, posiadających stosowne kompetencje i doświadczenie;* *11) zobowiązania uzyskania przez producenta sprzętu telekomunikacyjnego międzynarodowych lub uznanych przez UE norm bezpieczeństwa cybernetycznego;* *12) zobowiązania zapewnienia przez producenta ciągłości dostaw*". **Uzasadnienie:** Projekt znacząco ogranicza ilość kryteriów oceny umożliwiających ocenę sprzętu lub oprogramowania pod względem technicznym bezpieczeństwa infrastruktury, czyli weryfikacji za pomocą mierzalnych technicznych kryteriów, bezpieczeństwa tej infrastruktury (art. 66a ust. 8 pkt 4-6 Projektu). Proponowane aktualnie kryteria nie składają się na systemowe, spójne rozwiązanie i należy obawiać się, że nie będą w praktyce odgrywać istotnej roli w procesie decyzyjnym. Tymczasem zalecenia Komisji europejskiej odnoszące się do wdrażania rozwiązań 5G Toolbox jednoznacznie przewidują, że ocena ryzyka dostawców powinna być niedyskryminująca a „ocena profili ryzyka dostawców była prowadzona wyłącznie ze względów bezpieczeństwa i na podstawie obiektywnych kryteriów". Przedstawione w propozycji uzupełnienia tego artykułu o techniczne kryteria oceny są ze sobą powiązane i tworzą spójny model ochrony bezpieczeństwa infrastruktury. Model ten charakteryzuje się obiektywnością weryfikacji kryteriów i bardzo dużym stopniem profesjonalizacji weryfikacji, gwarantującej poprawność wyników stosowanych kryteriów oceny. Kryteria pozatechnologiczne, bardzo często są niedefiniowalne i posługują się niedookreślonymi pojęciami, które są bardzo trudne do zweryfikowania i dokonania oceny. Nie powinny więc odgrywać kluczowej roli w procesie decyzyjnym. Proponowane rozwiązania, zgodnie z najlepszymi praktykami, obejmują m.in: • Uzyskanie deklaracji dostawcy odnoszącej się do wszystkich kwestii istotnych z punktu widzenia zapewnienia bezpieczeństwa. Konkretna treść deklaracji powinna być ustalana pomiędzy przedsiębiorcą telekomunikacyjnym a dostawcą lub producentem w każdym indywidualnym przypadku. W propozycji uzupełnienia przepisu podany jest tylko przykładowy wykaz zawartości deklaracji wiarygodności danego dostawcy lub producenta; • Zapewnienie możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu. • Zapewnienie monitoringu bezpieczeństwa infrastruktury w celu ciągłego identyfikowania zagrożeń i zapobiegania im. Monitoring bezpieczeństwa infrastruktury powinien obejmować wszystkie krytyczne składniki infrastruktury telekomunikacyjnej, a w szczególności te składniki, które przekazują dane osobowe zewnętrznym kontrahentom, np. w związku z roamingiem. Powinny być przygotowane odpowiednie procedury monitoringu bezpieczeństwa.	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			• Zatrudnienie odpowiedniego personelu technicznego posiadającego stosowne kompetencje, z uwagi na postępowanie z krytycznymi składnikami infrastruktury i regularnie szkolonego.	
20.	**Art. 1 pkt 50** (dot. art. 66a ust. 10, pkt 1)	KIGEiT	**W art. 1 pkt 50 w art. 66a ust. 10 do punktu 1 dodaje się zdanie w następującym brzmieniu:** „*oraz przedstawiciele operatora strategicznej sieci bezpieczeństwa, który nabywa lub posiada produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie*” Alternatywnie – w razie brak uwzględnienia uwagi zawartej w pkt 12 w zakresie odniesienia decyzji wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB: „*oraz przedstawiciele podmiotów wskazanych w pkt 66a pkt 1) – 4), które nabywają lub posiadają produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub stowarzyszenia zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie*” **Uzasadnienie:** Proces analizy ma charakter krytyczny dla postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Opinia Kolegium stanowi faktyczną podstawę merytoryczną dla wydania decyzji przez właściwy organ. Zasadne jest, by w jej przygotowaniu wzięli udział nie tylko członkowie Kolegium, będącego – z definicji – organem politycznym, ale także podmioty działające na rynku, posiadające odpowiednie doświadczenie merytoryczne i znajomość uwarunkowań rynkowych oraz posiadające szeroką wiedzę w obszarze cyberzagrożeń. Z tego względu proponuje się rozszerzyć katalog podmiotów uczestniczących w procesie o przedstawicieli podmiotu lub podmiotów potencjalnie dotkniętych decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka, jak również właściwe izby gospodarcze lub stowarzyszenia o podobnym profilu. Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma specyficzny charakter i wywiera dalekosiężne skutki. Zasadne jest więc także uwzględnienie w składzie zespołu pracującego nad opinią, także samego dostawcy, którego postępowanie dotyczy. Umożliwi to bieżące udzielanie wyjaśnień, przedstawianie dokumentów czy dodatkowych informacji. Udział dostawcy umożliwi mu bieżącą korektę w obszarach wiążących się z ryzykiem zakwestionowania oraz przygotowanie się z wyprzedzaniem na ewentualną konieczność podjęcia kroków naprawczych (w razie wydania decyzji o uznaniu za dostawcę wysokiego ryzyka). Propozycja skorelowana z propozycją zawartą w pkt 9 powyżej.	
21.	**Art. 1 pkt 50** (dot. art. 66a ust. 10, pkt. 5)	KIGEiT	**W art. 1 pkt 50 w art. 66a ust. 10 punkt 5 otrzymuje następujące brzmienie:** „*uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji oraz dostawcy sprzętu i oprogramowania, którego dotyczy ta opinia”* **Uzasadnienie:** O treści opinii powinien być poinformowany ten, kogo dotyczy ta opinia, czyli dostawca sprzętu lub oprogramowania, którego dotyczy postępowanie. Zmiana skorelowana jest z propozycjami odnoszącymi się do zwiększenia udziału dostawcy w postępowaniu, w tym w procesie sporządzania opinii, a także z postulatem zwiększenia przejrzystości postępowania w stosunku do dostawcy, którego ono dotyczy.	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Przekazanie uzgodnionej opinii dostawcy pozwoli mu z wyprzedzeniem poczynić przygotowania do opracowania planu naprawczego lub innych działań niwelujących zidentyfikowane cyberzagrożenia.	
22.	**Art. 1 pkt 50** (dot. art. 66a, ust. 10)	KIGEiT	**W art. 1 pkt 50 w art. 66a po ust. 10 dodaje się ust. 10a-10f w następującym brzmieniu:** *10a. W ciągu miesiąca od otrzymania opinii Kolegium, dostawca sprzętu lub oprogramowania, którego dotyczy ta opinia, może przedstawić środki naprawcze i plan naprawczy.* *10b. Środki naprawcze powinny wskazywać sposób usunięcia sformułowanych w opinii Kolegium zagrożeń dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.* *10c. Plan naprawczy powinien przedstawiać harmonogram realizacji poszczególnych środków naprawczych.* *10d. W przypadku zaakceptowania środków naprawczych i planu naprawczego, Kolegium zmienia ocenę.* *10e. Do czasu zakończenia postępowania w sprawie zaakceptowania środków naprawczych i planu naprawczego, minister właściwy do spraw informatyzacji nie wydaje decyzji o której mowa w art. 66a ust. 11* **Uzasadnienie:** Przepisy Projektu w obecnej wersji nie przewidują żadnych postanowień, które dawałyby możliwość podjęcia właściwych środków naprawczych przez dostawcę sprzętu lub oprogramowania, którego dotyczy postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Zważywszy na daleko idące skutki decyzji – zarówno dla dostawcy, jak i dla jego klientów zobowiązanych do zaprzestania użytkowania rozwiązań objętych decyzją – decyzja powinna stanowić *ultima ratio*, czyli być podejmowana dopiero wtedy, gdy inne, mniej dotkliwe, ale możliwe środki naprawcze okazały bezskuteczne. Wprowadzenie omawianych tu rozwiązań mogłoby zapobiec wydaniu decyzji na podstawie ust. 11, a więc byłoby rozwiązaniem względniejszym zarówno dla dostawców, jak i podmiotów nabywających sprzęt lub oprogramowanie dostawcy, zwłaszcza dla dostawcy i dla operatorów. Biorąc pod uwagę fakt, że wydanie decyzji, na podstawie projektowanego art. 66a ust. 11 będzie stanowić przejaw dużego ograniczenia (o ile nie zupełnego wyłączenia) swobody działalności gospodarczej, to wprowadzenie rozwiązań mniej uciążliwych należy uznać za konieczne w kontekście art. 31 ust. 3 Konstytucji i wywodzonej z tego zasady proporcjonalności. Prawodawca powinien dążyć do wprowadzenia regulacji, które w jak najmniejszym stopniu ograniczą konstytucyjne wolności i prawa jednostek, a doprowadzą do ochrony tych samych wartości (tu: bezpieczeństwo państwa). Proponowane rozwiązanie jest zbliżone do rozwiązań funkcjonujących w innych państwach członkowskich UE (przykładowo – § 244a fińskiej ustawy o usługach łączności elektronicznej).	
23.	**Art. 1 pkt 50** (dot. art. 66a ust. 11)	KIGEiT	**W art. 1 pkt 50 dodany art. 66a ust. 11 otrzymuje następujące brzmienie:** *„11. Minister właściwy do spraw informatyzacji, w drodze decyzji na okres nie dłuższy niż 24 miesiące, po wcześniejszym jej zaakceptowaniu przez ministra właściwego do spraw rozwoju i technologii, ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw obrony narodowej, ministra właściwego do spraw sprawiedliwości oraz wyrażenia pozytywnej opinii przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów, uznaje dostawcę sprzętu lub oprogramowania o funkcjach krytycznych, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi”.* **Uzasadnienie:**	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Proponowane zmiany odnoszą się do dwóch zagadnień – poszerzenia kręgu podmiotów uczestniczących w wydaniu decyzji o uznaniu za dostawcę wysokiego ryzyka oraz określeniu okresu obowiązywania tej decyzji. W obecnym kształcie decyzja jest podejmowana jednoosobowo przez ministra właściwego do spraw informatyzacji. Z uwagi na wpływ tej decyzji na stosunki międzynarodowe z innymi państwami czy bezpieczeństwo wewnętrzne oraz skomplikowany charakter prawny, powinny uczestniczyć w jej podejmowaniu także inni ministrowie odpowiedzialni za obszary istotne z perspektywy chronionych wartości (obronność, bezpieczeństwo i porządek publiczny, zdrowie i życie ludzi) lub za obszary właściwe merytorycznie z perspektywy sektora, którego dotyczy decyzja (rozwój i technologia). Będzie to zgodne z analogicznymi rozwiązaniami funkcjonującymi w innych krajach UE. Przykładowo decyzja taka w Niemczech jest podejmowana przy udziale federalnego ministerstwa spraw wewnętrznych, zagranicznych i gospodarki[5]. Pozytywną opinię powinien wyrazić także Prezes Urzędu Ochrony Konkurencji i Konsumentów. Decyzja w sprawie uznania za dostawcę wysokiego ryzyka może bowiem, poprzez ograniczenie możliwości oferowania określonych produktów lub usług przez tego dostawcę, wpływać istotnie na konkurencję na rynku oraz korzystanie z usług przez użytkowników. Konsekwencją takiego – częściowego lub całkowitego – wykluczenia z rynku dostawcy czy dostawców, może być wzrost cen infrastruktury telekomunikacyjnej, a w konsekwencji wzrost cen świadczonych dla indywidulanych klientów usług telekomunikacyjnych. Wyłączenie możliwości prowadzenia działalności gospodarczej danego rodzaju (a do tego sprowadzałoby się dla dostawcy wydanie decyzji na podstawie projektowanego art. 66a ust. 11), nie może być przy tym w demokratycznym państwie prawnym bezterminowe. Regulacja powinna w szczególności uwzględniać wpływ bardzo szybkiego rozwoju technologicznego i dynamicznych zmian w zakresie zagrożeń związanych z cyberbezpieczeństwem na aktualność decyzji. Z tego względu w naszej ocenie regulacja powinna wymuszać przegląd aktualnych uwarunkowań, i stosownie do przypadku – dokonanie zmian w wydanej decyzji, wydanie nowej decyzji albo uznanie, że nie zachodzi już potrzeba wydawania w omawianym zakresie kolejnej decyzji. Uregulowania takie występują w innych krajach UE, np. w Austrii.	
24.	**Art. 1 pkt 50** (dot. art. art. 66a, ust. 11)	KIGEiT	**W art. 1 pkt 50 w art. 66a po ust. 11 dodaje się ust. 11a-11f w następującym brzmieniu:** *11a. Decyzja, o której mowa w art. 66a ust. 11, powinna wskazywać sposób usunięcia cyberzagrożeń których usunięcie przez dostawcę sprzętu i oprogramowania, spowoduje uchylenie decyzji przez ministra właściwego do spraw informatyzacji.* *11b. W ciągu miesiąca od dnia otrzymania lub ogłoszenia decyzji ministra właściwego do spraw informatyzacji, o której mowa w art. 66a ust. 11, dostawca sprzętu lub oprogramowania, którego dotyczy ta decyzja, powinien przedstawić środki naprawcze i plan naprawczy.* *11c. Środki naprawcze powinny wskazywać sposób usunięcia sformułowanych w decyzji ministra właściwego do spraw informatyzacji zagrożeń dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.* *11d. Plan naprawczy powinien przedstawiać harmonogram realizacji poszczególnych środków naprawczych.*	

[5] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, Dziennik Nr 25 z 27.05.2021, s. 1122, https://www.bundesanzeiger-verlag.de/

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			10e. W przypadku zaakceptowania środków naprawczych i planu naprawczego, minister właściwy do spraw informatyzacji uchyla decyzję. *11f. Do czasu zakończenia postępowania w sprawie zaakceptowania środków naprawczych i planu naprawczego, minister właściwy do spraw informatyzacji wstrzymuje wykonanie decyzji".* **Uzasadnienie:** W uzupełnieniu propozycji zawartej w pkt 28, proponuje się umożliwienie dostawcy przedstawienie planu naprawczego i środków naprawczych także po wydaniu decyzji. Nie zawsze bowiem przebieg analizy po stronie Kolegium i jego Opinia będą na tyle jasne, by już na etapie sporządzenia opinii możliwe lub zasadne było opracowywanie takich materiałów. Z kolei zaproponowanie po wydaniu decyzji rozwiązań sanacyjnych, podlegających ocenie organu, najpełniej pozwoli urzeczywistnić cel regulacji, jakim jest usuwanie cyberzagrożeń i stałe zwiększanie poziomu bezpieczeństwa państwa, w tym w związku z korzystaniem z dostawców, których rozwiązania ICT wiążą się ze zidentyfikowanymi w postępowaniu ryzykami. Proponowana zmiana zapewnia także, że organ wydając decyzję, będzie wskazywał konkretne uchybienia i konkretne oczekiwania względem dostawcy wysokiego ryzyka. Z jednej strony przyczyni się to do polepszania jakości wydawanych rozstrzygnięć i skłoni organ do opracowania uzasadnienia decyzji dokładnie i precyzyjnie, z drugiej – wzmocni oparty na zaufaniu dialog pomiędzy organem a dostawcą, nakierowany na osiągnięcie celu w postaci minimalizacji ryzyk cybernetycznych.	
25.	**Art. 1 pkt 50** (dot. art. 66a, ust. 12)	KIGEiT	**W art. 1 pkt 50 dodany art. 66a ust. 12 otrzymuje następujące brzmienie:** *„12. Decyzja, o której mowa w ust. 11, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT o funkcjach krytycznych pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka".* **Uzasadnienie:** Wyłączna zmiana w przepisie art. 66a ust. 12, polega na dodaniu po słowach „*konkretnych procesów ICT*" słów „*o funkcjach krytycznych*". Zmiana ta powodowana jest koniecznością zapewnienia spójności z pozostałymi propozycjami i jest skorelowana ze zmianami proponowanymi w pkt 10 powyżej.	
26.	**Art. 1 pkt 50** (dot. art. 66a ust. 14)	KIGEiT	**W art. 1 pkt 50 w art. 66a skreśla się ust. 14** **Uzasadnienie:** Projekt przewiduje aktualnie, że decyzja o uznaniu za dostawcę wysokiego ryzyka podlega natychmiastowemu wykonaniu. Natychmiastowa wykonalność decyzji – jako zasada, nie zaś wyjątek – może ograniczać prawa strony do sprawiedliwego i rzetelnego procesu i stać w sprzeczności z założeniami KPA. Zgodnie z przepisami KPA, rygor natychmiastowej wykonalności może zostać nadany decyzji w przypadku, gdy jest to niezbędne ze względu na ochronę zdrowia lub życia ludzkiego albo dla zabezpieczenia gospodarstwa narodowego przed ciężkimi stratami bądź też ze względu na inny interes społeczny lub wyjątkowo ważny interes strony. W każdym jednak wypadku to na organie wydającym decyzję leży obowiązek wskazania – i wykazania występowania – przesłanek uzasadniających zastosowanie tego mechanizmu. Rygor natychmiastowej wykonalności decyzji uznającej dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (art. 66a ust. 11) przy jednoczesnym wyłączeniu możliwości wstrzymania wykonania zaskarżonej decyzji przez	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			sąd administracyjny (art. 66d ust. 3) praktycznie uniemożliwia jakiekolwiek ograniczanie negatywnych skutków decyzji dla dostawcy i brak możliwości kontroli w tym zakresie prawidłowości decyzji przez sąd. Rygor natychmiastowej wykonalności, w połączeniu z przewidzianym w Projekcie zakazem wstrzymania wykonalności decyzji w sprawie dostawcy wysokiego ryzyka (art. 66d ust. 3 Projektu), doprowadzi do natychmiastowego rozpoczęcia po stronie podmiotu lub podmiotów do tego zobowiązanych zgodnie z art. 66b procesu wycofywania sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Od momentu wydania takiej decyzji będzie musiał rozpocząć się proces usuwania sprzętu dostawcy już wykorzystywanego , a także – co następuje natychmiast – sprzęt od dostawcy nie będzie mógł być nabywany przez podmiot lub podmioty wskazane w ustawie. Dla zaistnienia i w wielu przypadkach skonsumowania takich skutków nie będzie miało znaczenia nawet późniejsze korzystne rozstrzygnięcie sądowe (skoro z uwagi na rygor natychmiastowego wykonania decyzji, sprzęt zostanie usunięty lub nie zostanie już zakupiony). Nadanie rygoru natychmiastowej wykonalności powinien więc następować każdorazowo po rozważeniu przesłanek ustawowych określonych w kpa, a postanowienie w tym zakresie powinno podlegać zaskarżeniu na zasadach ogólnych. W obecnej postaci – zwłaszcza wobec wyłączenia możliwości wstrzymania wykonalności decyzji przez sąd zgodnie z projektowanym art. 66d ust. 3 – środek ten może być sprzeczny z podstawowym – gwarantowanym konstytucyjnie i traktatowo – prawem do sprawiedliwego rozpatrzenia sprawy przez sąd (art. 45 ust. 1 w zw. z art. 31 ust. 3 Konstytucji, art. 47 w zw. z art. 52 ust. 1 i 3 Karty Praw Podstawowych UE i art. 6 w zw. z art. 13 Europejskiej Konwencji Praw Człowieka - EKPC). W tym zakresie rekomendowane jest zatem stosowanie zasad ogólnych wynikających z KPA.	
27.	**Art. 1 pkt 50** (dot. art. 66a, ust. 15)	KIGEiT	**W art. 1 pkt 50 dodany w art. 66a ust. 15 otrzymuje następujące brzmienie:** *„15. Od decyzji, o której mowa w ust. 11, przysługuje wniosek o ponowne rozpatrzenie sprawy”.* **Uzasadnienie:** Zasada dwuinstancyjności postępowania ma rangę konstytucyjną (art. 78 Konstytucji RP) i powtórzona została wyraźnie w art. 15 k.p.a. Jak wskazuje doktryna, regulacja wyłączenia dwuinstancyjności na rzecz ponownego rozpatrzenia sprawy to już samo w sobie ograniczenie zasady dwuinstancyjności postępowania[6]. Ustrojodawca przewiduje wprawdzie możliwość ustanawiania wyjątków od tej zasady, jednak w ślad za Trybunałem Konstytucyjnym[7], należy uznać, że „*z art. 78 zd. 1 Konstytucji można zatem wywieść skierowany do prawodawcy postulat takiego kształtowania procedury, aby w miarę możliwości przewidziane w niej było prawo wniesienia przez stronę środka zaskarżenia. Omawiany przepis ma charakter ogólny i zamieszczony został w rozdziale drugim Konstytucji, poświęconym wolnościom, prawom i obowiązkom człowieka i obywatela, w części normującej środki ochrony wolności i praw. Jak wynika z jego brzmienia ma on zastosowanie zarówno do postępowania sądowego, jak i administracyjnego*”. Uzasadnienie Projektu nie wyjaśnia, dlaczego prawa strony postępowania zostały ograniczone poprzez odebranie możliwości złożenia wniosku o ponowne rozpatrzenie sprawy. Należy więc dopuścić możliwość złożenia wniosku o ponowne rozpoznanie sprawy i w ten sposób umożliwić weryfikację - przez ten sam organ – prawidłowości podjętej przez niego decyzji.	

[6] A. Wróbel [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, Komentarz aktualizowany do Kodeksu postępowania administracyjnego, LEX/el. 2021, art. 15, teza 3.
[7] Wyrok Trybunału Konstytucyjnego z dnia 3 lipca 2002 r., sygn. SK 31/01.

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Jakkolwiek rozpatrzenie sprawy ponownie przez ten sam organ, nie stanowi pełnego urzeczywistnienia zasady dwuinstancyjności postępowania, to jednak jest przyjętym w polskim systemie prawnym rozwiązaniem zapewniającym dodatkową (auto)kontrolę prawidłowości decyzji. Zapewnienie możliwości tej weryfikacji pozwoli potencjalnie na samodzielną rewizję przez organ ewentualnych decyzji nieprawidłowych oraz wymusza ponowną analizę merytoryczna sprawy. Większe gwarancje co do prawidłowości merytorycznej decyzji mogą ograniczyć konieczność składania skargi do sądu administracyjnego i zapewnią wyższy poziom sprawiedliwości proceduralnej względem strony.	
28.	**Art. 1 pkt. 50** (dot. art. 66a ust. 14-15)	KIGEiT	Izba podtrzymuje uwagi złożone w piśmie z dn. 2 lutego 2021 r. (sygn. KIGEiT/365/02/2021) pkt 6.	
29.	**Art. 1 ust. 50** (dot. art. 66b)	KIGEiT	Izba podtrzymuje uwagi złożone w piśmie z dn. 2 lutego 2021 r. (sygn. KIGEiT/365/02/2021) pkt 2 - w zakresie obowiązku wycofania z użytkowania określonych w decyzji produktów, usług czy procesów.	
30.	**Art. 1 pkt 50** (dot. art. 66b ust.2)	KIGEiT	**W art. 1 pkt 50 dodany art. 66b ust. 2 otrzymuje następujące brzmienie:** *„2. Przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, wycofują w ciągu 7 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT o funkcjach krytycznych* Uwaga aktualna jedynie w przypadku braku akceptacji propozycji zawartej w pkt 12 dotyczącej ograniczenia decyzji o uznaniu za dostawcę wysokiego ryzyka wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB **Uzasadnienie:** Zmiana w przepisie art. 66b ust. 2, polega na dodaniu po słowach „*konkretne procesy ICT*” słów „*o funkcjach krytycznych*” i przedłużenia okresu wycofania sprzętu do 7 lat. Przepis art. 66b ust. 2 Projektu dotyczy określonej grupy przedsiębiorców telekomunikacyjnych, tj. tych, którzy obowiązani są posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. W uzasadnieniu Projektu wyjaśniono, że jest to grupa ok. 100 podmiotów, czyli znacząca. W tym do tej grupy zaliczają się najwięksi operatorzy telekomunikacyjni. Umowy z dostawcami zawierane są z reguły na długie okresy. Proces wymiany sprzętu będzie więc długotrwały zarówno z uwagi na ilość podmiotów jak i na poziomie indywidualnym, w odniesieniu do poszczególnych podmiotów, zmuszonych do przejrzenia infrastruktury, zaprojektowaniu niezbędnych zmian, przeprowadzenia postępowania zakupowego, wynegocjowania nowej umowy itd. Przedstawiona w załączniku nr 3 do ustawy lista funkcji jest bardzo obszerna. Decyzje odnoszące się do elementów infrastruktury tam wskazanych będą wymuszać bardzo istotne techniczne zmiany w sieci telekomunikacyjnej, wymagające technologicznego przeprojektowania całych sieci – a co za tym idzie, będą wiązać się z koniecznością alokowania w tym celu istotnych kosztów. Konieczność zapewnienia stabilności sieci będzie wymagał zaplanowania skomplikowanego i trudnego technicznie procesu, wymagającego zdecydowanie więcej czasu niż 5 lat. Z tego względu proponowany okres to 7 lat.	
31.	**Art. 1 pkt 50** (dot. art.66b ust.3)	KIGEiT	**W art. 1 pkt 50 dodany art. 66b ust. 3 skreśla się:**	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			„3. Podmioty, o których mowa w art. 66 ust. 1 pkt 1-4, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 i 1598), nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 11”. Uwaga aktualna jedynie w przypadku braku akceptacji propozycji zawartej w pkt 12 dotyczącej ograniczenia decyzji o uznaniu za dostawcę wysokiego ryzyka wyłącznie do sprzętu lub oprogramowania wykorzystywanego przez OSSB **Uzasadnienie:** Przepis art. 66b ust. 3 Projektu wprowadza przesłankę dodatkową wykluczenia wykonawcy z postępowania o udzielenie zamówienia, która w stosunku do przesłanek przewidzianych już w ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych, a wynikających z 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 2014/24/UE”) jest nadmiarowa. W sprawie projektowanej regulacji wypowiadał się także MSUE (zob. pismo: https://legislacja.gov.pl/docs//2/12337950/12716624/12716626/dokument487161.pdf), który wskazał, że projektodawca powinien przygotować się na przedstawienie uzasadnienia dopuszczalności tego przepisu w świetle przewidzianych w dyrektywie 2014/24/UE przesłanek pozwalających na wyłączenie jej stosowania, w tym przesłanki odnoszącej się do podstawowych interesów danego państwa członkowskiego w zakresie bezpieczeństwa. Polskie prawo zamówień publicznych stanowi transpozycję art. 57 dyrektywy 2014/24/UE, w którym określono precyzyjnie podstawy wykluczenia wykonawcy. Regulacje zawarte w Projekcie muszą być zgodne z dyrektywą 2014/24/UE, a wśród podstaw wykluczenia zawartych w dyrektywie brak jest podstawy wykluczenia sformułowanej w art. 66b ust. 3 Projektu. Minister ds. UE („MSUE”) zwrócił uwagę, że aktualne pozostaje zastrzeżenie, w myśl którego zgodnie z utrwalonym orzecznictwem Trybunału Sprawiedliwości UE wszelkie wyjątki od stosowania przepisów dyrektyw dotyczących zamówień publicznych podlegają wykładni zawężającej. Dotychczas nie przedstawiono argumentacji dotyczącej związku dokonywanych zakupów sprzętu, oprogramowania i usług ze sferą podstawowych interesów państwa w zakresie bezpieczeństwa. Powoduje to uzasadnione wątpliwości co do konieczności i prawidłowości wprowadzenia regulacji w art. 66b ust. 3 Projektu jako odstępstwa od postanowień dyrektywy 2014/24/UE.	
32.	**Art. 1 pkt 50** (dot. art. 66b ust.4)	KIGEiT	**W art. 1 pkt 50 dodaje się art. 66b ust. 4 w brzmieniu następującym:** *„3. Przepisów ust. 1-3 nie stosuje się, do nabywania i wprowadzania do użytkowania produktów, usług i procesów ICT o funkcjach krytycznych wskazanych w decyzji, o której mowa w art. 66a ust. 11, jeżeli jest to niezbędne do zachowania ciągłości utrzymania funkcjonowania sieci.”* **Uzasadnienie:** Dodanie przepisu art. 66b ust. 4 wynika z konieczności zapewnia ciągłości dostaw do bieżącego funkcjonowania operatorów telekomunikacyjnych i pozostałych podmiotów zobowiązanych stosować się do ograniczeń wynikających z decyzji o uznaniu za dostawcę wysokiego ryzyka. Decyzja o uznaniu za dostawcę wysokiego ryzyka nie powinna być przesłanką do zakończenia wsparcia eksploatacyjnego przez dostawcę tego sprzętu. Podmiotowi (lub podmiotom) zobowiązanym do wycofania z użytkowania określonego sprzętu należy zapewnić możliwość realizacji niezbędnych czynności zakupowych, wdrożeniowych i serwisowych odnoszących się do już	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			eksploatowanych produktów, usług lub procesów ICT oraz objętych zakresem decyzji. Brak możliwości realizacji szeroko rozumianych funkcji utrzymania infrastruktury będzie potencjalnie skutkował awariami (także fizycznymi) oraz trudnościami (lub nawet niemożliwością) usuwania luk lub podatności. W konsekwencji wzrośnie prawdopodobieństwo incydentów cyberbezpieczeństwa, w tym przerwanie ciągłości świadczenia usług przez podmiot (lub podmioty) zobowiązany do uwzględnienia skutków decyzji. Proponowana zmiana ma też uzasadnienie w istniejących – nierzadko długoterminowych – umowach z dostawcami, w ramach których zapewniane jest wsparcie dostawcy. Zakończenie korzystania z tych usług, zwłaszcza w trybie nagłym, będzie wymagać potencjalnie renegocjacji umowy lub nawet – ponoszenia przez podmiot lub podmioty zobowiązane do uwzględnienia skutków decyzji, dodatkowych kosztów związanych z wyjściem z zawartej umowy i poszukiwaniem rozwiązań alternatywnych – nie zawsze zresztą dostępnych. W przypadku braku możliwości uwzględnienia proponowanej zmiany w pełnym brzmieniu, proponujemy zachowanie możliwości nabywania produktów, usług i procesów ICT co najmniej przez okres odpowiadający okresowi wycofania ich z użytku zgodnie z ust. 1 pkt 2) oraz ust. 2) – ze wskazanych wyżej przyczyn związanych z koniecznością zapewnienia bezpieczeństwa eksploatacji wykorzystywanych rozwiązań.	
33.	**Art. 1 pkt 50** (dot. art. 66b ust. 5-6)	KIGEiT	**W art. 1 pkt 50 dodaje się art. 66b ust. 5-6 w brzmieniu następującym:** *„5. Podmiot lub podmioty, zobowiązane do wycofania z użytkowania sprzętu lub oprogramowania, na skutek wydania decyzji, o której mowa w art. 66a ust. 11, otrzymują odszkodowanie za koszty związane z wymianą tego sprzętu lub oprogramowania.* *6. Rekompensata jest obliczana na podstawie wydatków poniesionych na zakup sprzętu lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów wykazujących poniesione koszty”.* **Uzasadnienie:** Wprowadzenie obowiązku wycofania z użytku sprzętu lub oprogramowania objętego decyzją w sprawie uznania za dostawcę wysokiego ryzyka spowodowuje wysokie koszty dla podmiotu lub podmiotów zobowiązanych do wycofania z użytkowania zakwestionowanych rozwiązań ICT. Koszty te nie będą w żaden sposób zawinione przez te podmioty, a wynikać będą z regulacji o szczególnym charakterze – z założenia mających zastosowanie w sytuacjach wyjątkowych. Zaproponowane regulacje w praktyce oznaczają, że podmioty zobowiązane (w zależności od przyjętej koncepcji – OSSB lub wszystkie podmioty wymienione w aktualnie projektowanym art. 66a ust 1 pkt 1-4) muszą pozbyć się sprzętu lub oprogramowania, które potencjalnie mogłoby być eksploatowane jeszcze przez długi czas – gdyby nie wprowadzono określonych regulacji. Z tego względu uzasadnione jest zdefiniowanie w przepisach rozsądnej rekompensaty dla podmiotów ponoszących tego rodzaju koszty. Warto wskazać przy tym, że podobne rozwiązania wprowadzone zostały m.in. w Finlandii. Propozycja zakłada rekompensatę pochodzącą z budżetu Skarbu Państwa – Prezesa UKE. Z uwagi jednak na fakt, że rekompensata ma związek ze szczególnymi działaniami państwa, związanymi z kluczowymi aspektami bezpieczeństwa, propozycja ogranicza się przy tym do pokrycia wydatków poniesionych na zakup wymienianego sprzętu, bez uwzględnienia innych kosztów związanych z wydaną decyzją (np. przeprowadzenie procesu zakupowego,	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			przeprojektowanie infrastruktury itd.). Z tego względu uważamy, że propozycja jest rozsądna i do pewnego stopnia ma szansę zniwelować negatywne konsekwencje ponoszone przez podmioty, zobowiązane do stosowania się do decyzji.	
34.	**Art. 1 pkt 50** (dot. art. 66d ust. 1-2)	KIGEiT	**W art. 1 pkt 50 postanowienia art. 66d ust. 1-2 otrzymują brzmienie następujące:** *„1. Sąd administracyjny rozpatruje skargę na decyzje, o których mowa w art. 66a ust. 11, na posiedzeniu jawnym.* *2. Odpis sentencji wyroku z uzasadnieniem doręcza się ministrowi właściwemu do spraw informatyzacji oraz skarżącemu."* **Uzasadnienie:** W zaproponowanej w Projekcie postaci, przepis art. 66d stanowi odstępstwo od kardynalnych zasad nie tylko procedury administracyjnej (art. 10 oraz art. 142 ustawy p.p.s.a.), ale każdego rzetelnego postępowania, w postaci jego jawności, ustności, prawa do skutecznego wniesienia środka zaskarżenia i generalnie prawa do obrony. Zainteresowany podmiot nie będzie mógł bronić swoich praw, skoro skarga będzie rozpoznawana na posiedzeniu niejawnym i nie będzie on mógł zapoznać się z pełnym uzasadnieniem wyroku. W ten sposób postępowanie to będzie spełniało cechy procesu inkwizycyjnego. Wbrew twierdzeniom w uzasadnieniu Projektu, że strona i tak będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym, czyli nie powinno ucierpieć jej prawo do obrony, nie będzie jednak miała dostępu do dowodów i materiałów postępowania, skoro niejawne będzie posiedzenie i uzasadnienie wyroku. W sposób więc oczywisty jej prawa w tym postępowaniu zostaną ograniczone. Przyjęta w Projekcie konstrukcja w praktyce będzie wyłączać skuteczną obronę oraz możliwość wnoszenia środków odwoławczych do sądu wyższej instancji w celu weryfikacji rozstrzygnięcia sądu pierwszej instancji. Strona nie będzie bowiem posiadała pełnej wiedzy na temat powodów takiego a nie innego rozstrzygnięcia – w szczególności występuje wysokie ryzyko odmowy stronie dostępu do kluczowych elementów ustalonego stanu faktycznego. Wskazujemy, że na wady prawne art. 66d wskazywała także Rada Legislacyjna już w opinii do projektu z dnia 23 lutego 2021 r. W szczególności Rada Legislacyjna podniosła wątpliwość, czy w ogóle jest zgodne z Konstytucją RP odstępowanie od doręczania stronie pełnego uzasadnienia wyroku sądu administracyjnego (art. 66d ust. 2). Według Rady, zasadą musi być dostarczanie stronie pełnego uzasadnienia faktycznego decyzji administracyjnej, tak aby strona (będąca adresatem decyzji) mogła w sposób skuteczny – w oparciu o pełną znajomość relewantnych prawnie faktów, które wpłynęły na treść decyzji – zaskarżyć tę decyzję do sądu administracyjnego. Podobnie też wyrok sądu administracyjnego musi w świetle konstytucyjnego prawa do sądu zawierać pełne uzasadnienie doręczane stronie, gdyż w oparciu o to uzasadnienie strona może skutecznie wykorzystać swoje uprawnienia do zaskarżenia tego wyroku na drodze sądowej (w omawianym przypadku: zwłaszcza skargą kasacyjną do Naczelnego Sądu Administracyjnego), a ponadto jest to konieczne dla pogłębiania zaufania obywateli do państwa i stosowanego prawa (art. 2 Konstytucji RP). Wreszcie także w tym obszarze pojawiają się duże wątpliwości co do proporcjonalności proponowanego rozwiązania – z uwagi na niezwykle szerokie ograniczenia praw strony. Przyjęcie w obecnej postaci w Projekcie postanowień art. 66d ust. 1-2 rodzi poważne ryzyko uznania tych przepisów za sprzecznie z Konstytucją RP.	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
35.	**Art. 1 pkt. 50** (dot. art. 66d ust. 1-3)	KIGEiT	Izba podtrzymuje uwagi złożone w piśmie z dn. 2 lutego 2021 r. (sygn. KIGEiT/365/02/2021) pkt 6.	
36.	**Art. 1 pkt 50** (dot. art. 66d, ust.3)	KIGEiT	**W art. 1 pkt 50 postanowienia art. 66d skreśla się ust. 3** **Uzasadnienie:** Przepis, którego dotyczy niniejszy punkt, wyłącza możliwość wstrzymania wykonalności zaskarżonej decyzji przez sąd. Uzasadnienie Projektu nie zawiera szczegółowego wyjaśnienia, poza ogólnym powołaniem się na szczególne interesy bezpieczeństwa państwa, przyczyny zrezygnowania z jednej z zasad ogólnych odnoszących się do wstrzymania wykonalności decyzji. Art. 61 ust. 3 p.p.s.a. reguluje instytucję tzw. ochrony tymczasowej w postępowaniu sądowo-administracyjnym. Celem przewidzianej w art. 61 § 3 p.p.s.a. ochrony tymczasowej jest uchronienie strony skarżącej przed skutkami wykonania zakwestionowanego aktu, które mogą być trudne do odwrócenia, po ewentualnym jego uchyleniu przez sąd (por. postanowienie Wojewódzkiego Sądu Administracyjnego („WSA") w Poznaniu z 25 czerwca 2019 r. sygn. akt IV SA/Po 425/19). Wstrzymanie wykonania zaskarżonej decyzji jest dodatkowym, obok skargi, środkiem ochrony przysługującym skarżącemu. Wyłączenie możliwości wstrzymania przez sąd wykonania decyzji stanowi wyjątek od zasady ogólnej wynikającej z art. 61 § 3 ustawy prawo o postępowaniu przed sądami administracyjnymi („p.p.s.a.")[8], który dotychczas w polskim prawie był stosowany niezwykle rzadko. Ustawowe wyjątki od zasady istnienia możliwości wstrzymania wykonania decyzji powinny być przy tym wprowadzane z najwyższą ostrożnością. Trafny jest pogląd Naczelnego Sądu Administracyjnego („NSA"), zwracający uwagę na konieczność zachowania „*daleko idącej ostrożności*" przy wykonywaniu decyzji ostatecznych przed upływem terminu do ich zaskarżenia, co może doprowadzić do powstania stanów nieodwracalnych[9]. Instytucja wstrzymania decyzji jest stosowana od dawna także w UE. Celem ochrony tymczasowej jest zapewnienie możliwości wstrzymania decyzji, jeżeli zachodzi niebezpieczeństwo wyrządzenia znacznej szkody lub spowodowania trudnych do odwrócenia skutków. Dokładnie taka sytuacja może nastąpić w następstwie zastosowania rozwiązań proponowanych w Projekcie, tj. w następstwie wydania decyzji mogą powstać już nieodwracalne konsekwencje dla podmiotu, którego dotyczyć będzie taka decyzja. Badanie przesłanek wstrzymania wykonania decyzji powinno odbywać się w odniesieniu do konkretnej sprawy – to niezawisły sąd bada, czy w świetle indywidualnych okoliczności nad interesami strony przeważa ochrona interesu bezpieczeństwa państwa. Dokonywanie takiej oceny przez ustawodawcę w sposób generalny na etapie projektu ustawy będzie pozbawiać stronę możliwości ochrony jej praw i skutkować pozornością ochrony sądowej. Z tego względu wskazany przepis należy usunąć z Projektu; zastosowanie powinny znaleźć zaś zasady ogólne wynikające z p.p.s.a.	
37.	**Art. 1 pkt 50** (dot. art. 66f)		**W art. 1 pkt 50 dodaje się art. 66f w brzmieniu następującym:**	

[8] Dz. U. z 2002 r., Nr 153, poz. 1270 ze zm.
[9] Zob. T. Woś red., *Prawo o postępowaniu przed sądami administracyjnymi,* Komentarz do art. 61, LEX 2016 i przywołane tam orzecznictwo.

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			„Prezes UKE ustala z odpowiednim CSRIT oraz przedsiębiorcami komunikacji elektronicznej świadczącymi usługi publicznej sieci telekomunikacyjnej oraz ich stowarzyszeniami, producentami i dostawcami infrastruktury telekomunikacyjnej oraz ich stowarzyszeniami, z uwzględnieniem stanowisk ENISA oraz wytycznych wydawanych przez inne właściwe organy Unii Europejskiej, wykaz funkcji oraz komponentów krytycznych dla bezpieczeństwa sieci i usług, i publikuje go na swojej stronie internetowej”, **Uzasadnienie:** Istotną częścią systemu zapewnienia bezpieczeństwa jest identyfikacja krytycznych obszarów architektury sieciowej. W przypadku bowiem tych elementów infrastruktury należy zastosować wyższy poziom bezpieczeństwa. Składniki są krytyczne w szczególności wtedy, gdy techniczne nieprawidłowości prowadzić mogą do istotnych naruszeń bezpieczeństwa lub naruszeń ochrony danych w znacznym stopniu. Krytyczność danego składnia jest uzasadniona przez te jego funkcje, które mogą doprowadzić do nieprawidłowości technicznych w przypadku awarii. Lista zawarta w załączniku nr 3 („Kategorie funkcji krytycznych dla bezpieczeństwa sieci i usług”) ma więc kluczowe znaczenie – zarówno z perspektywy wymogu wycofania z użytku produktów / usług / procesów przez przedsiębiorców telekomunikacyjnych (obecne brzmienie projektu – art. 66b ust. 2), jak i dla ustalenia zakresu dopuszczalnego zakresu postępowania w sprawie uznania za dostawcę wysokiego ryzyka (por. pkt 5). Zważywszy na wagę tej listy – ale również mając na uwadze dynamicznie zmieniające się okoliczności, zarówno technologiczne jak i podmiotowe – zasadne jest, by nie stanowiła ona załącznika do ustawy. Takie ujęcie uniemożliwia bowiem jej sprawną zmianę w przypadku zmieniających się okoliczności, a de facto uzależnia możliwości stosowanego dostosowania wykazu funkcji krytycznych od możliwości uzyskania porozumienia politycznego umożliwiającego zmianę ustawy. W praktyce innych państw europejskich, analogiczne listy są tworzone przez – lub przy udziale – regulatora rynku telekomunikacyjnego. Zapewniana jest też współpraca z organami odpowiedzialnymi za bezpieczeństwo oraz konsultacje z uczestnikami rynku oraz aktorów społecznych. Lista podlega aktualizacji w zależności od zmieniających się okoliczności. Ponadto zapewniony jest wówczas udział podmiotów, posiadających szeroką wiedzę i doświadczenie, co umożliwia stworzenie wykazu racjonalnego, adresującego cyberzagrożenia a jednocześnie zapewniającego stabilizację rynku rozwiązań ICT. Tytułem przykładu podobne rozwiązania funkcjonują w innych państwach europejskich: **a)** W Finlandii, proces identyfikacji funkcji krytycznych odbywa się przez pryzmat podstawowych funkcji sieciowych opartych o standardy ETSI i specyfikacje techniczne 3GPP, zdefiniowane przez regulatora. Ocena ryzyka dla bezpieczeństwa sieci skupia się na konkretnym sprzęcie stanowiącym element infrastruktury krytycznej, zaś regulator wspierany jest w procesie decyzyjnym przez dedykowane ciało doradcze., składające się z przedstawicieli organów rządowych, operatorów telekomunikacyjnych, głównych dostawców sprzętu i innych interesariuszy **b)** W Austrii środki bezpieczeństwa opracowane w tym kraju mają zastosowanie do produktów bezpośrednio zidentyfikowanych jako komponenty krytyczne w sieci 5G zgodnie z załącznikiem do rozporządzenia dotyczącym bezpieczeństwa sieci wydanego przez austriacki organ regulacyjny Rundfunk und Telekom Regulierungs-GmbH	

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			(RTR-GmbH)[10]. Jednocześnie każdy z operatorów sieci telekomunikacyjnych działających w technologii 5G w Austrii został zobowiązany do regularnego przedkładania deklaracji wiarygodności dotyczącej spełnienia wymogów bezpieczeństwa sieci określonych w załączniku nr 1 do przedmiotowego rozporządzenia.[11] Podobnie jak w przypadku Finlandii, rozwiązanie wdrożone w Austrii odwołuje się do międzynarodowych standardów technicznych 3GPP. Wreszcie uznaniowość zaproponowanego wykazu nie wzmacnia zaufania uczestników rynku – w tym uczestników krajowego systemu cyberbezpieczeństwa – do państwa i jego organów. Z niniejszym punktem skorelowany jest pkt 45 przewidujący usunięcie załącznika nr 3 z ustawy. W przypadku bowiem przyjęcia w zaproponowanym brzmieniu art. 66f, załącznik ten będzie zbędny; wykaz kategorii funkcji krytycznych będzie bowiem ustalany w trybie art. 66f.	
38.	**Art. 1 pkt 50**		**W przypadku nieuwzględnienia propozycji zawartych w pkt 37 i 45, proponujemy usunięcie z listy stanowiącej Załącznik nr 3 do Projektu postanowienia dotyczącego RAN w brzemieniu następującym:** *„3. Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych."* **Uzasadnienie:** Jak wskazano wyżej, aktualna lista wydaje się być przygotowana weryfikacji technicznej i rynkowej. Brak zapewnienia udziału podmiotów rynkowej w jej tworzeniu powoduje poważne wątpliwości co do jej zawartości zaproponowanej w załączniku nr 3 do Projektu. W Załączniku nr 3 do Projektu wymieniona jest usługa obejmująca *Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych (*RAN – *Radio Access Network).* Zgodnie jednak z modelem 3GPP (raport ETSI TR 121 915 V.15.0.0. (2019-10), s. 41) funkcje takie jak UDM (*Unified Data Management*), tj. zarządzanie subskrypcją, dane użytkownika, rejestracja i zarządzanie mobilnością oraz ARPF (*Authentication Credential Repository and Processing Function*), tj. przechowanie danych uwierzytelniających, są elementami architektury sieciowej wymagającymi większego poziomu ochrony niż stacje bazowe. Wspomniany raport ETSI został przywołany w § 3 ust. 1 rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych, jako wytyczna dla rozumienia pojęcia „sieci 5G" („*Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) (...)*"). Idąc za wskazanym w Raporcie sposobem rozumienia sieci 5G, należy również konsekwentnie przyjąć podział na elementy krytyczne sieci 5G (takie jak UDM, ARPF) i pozostałe, niekrytyczne elementy sieci 5G, do których należy radiowa sieć dostępowa. Podejście przedstawione w Raporcie ETSI zostało również przyjęte w dokumentach Unii Europejskiej (*Raport on EU Coordinated Risk Assessment for 5G*, s. 16 i 17 i Toolbox, s. 39 i 40), z których również wynika, iż RAN nie stanowi krytycznego elementu sieci. Analogiczne podejście, czyli wyłączenie funkcji dostępowych z kategorii krytycznych elementów sieci 5G, przyjął Rząd polski w lipcu 2019 r. w swoim stanowisku, przygotowanym dla potrzeb stworzenia dokumentu *Raport on EU*	

[10] Załącznik nr 2 do rozporządzenie RTR nr 301: Telekom-Netzsicherheitsverordnung 2020 – TK-NSiV 2020, wydanego zgodnie z § 6 ust. 4, https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/Telekom-Netzsicherheitsverordnung_2020_TK-NSiV_2020.de.html.
[11] Załącznik nr 1 do Rozporządzenia – TK-NSiV.

Lp.	Jednostka redakcyjna	Podmiot zgłaszający uwagę	Treść uwagi	Stanowisko projektodawcy
			Coordinated Risk Assessment for 5G (*Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings*, s. 7). Z uwagi na powyższe, zasadne jest usunięcie z listy zawartej w załączniku nr 3, pozycji odnoszącej się do RAN.	
39.	**Art. 1 pkt. 53** (dot. art. 73 ust 2a)	KIGEiT	Izba podtrzymuje uwagi złożone w piśmie z dn. 2 lutego 2021 r. (sygn. KIGEiT/365/02/2021) w pkt 7.	
40.	**Art 1 pkt. 56** (dot. art. 76f)	KIGEiT	Sprzeczność pomiędzy art. 1 pkt 2 lit. c ppkt 1 stanowiącym, że do przedsiębiorców telekomunikacyjnych nie stosuje się przepisów ustawy o KSC, z wyjątkiem działu II, art. 66a-66c, art. 67a i 67b oraz art. 73 i 74 oraz art. 76f nakładającym na przedsiębiorcę telekomunikacyjnego obowiązek kolokacji oraz udostępniania.	
41.	**Art. 1 pkt. 56** (dot. art. 76j)	KIGEiT	Stwierdzenie, że w zakresie nieuregulowanym w ustanie do OSSB stosuje się przepisy Pt wymaga sprecyzowania. Nie ulega wątpliwości, że do OSSB mają zastosowania wszystkie przepisy Pt, których materia nie została uregulowana przez UKSC, ponieważ jest on przedsiębiorcą telekomunikacyjnym, czemu zatem ma służyć art. 76j?	
42.	**Art. 1 pkt. 56** (dot. art. 76c ust. 1)	KIGEiT	Błędne odwołanie do ust. 1.	
43.	**Art. 1 pkt. 56** (dot. art. 76p)	KIGEiT	Zasady dotyczące przeprowadzania postępowań selekcyjnych zostały kompleksowo uregulowane w Rozdziale 1 Działu IV ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.	
44.	**Art. 1 pkt. 56** (dot. art. 76k ust. 1)	KIGEiT	Błędne odwołanie do art. 76a ust. 3 zamiast art. 76b	
45.	**Art. 1 pkt 61**		**W art. 1 pkt 61 skreśla się pkt 61) (Załącznik nr 3).** **Uzasadnienie:** Zmiana skorelowana jest z pkt 37 określającym proponowany tryb określania funkcji krytycznych.	