WNIOSEK O DODATKOWE KONSULTACJE W SPRAWIE PROJEKTU USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA (UD68)

Warszawa, 12 października 2022 roku

Sz. P.

Mateusz Morawiecki

Prezes Rady Ministrów, Minister Cyfryzacji
Al. Ujazdowskie 1/3
00-001 Warszawa

WNIOSEK O DODATKOWE KONSULTACJE
W SPRAWIE PROJEKTU USTAWY
O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA (UD68)

Szanowny Panie Premierze,

w związku z opublikowaniem w dniu 05 października 2022 roku w biuletynie informacji publicznej Ministra Cyfryzacji projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (UD68) (dalej „**Nowelizacja KSC**"), jako organizacja działająca na rzecz małych i średnich przedsiębiorstw (dalej „**MŚP**"), zwracamy się do Pana Premiera z wnioskiem o:

- niezwłoczne przeprowadzenie dodatkowych konsultacji publicznych oraz zorganizowanie konferencji uzgodnieniowej z udziałem MŚP, które w szczególności objęłyby m.in. zmianę art. 66a ust.5 i włączenie MŚP w postepowanie w sprawie uznania za dostawcę wysokiego ryzyka;
- przeprowadzenie kampanii informacyjnej dedykowanej MŚP, której celem będzie przybliżenie przedsiębiorcom nowych obowiązków wynikających z nowelizacji KSC;
- wstrzymania prac nad dalszym procedowaniem Nowelizacji KSC do czasu przeprowadzenia konsultacji publicznych.

Poniżej przedstawiamy argumenty świadczące o tym, że przyjęcie Nowelizacji KSC w obecnym brzmieniu wpłynie negatywnie na tak kluczowy segment gospodarki polskiej jakim są MŚP.

- **Wyłączenie MŚP z postępowania w sprawie uznania za dostawcę wysokiego ryzyka – art. 66a ust. 5 Nowelizacji KSC**

Pragniemy zauważyć, że w obecnym brzmieniu Nowelizacji KSC zostało utrzymane brzmienie art. 66a ust. 5 które zakłada, że do postępowania o uznanie za dostawcę wysokiego ryzyka mogą dołączyć tylko ci przedsiębiorcy, którzy w poprzednim roku osiągnęli przychody większe niż 113 mln zł za 2021 rok (20.000 krotność przeciętnego wynagrodzenia w gospodarce narodowej w roku ubiegłym). Wielokrotnie przedsiębiorcy z sektora MŚP wskazywali, że taki zapis w rezultacie wyklucza ich możliwość udziału w postępowaniu, pomimo faktu, że ewentualne decyzje w postepowaniu będą mieć bezpośredni wpływ na MŚP.

Należy wskazać, że decyzja o uznaniu danego dostawy za dostawcę wysokiego ryzyka i związane z taką decyzją konsekwencje dotkną najbardziej przedsiębiorców telekomunikacyjnych oraz dostawców sprzętu z segmentu MŚP. W przypadku wydania takiej decyzji, to właśnie ci przedsiębiorcy będą zobowiązani ponieść koszt wymiany sprzętu, a swoboda w działalności gospodarczej dystrybutorów sprzętu zostanie ograniczona (poprzez likwidację popytu na określone towary – zakaz wprowadzania tych towarów do użytkowania). Niewątpliwie wynik postępowania w sprawie uznania za dostawcę wysokiego ryzyka będzie bezpośrednio wpływać na prawa i obowiązki przedsiębiorców z sektora MŚP, zatem powinni oni mieć prawo czynnego udziału w takim postępowaniu.

Pragniemy przypomnieć, że już w liście Prezesa KIKE, Pana Karola Skupnia do Pana Premiera, który dotyczył wersji projektu nowelizacji KSC z dnia 15 marca 2022, Prezes KIKE wskazywał argumenty, dlaczego zmiana art. 66a ust.5 jest tak istotna dla segmentu MŚP – niestety ówczesne argumenty nie zostały uwzględnione w obecnym projekcie Nowelizacji KSC. **Dlatego raz jeszcze zwracamy się z prośbą o przeprowadzenie konsultacji oraz konferencji uzgodnieniowej z udziałem MŚP, w szczególności w zakresie omawianego przepisu i wypracowanie kompromisowego rozwiązania, które ochroni interesy sektora MŚP.**

- **Negatywne skutki finansowe dla sektora MŚP**

Wyłączenie możliwość korzystania z dostawców uznanych za dostawców wysokiego ryzyka przez przedsiębiorców będzie generowało dla nich dodatkowe koszty, zarówno koszty bezpośrednie związane z wymianą sprzętu w wyznaczonym okresie czasu, jak i koszty związane z koniecznością korzystania z droższego dostawcy. Należy zaznaczyć, że odebranie przedsiębiorcom możliwości skorzystania z podmiotu tańszego, który bazuje na równie bezpiecznej technologii co inni na rynku, ale ocenionego jako dostawcę wysokiego ryzyka redukuje możliwość szybkiego rozwoju mniejszym firmom i ogranicza ich konkurencyjność na rynku europejskim.

Dodatkowo, zauważamy, że do dzisiaj nie zostały przewidziane żadne realne wsparcie finansowe dla MŚP w związku z koniecznością dostosowania się do Nowelizacji KSC oraz do ewentualnych decyzji wydanych na jej podstawie. Należy zauważyć, że przedsiębiorcy z segmentu MŚP będą musieli ponieść koszty niewspółmiernie wyższe niż duzi przedsiębiorcy, w szczególności te związane z wymianą sprzętu.

- **Brak przygotowania sektora MŚP na Nowelizację KSC**

Nowelizacja KSC przewiduje nieproporcjonalne obciążenie MŚP obowiązkami w zakresie cyberbezpieczeństwa. Jako przykład należy wskazać przedsiębiorców komunikacji elektronicznej będących mikro-, małymi i średnimi przedsiębiorcami, którzy zostaną włączeni do krajowego systemu cyberbezpieczeństwa. Przedsiębiorcy będą musieli wypracować i wdrożyć wewnętrzne procedury w zakresie stosowania środków technicznych i organizacyjnych zapewniających bezpieczeństwo sieci, procedury w zakresie obsługi incydentów telekomunikacyjnych oraz będą musieli wypracować kanały komunikacji z CSIRT Telco oraz z właściwym CSIRT poziomu krajowego.

Należy zauważyć, że poziom świadomości w zakresie Nowelizacji KSC jest na dzień dzisiejszy niski – proces konsultacji do tej pory był skupiony na sektorze dużych przedsiębiorstw telekomunikacyjnych z wyłączeniem realnego udziału przedstawicieli sektora MŚP. Takie podejście spowodowało, że sektor MŚP nie jest obecnie przygotowany na nowe obowiązki ani merytorycznie, ani finansowo, ani jeżeli chodzi o posiadane kompetencje w organizacjach. Dodatkowo należy zauważyć, że zgodnie z obecną wersja Nowelizacji KSC, ma ona wejść w życie 30 dni od dnia jej ogłoszenia, co zdecydowanie jest terminem zbyt krótkim na dostosowanie się do nowej regulacji dla przedsiębiorców z sektora MŚP.

W związku z powyższym wnioskujemy o przeprowadzenie kampanii informacyjnej wśród sektora MŚP w całej Polsce, która pozwoli przedsiębiorcom zrozumieć nadchodzące obowiązki i lepiej przygotować się na ich wdrożenie.

- **Dodatkowe obowiązki wynikające z Dyrektywy NIS 2 i niepewność prawna**

Pragniemy zauważyć, że obecnie trwają bardzo zaawansowane prace nad przyjęciem nowej Dyrektywy NIS 2, które mają zakończyć się w przeciągu najbliższych tygodni. Analiza Dyrektywy NIS 2 i obecnej wersji Nowelizacji KSC pokazuje, że Nowelizacja KSC nie adresuje na ten moment wszystkich zaleceń i obowiązków NIS 2. Dodatkowo istniejące rozbieżności pomiędzy obiema regulacjami, również w zakresie obowiązków nakładanych na MŚP, spowodują negatywne zjawisko niepewności prawa oraz daleko idące skomplikowanie systemu prawnego w zakresie cyberbezpieczeństwa. Zauważamy, że już teraz przedsiębiorcy z sektora MŚP mają trudności w zrozumieniu zakresu nowych obowiązków wynikających z Nowelizacji KSC. Dodatkowe obowiązki wynikające z Dyrektywy NIS 2, w połączeniu z niepewnością po stronie sektora MŚP w zakresie wymogów jakie w danym momencie obowiązują, może stworzyć środowisko skrajnie niesprzyjające tak potrzebnym w sektorze cyberbezpieczeństwa inicjatywom i inwestycjom.

Biorąc pod uwagę obecną treść Nowelizacji KSC oraz jej skutki gospodarcze dla sektora dla MŚP, brak dostatecznego przygotowanie sektora MŚP na nowe regulacje oraz sprzeczność krajowych przepisów z projektowaną Dyrektywą NIS 2, zwracamy się z prośbą o pilne przedstawienie projektu do konsultacji publicznych i zorganizowanie konferencji uzgodnieniowej, w ramach procedury wskazanej w §36 oraz §44 Regulaminu pracy Rady Ministrów.

Z poważaniem,

_____