Warszawa, 8 października 2020 r.

STANOWISKO ZWIĄZKU PRZEDSIĘBIORCÓW I PRACODAWCÓW WS. PROJEKTU USTAWY O ZMIANIE USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA ORAZ USTAWY – PRAWO ZAMÓWIEŃ PUBLICZNYCH Z 7 WRZEŚNIA 2020 ROKU

Związek Przedsiębiorców i Pracodawców już kilkukrotnie podkreślał potrzebę jeszcze bardziej intensywnych działań w zakresie budowania powszechnego dostępu do szybkiego internetu. Uważamy, że jest to czynnik kluczowy z punktu widzenia dalszego dynamicznego rozwoju gospodarczego Polski. Ostatnie lata pokazały, że konsekwentna praca legislacyjna, eliminowanie barier i przeznaczenie istotnych środków na inwestycje, może doprowadzić do osiągnięcia realnych skutków w zakresie poprawy dostępności internetu w Polsce, o czym świadczyć może choćby poprawa pozycji naszego kraju w rankingu DESI. Na horyzoncie pojawiają się jednak kolejne wyzwania, wśród których wymienić można choćby rosnące zapotrzebowanie na internet, potrzeba skutecznego zaimplementowania (w przypadku 5G) bądź istotnego upowszechnienia (światłowód) nowych technologii w zakresie dostępu do sieci. Wszystko to świadczy o tym, że cyfryzacja kraju, dalsze inwestycje w infrastrukturę cyfrową i prowadzenie działań ukierunkowanych na zwiększanie kompetencji cyfrowych Polaków, to wciąż tematy, które nie mogą zejść z listy priorytetów na agendzie rządu.

Równolegle, bez wątpienia istotnym wyzwaniem pozostaje zapewnienie cyberbezpieczeństwa. Wraz ze wzrostem znaczenia sieci telekomunikacyjnych i wykorzystywaniem jej do realizacji coraz szerszego katalogu usług publicznych, niekiedy krytycznych, wprowadzenie regulacji minimalizujących ryzyko występowania incydentów zakłócających świadczenie usług wydaje się być oczywiste.

Przedstawiony projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa rozumiemy jako próbę odpowiedzi na to wyzwanie, sformułowaną po dwuletnim okresie obowiązywania zmienianego aktu. W tym sensie zrozumiałe wydaje się być zaproponowanie przepisów wprowadzających centra wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzających obowiązek ustanawiania sektorowych CSIRT (zamiast dotychczasowego trybu fakultatywnego).

Niemniej jednak niektóre z przepisów budzą kontrowersje. Dotyczy to przede wszystkim przepisów zaproponowanych w odniesieniu do możliwości weryfikowania dostawców sprzętu lub oprogramowania.

Uwzględnione w projekcie regulacje zakładają, że możliwe będzie wyłączenie podmiotów zidentyfikowanych jako źródło zagrożenia z systemu zamówień publicznych w Polsce, czy zobowiązanie podmiotów krajowego systemu cyberbezpieczeństwa do ograniczenia korzystania z produktów, oprogramowania i usług takich dostawców. Tego rodzaju oceny ryzyka może, zgodnie z art. 66a projektu, dokonać Kolegium ds. Cyberbezpieczeństwa.

Jednym z bardziej wrażliwych elementów sporządzania oceny w projekcie ustawy, są kryteria brane pod uwagę w toku procesu. Zgodnie z projektem, przy sporządzaniu oceny przeprowadzać ma się analizy dotyczące w szczególności m.in.:

- zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania;

- prawdopodobieństwa, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza UE bądź NATO (analiza ta ma uwzględniać m.in. stopień i rodzaj powiązań między dostawcą a tym państwem, prawodawstwo państwa w zakresie ochrony praw obywatelskich i praw człowieka, czy strukturę własnościową dostawcy).

Przedstawione kryteria mają charakter nieostry i podmiotowy, a nie przedmiotowy, co umożliwia uznanie takiego samego sprzętu lub oprogramowania za stanowiące zagrożenie albo nie, w zależności wyłącznie od jego dostawcy.

Kryteria (*de facto*) doboru dostawców sprzętu i oprogramowania uznajemy zatem za przejaw chęci pozostawienia otwartego pola gry i możliwości podjęcia każdej decyzji, w zależności od rozwoju sytuacji geopolitycznej, jak i dynamiki wydarzeń w innych państwach. W tym sensie – polityki międzynarodowej, a niekoniecznie bezpośredniego interesu gospodarczego – przyjęte przez projektodawcę podejście pozwala na dostosowanie aktywności Polski do uwarunkowań międzynarodowych i podjęcie dowolnej decyzji. Należy jednak pamiętać o konieczności zapewnienia pewnej przewidywalności otoczenia regulacyjnego dla działających w Polsce przedsiębiorców.

Zwracamy również uwagę na specyfikę niektórych sektorów – sparaliżowanie dostępu do produktów niektórych producentów urządzeń elektronicznych może spowodować np. istotne trudności w zakresie technicznych możliwości produkowania leków.

Ponadto, pragniemy poddać pod rozwagę ustawodawcy możliwość zastosowania uzupełniających rozwiązań w zakresie cyberbezpieczeństwa, które zminimalizują negatywne skutki finansowe dla przedsiębiorców telekomunikacyjnych, przy równoczesnym zapewnieniu najwyższych standardów cyberbezpieczeństwa. W szczególności zwracamy uwagę na zbyt krótki przewidziany 5-cio letni okres na eliminację sprzętu dostawcy określonego jako dostawcy wysokiego ryzyka. Użytkownicy tego sprzętu lub oprogramowania nabywali go w dobrej wierze i z założeniem pełnego wykorzystania biznesowego przez okres zdecydowanie dłuższy, niż 5 lat. Realny czas na amortyzację sprzętu wykorzystywanego w sieciach telekomunikacyjnych stanowi minimum 7-8 lat. W tym okresie zasadne byłoby również dopuszczenie dokonywania dalszych niezbędnych zakupów i wdrożeń, w tym np. aktualizacji oprogramowania kluczowego dla bezpieczeństwa. Dodatkowo, zwracamy uwagę na ewentualną możliwość uzależnienia zasad eliminacji sprzętu dostawcy określonego jako dostawcy wysokiego ryzyka od poziomu wrażliwości danego obszaru dla krajowego systemu cyberbezpieczeństwa, na którym sprzęt jest wykorzystywany. Ustawodawca może wskazać regiony, w których należy zastosować najbardziej rygorystyczne podejście ze względu na ich krytyczną i strategiczną rolę w krajowym systemie cyberbezpieczeństwa.

Istotnym wątkiem jest również kwestia rozszerzenia zakresu ustawy na podmioty spoza tych uznanych za operatora usługi kluczowej. Należy podkreślić, że autonomiczne zarządzanie bezpieczeństwem przez te podmioty doprowadziło do zbudowania złożonych i wzajemnie powiązanych systemów zabezpieczeń, w trybie ciągłym analizowanych pod kątem skuteczności i aktualności. Omawiana regulacja może spowodować, że funkcjonalność tych systemów zostanie ograniczona z uwagi na komunikaty bezpieczeństwa ogłaszane przez organy administracji. Tym samym, podmioty gospodarcze poniosą niejako podwójne koszty.

Należy ponadto zwrócić uwagę na regulacje dot. ostrzeżeń oraz poleceń zabezpieczających, wydawanych przez Pełnomocnika ds. Cyberbezpieczeństwa. Zarówno ostrzeżenia jak i polecenia zabezpieczające w swojej treści wskazują określone zachowanie, które należy podjąć i które ma w swoim założeniu zmniejszyć ryzyko incydentu. Jednym ze wskazanych w ustawie zachowań zmniejszających ryzyko incydentu jest nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL (art. 67b ust. 3 pkt 7 uksc), czyli działanie polegające na ograniczaniu (blokowaniu) dostępu do niektórych stron lub usług. Zgodnie z regulacją Rozporządzenia EU dot. otwartego internetu, użytkownicy końcowi mają prawo do uzyskania za pomocą internetu dostępu do informacji i treści oraz do ich rozpowszechniania, a także do korzystania z wybranych aplikacji i usług oraz

ich udostępniania, jak również do korzystania z wybranych urządzeń końcowych, niezależnie od lokalizacji użytkownika końcowego lub dostawcy usług czy też od lokalizacji, miejsca pochodzenia lub miejsca docelowego informacji, treści lub usługi. Zasada otwartego internetu może podlegać ograniczeniu tylko wyjątkowo i przy zachowaniu proporcjonalnych środków – należałoby zatem uzupełnić projekt ustawy o regulacje gwarantujące wyjątkowość i proporcjonalność radykalnego środka, jakim jest zablokowanie dostępu do niektórych stron lub usług.

Przedstawiony projekt zakłada wprowadzenie do ustawy o krajowym systemie cyberbezpieczeństwa zupełnie nowego rozdziału 4a dotyczącego obowiązków przedsiębiorców komunikacji elektronicznej. Pragniemy podkreślić, że analogiczne regulacje znajdują się już w projekcie prawa komunikacji elektronicznej. Istnieje zatem potrzeba przyjęcia jednolitego podejścia i uregulowania obowiązków przedsiębiorców komunikacji elektronicznej w jednym akcie. Część z opisywanych obowiązków podmiotów ma charakter dosyć ogólny (jak choćby „podejmowanie środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka"). Faktyczna „głębokość" tychże obowiązków zależeć będzie w dużej mierze od wydanych na podstawie nowych przepisów aktów wykonawczych. Szczegółowe parametry tychże obowiązków, takie jak minimalny zakres ww. środków technicznych i organizacyjnych, czy sposób dokumentowania ich, mają być zgodnie z analizowanym projektem opisane w rozporządzeniu ministra właściwego ds. informatyzacji. Minister ten będzie również określał próg incydentu telekomunikacyjnego, którego przekroczenie spowoduje obowiązek zgłoszenia incydentu przez przedsiębiorcę. Należy w tym miejscu podkreślić, że proponowane regulacje wykraczają nieco ponad minimalny poziom obowiązków przewidziany w EKŁE, choćby w zakresie dostawców interpersonalnej komunikacji elektronicznej niewykorzystujących numerów.

Niezależnie od potrzeby ujednolicenia i skoordynowania prawodawstwa w zakresie obowiązków ciążących na przedsiębiorcach komunikacji elektronicznej, ważne jest aby na etapie projektowania aktów wykonawczych pamiętać o konieczności zachowania zasady proporcjonalności i nieobciążania przedsiębiorców dodatkowymi obowiązkami w stopniu wyższym, niż jest to konieczne dla zrealizowania celów ustawy.

Jednocześnie, wszelkie mechanizmy ocenne należy umocować w istniejących już przepisach, takich jak te zawarte w ustawie Prawo przedsiębiorców oraz ustawie Kodeks postępowania administracyjnego.

Gwarantują one przejrzystość procedur i ich zasad, umożliwiają udział dostawcy w postępowaniu oraz zapewniają niedyskryminującą procedurę odwoławczą.

Mając na uwadze wszelkie powyższe aspekty, postulujemy o dalsze prace nad przedstawionym projektem ustawy i kontynuowanie szerokich konsultacji tego aktu, tak aby każdy zainteresowany podmiot miał możliwość skutecznego przekazania swojej opinii na jego temat. Nie ulega wątpliwości, że projekt będzie miał bezpośredni wpływ na wiele podmiotów obecnych na polskim rynku, dlatego szczególnie istotne jest, by wysłuchać wszystkich racji i rozważyć np. możliwość przeprowadzenia konferencji uzgodnieniowej, zgodnie z bardzo dobrą praktyką obecną w niektórych procesach legislacyjnych.