WRDS WOJEWÓDZKA RADA DIALOGU SPOŁECZNEGO

Wojewódzka Rada Dialogu Społecznego w województwie mazowieckim
ul. Jagiellońska 26, 03-719 Warszawa
Telefon: 22-590-7739, wrds@mazovia.pl

Do druku nr 1955

P_4072510

Warszawa, 17 maja 2024 r.

KM-WRDS.111.42.2024.EM

Pan
Szymon Hołownia
Marszałek Sejmu Rzeczypospolitej Polskiej

Dotyczy: przekazanie stanowiska stron WRDS.

Szanowny Panie Marszałku,

w załączeniu przekazuję stanowisko nr 2/24 strony pracodawców, strony pracowników oraz strony samorządowej Wojewódzkiej Rady Dialogu Społecznego w województwie mazowieckim z 15 maja 2024 r. w sprawie wykazania ryzyk i zagrożeń dla jednostek samorządu terytorialnego i przedsiębiorców wynikających z projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (UC32).

Z poważaniem

Przewodniczący
Wojewódzkiej Rady Dialogu Społecznego
w województwie mazowieckim

Dariusz Paczuski

Podstawa prawna:
art. 50 ust. 4 *Ustawy o Radzie Dialogu Społecznego i innych instytucjach dialogu społecznego* (Dz. U. z 2018 r. poz. 2232, z późn. zm.).

Załącznik:

1. Stanowisko nr 2/24 strony pracodawców, strony pracowników oraz strony samorządowej Wojewódzkiej Rady Dialogu Społecznego w województwie mazowieckim z dnia 15 maja 2024 r.

Sprawę prowadzi:
Ewelina Mikulska

WRDS WOJEWÓDZKA RADA DIALOGU SPOŁECZNEGO

Stanowisko nr 2/24
strony pracodawców, strony pracowników oraz strony samorządowej
Wojewódzkiej Rady Dialogu Społecznego w województwie mazowieckim
z dnia 15 maja 2024 r.

w sprawie wykazania ryzyk i zagrożeń dla jednostek samorządu terytorialnego i przedsiębiorców wynikających z projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (UC32)

Na podstawie art. 42 ust. 1 pkt 1 lit. a w zw. z ust. 1b ustawy z dnia 24 lipca 2015 r. o Radzie Dialogu Społecznego i innych instytucjach dialogu społecznego (Dz. U. z 2018 r. poz. 2232, z późn. zm.[1]) strona pracodawców, strona pracowników oraz strona samorządowa Wojewódzkiej Rady Dialogu Społecznego w województwie mazowieckim, przyjmują stanowisko, w którym apelują o wyeliminowanie nadregulacji zawartych w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa w stosunku do dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

I. Wstęp

Polska do dnia 17 października 2024 r. zobowiązana jest do wdrożenia (implementowania) unijnej dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Wymóg dostosowania przepisów prawa krajowego do tejże dyrektywy w w/w terminie wynika z przepisu art. 41 ust. 1 dyrektywy NIS 2.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa z dnia 23 kwietnia 2024 r. opublikowany na stronach Rządowego Centrum Legislacji w dniu 24 kwietnia 2024 r. w sposób rażący wykracza jednak poza regulacje dyrektywy NIS 2, stanowiąc tym samym tzw. nadregulację, która powoduje daleko idące negatywne skutki dla wielu podmiotów – przedsiębiorców oraz dla administracji publicznej, w tym dla jednostek samorządu terytorialnego.

---

[1] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2020 r. poz. 568, 2157, z 2021 r. poz. 2445, z 2022 r. poz. 2666 oraz z 2023 r. poz. 1586 i 1723.

Innymi słowy, projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa zawiera bardziej restrykcyjne uregulowania niż dyrektywa unijna NIS 2. W niniejszym stanowisku zaprezentowane one zostaną w sposób możliwie najbardziej syntetyczny i czytelny.

II. Rozszerzenie podmiotów kluczowych o nowe sektory i podsektory – nadregulacja w stosunku do dyrektywy NIS 2

W pierwszej kolejności projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (dalej również: „**projekt ustawy o KSC**") w sposób znaczący – w stosunku do dyrektywy NIS 2 – rozszerza ilość podmiotów kluczowych, których ustawa ta ma dotyczyć, w tym identyfikując jako sektory kluczowe, sektory które w dyrektywie NIS 2 traktowane są jedynie jako ważne, a zatem podlegające mniejszemu zakresowi nadzoru. Klasyfikacja przez projekt ustawy o KSC podmiotów ważnych jako podmiotów kluczowych wiąże się z podwyższeniem stopnia nadzoru nad tymi podmiotami również o nadzór prewencyjny. To znaczące wyjście poza wymogi dyrektywy NIS 2 neguje podstawowe zasady, zgodnie z którymi powinna następować implementacja dyrektyw unijnych.

Dyrektywa NIS 2 przewiduje, że jednym z kryteriów pozwalających na zakwalifikowanie danego podmiotu, jako podmiotu kluczowego lub ważnego, jest zaliczenie działalności tego podmiotu do sektora kluczowego, które wyszczególnione są odpowiednio w załączniku nr I i załączniku nr II do dyrektywy NIS 2. Z kolei w polskim projekcie ustawy o KSC, polski prawodawca znacznie rozszerzył listę sektorów gospodarki umożliwiając tym samym zakwalifikowanie większej liczby podmiotów jako podmiotów kluczowych i jednocześnie ograniczając listę sektorów gospodarki pozwalających na zaliczenie podmiotu do kategorii podmiotów ważnych. Co więcej, polski projektodawca objął zakresem regulacji – w przeciwieństwie do dyrektywy NIS 2 – również lokalne jednostki samorządu a także instytucje edukacyjne, co powoduje konieczność wdrożenia przez te podmioty obowiązków, których koszty mogą być szacowane w milionach złotych. Dodatkowo dochodzi do tego ryzyko wszczęcia – rodzącej bardzo niebezpieczne konsekwencje – procedury uznania dostawcy sprzętu lub oprogramowania dla tych podmiotów (zarówno dla podmiotów kluczowych, jak i ważnych), za dostawcę wysokiego ryzyka, co wiązało się będzie z koniecznością pozbycia się takiego sprzętu w określonym czasie (co do zasady 7 lat) i nabycia nowego, co w konsekwencji generowało będzie ogromne koszty.

II.1. Nowe sektory i podsektory wskazane w projekcie ustawy o KSC - nadregulacja

Projekt ustawy o KSC w zakresie podmiotów kluczowych obejmuje – w przeciwieństwie do dyrektywy NIS 2 – hurtownie farmaceutyczne, przedsiębiorców posiadających pozwolenie na dopuszczenie do obrotu produktu leczniczego, importerów i wytwórców produktów leczniczych / substancji czynnych, importerów równoległych i wytwórców produktów leczniczych / substancji czynnych, importerów równoległych, dystrybutorów substancji czynnej oraz apteki. Zgodnie natomiast z załącznikiem nr 1 do dyrektywy NIS 2 status podmiotów kluczowych przysługuje tylko tym podmiotom, które prowadzą

działalność badawczo-rozwojową w zakresie produktów leczniczych, podmiotom produkującym podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, a także podmiotom produkującym wyroby medyczne, które uznane są za mające krytyczne znaczenie podczas stanu zagrożenia zdrowia publicznego. Zatem dyrektywa NIS 2 zawiera tutaj stosowny warunek, który musi zaistnieć, aby podmioty te zakwalifikowane zostały jako podmioty kluczowe. Warunkiem tym jest uznanie ich za mające krytyczne znaczenie podczas stanu zagrożenia zdrowia publicznego. Polski prawodawca wyeliminował z projektu ustawy o KSC tenże warunek, uznając „z góry" podmioty takie jak np. apteki, za podmioty kluczowe.

Projekt ustawy o KSC poszerza również – w stosunku do dyrektywy NIS 2 – sektor energii o podsektor wydobywania kopalin pomimo tego, iż sektor energetyka wskazany w załączniku I do dyrektywy NIS 2 nie zalicza do usług kluczowych podsektora wydobywania kopalin.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, jako podmioty kluczowe klasyfikuje podmioty, które w dyrektywie NIS 2 uznane zostały jedynie jako podmioty ważne i tym samym do podmiotów kluczowych zalicza takie sektory i podsektory jak: produkcja, wytwarzanie i dystrybucja chemikaliów; produkcja, przetwarzanie i dystrybucja żywności; produkcja w tym podsektor produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, podsektor produkcji komputerów, wyrobów elektronicznych i optycznych, podsektor produkcji urządzeń elektrycznych, podsektor produkcji maszyn i urządzeń, gdzie indziej niesklasyfikowaną, oraz podsektor produkcji pojazdów samochodowych, przyczep i naczep.

II.2 Rozszerzenie podmiotów kluczowych o jednostki samorządu terytorialnego oraz ich związki oraz inne jednostki sektora finansów publicznych

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa rozszerza zakres podmiotów kluczowych o jednostki sektora finansów publicznych o których mowa w art. 9 pkt 1-6, 8 i 10-13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r., poz. 1270, z późn. zm.), a zatem m.in. o jednostki samorządu terytorialnego oraz ich związki, ale również samodzielne publiczne zakłady opieki zdrowotnej, czy uczelnie publiczne. Należy podkreślić, że zarówno jednostki samorządu terytorialnego, jak i co do zasady instytucje edukacyjne nie są uznane za podmioty kluczowe przez dyrektywę NIS 2. Te ostatnie kwalifikowane są przez dyrektywę NIS 2 za podmioty kluczowe jedynie wówczas, gdy prowadzą działalność badawczą o krytycznym znaczeniu. Polski projektodawca nie wprowadza tego warunku. W wyniku tego zatem każda uczelnia publiczna będzie zobowiązana do realizacji kosztownych wymogów w zakresie cyberbezpieczeństwa.

W tym miejscu należy podkreślić, że dyrektywa NIS 2 w art. 2 ust. 2 lit. f) stanowi, że jednostki na poziomie regionalnym mogą zostać uznane za podmioty administracji publicznej tylko wtedy, gdy świadczą usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą, co powinno być potwierdzone oceną opartą na analizie ryzyka. Projekt

ustawy o KSC nie odnosi się do powyższego warunku. Dyrektywa NIS 2 – w sposób bezwarunkowy – jako podmioty kluczowe obejmuje tylko podmioty administracji publicznej na poziomie rządu centralnego, zaś projektodawca polski rozszerza podmioty kluczowe o m.in. jednostki samorządu terytorialnego, co generuje niepotrzebne, gigantyczne koszty dla tychże jednostek samorządu terytorialnego. Sektor administracji publicznej w Ocenie Skutków Regulacji projektu ustawy o KSC wyliczony został na 27.905 podmiotów, a przyjmuje się, że liczba ta – jak zresztą liczba wszystkich podmiotów kluczowych i ważnych – nie została doszacowana. Należy tutaj podkreślić, że przeważająca większość tych podmiotów, to jednostki samorządu terytorialnego i jednostki im podległe. Włączenie w projekcie ustawy o KSC takich podmiotów jak jednostki samorządu terytorialnego do kategorii podmiotów kluczowych, wbrew wymaganiom dyrektywy NIS 2, może prowadzić do znaczących trudności w ich funkcjonowaniu, nie przyczyniając się jednocześnie do realnego wzrostu bezpieczeństwa cybernetycznego kraju. Jednostki samorządu terytorialnego zobowiązane będą do wyłożenia olbrzymich pieniędzy na zrealizowanie licznych rygorystycznych i sformalizowanych obowiązków, nałożonych przez projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz objęte są ryzykiem gigantycznych, wielomilionowych kar za niezrealizowanie tychże obowiązków, które mogą być nałożone nawet wówczas, gdy doszło do jednorazowego naruszenia. Projekt ustawy o KSC nakłada osobistą odpowiedzialność na osoby kierujące danym podmiotem. Do tego dochodzi perspektywa wyeliminowania dostawcy sprzętu dla danej jednostki samorządu terytorialnego w przypadku uznania przez Ministra Cyfryzacji tegoż dostawcy za dostawcę wysokiego ryzyka. Ten aspekt dotyczy wszystkich podmiotów kluczowych i ważnych i co więcej nie został on w ogóle przewidziany w dyrektywie NIS 2, co zostanie omówione osobno w dalszej części stanowiska. Należy tutaj jeszcze wskazać na to, że podmioty kluczowe podlegały będą bardzo szerokiemu nadzorowi sprawowanemu przez organy właściwe do spraw cyberbezpieczeństwa. Będzie on miał charakter nie tylko następczy (jak w przypadku podmiotów ważnych), ale również prewencyjny (art. 53 ust. 3 projektu ustawy o KSC). W pełni nieuzasadnione jest kwalifikowanie jednostek samorządu terytorialnego za podmiot kluczowy. Jednostki samorządu terytorialnego nie są newralgicznymi podmiotami narażonymi na cyberzagrożenia. To zdecydowanie zbyt daleko idąca ingerencja polskiego projektodawcy, wykraczająca poza regulacje dyrektywy NIS 2.

Warto w tym miejscu podkreślić, że kraje takie, jak: Niemcy, Belgia, Węgry, Finlandia i Austria, które wdrożyły już dyrektywę NIS 2 lub przedstawiły projekt jej transpozycji, nie objęły zakresem nowych przepisów jednostek samorządu terytorialnego.

II.3. Podsumowanie skutków rozszerzenia w projekcie ustawy o KSC podmiotów zaliczanych do podmiotów kluczowych

Znaczące - w stosunku do dyrektywy NIS 2 - rozszerzenie katalogu podmiotów kluczowych i ważnych, na 18 sektorów (łącznie ponad 38.000 podmiotów), łączy się z daleko idącymi obowiązkami dla tychże podmiotów. Wskazać tutaj należy chociażby na obowiązkowe, cykliczne -

co najmniej raz na 2 lata - audyty bezpieczeństwa, nałożone nie tylko na podmioty kluczowe, ale również na podmioty ważne (co jest również sprzeczne z dyrektywą NIS 2, która nakłada ten obowiązek jedynie na podmioty kluczowe), przy czym pierwszy audyt (audyt wstępny) należy przeprowadzić już w ciągu 12 miesięcy. Audyty te (wstępny oraz cykliczne) muszą być przeprowadzane przez osoby o odpowiednich kompetencjach, a udostępnienie wyników audytu właściwemu organowi ma nastąpić w ciągu 3 dni od ich otrzymania. Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa nakłada na podmioty szereg nowych obowiązków, takich jak: obowiązek stworzenia systemów zarządzania bezpieczeństwem informacji, zgodnie z normami ISO, obowiązek wdrożenia zabezpieczeń przed incydentami cyberbezpieczeństwa, w oparciu o analizę ryzyka i najnowszy stan wiedzy, obowiązek dokonywania do organu nadzorczego zgłoszeń incydentów (wczesne ostrzeżenie już w terminie 12 h/24 h, kolejne w terminie 72 h) oraz powiadamianio incydentach własnych użytkowników. Nadto wskazać należy na: obowiązek wdrożenia rozbudowanej dokumentacji dotyczącej cyberbezpieczeństwa, obowiązek rejestracji w krajowym systemie informatycznym oraz wymiany informacji za jego pośrednictwem, obowiązek zarządzania ryzykiem łańcucha dostawców usług, obowiązek zapewnienia dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń dot. cyberbezpieczeństwa wśród własnych pracowników. Dodatkowo, dla każdego sektora Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności szczegółowe wymagania. To olbrzymie proceduralne, techniczne i biznesowe (kosztotwórcze) przedsięwzięcie, z którym będą musieli się zmierzyć - nieświadomi jeszcze tych obowiązków - przedsiębiorcy, ale również jednostki samorządu terytorialnego. Za ich niespełnienie przewidziane zostały wielomilionowe kary – do 10.000.000 euro lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej. Nie sposób oszacować kosztów wdrożenia tych przepisów, które w sektorze prywatnym mogą wynosić od kilkudziesięciu, kilkuset tysięcy złotych nawet do ponad miliona (w stosunku do pojedynczej firmy), nie mówiąc o wielomilionowych nakładach dla sektora administracji publicznej. Poza kosztami wdrożenia, wskazać należy na koszty coroczne, jakie podmioty kluczowe i ważne muszą wykładać w celu spełnienia obowiązków. Ułomności przedstawia w tym zakresie Ocena Skutków Ryzyka, która nie zawiera jakiejkolwiek estymacji w/w kosztów. Projekt ustawy nakłada szereg nowych obowiązków w tym m.in. obowiązek stworzenia systemów zarządzania bezpieczeństwem, zgodnie z normami ISO27001 oraz ISO22301 podczas gdy dyrektywa NIS 2 wskazuje, że standardy powinny być promowane, a nie narzucane (art. 25 dyrektywy NIS 2) i wskazuje, że podmioty kluczowe i ważne powinny wdrażać odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne wykorzystując najnowszy stan wiedzy oraz normy europejskie i organizacyjne (art. 21 ust. 1 dyrektywy NIS 2). Niezasadne jest zatem narzucenie przez polskiego projektodawcę obowiązku stosowania konkretnych norm.

Warto w tym miejscu wspomnieć, że polski projekt ustawy o KSC zaciera rozróżnienie podmiotów na kluczowe i ważne, gdyż przewiduje dla tychże podmiotów takie same obowiązki. Dyrektywa NIS

2 z kolei nakłada jedynie na podmioty kluczowe obowiązek przeprowadzenia audytów, podczas gdy projektodawca krajowy obejmuje tym obowiązkiem wszystkie podmioty: kluczowe i ważne (art. 15 ust. 1 projektu ustawy o KSC). W dotychczasowej wersji ustawy obowiązek przeprowadzenia audytu bezpieczeństwa dotyczył systemu informacyjnego wykorzystywanego jedynie do świadczenia usługi kluczowej.

III. Ryzyko uznania dostawcy usług i produktów dla podmiotu kluczowego i ważnego za dostawcę wysokiego ryzyka

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa reguluje całkowicie nieprzewidzianą w dyrektywie NIS 2 procedurę uznania dostawcy sprzętu lub oprogramowania dla danego podmiotu kluczowego lub ważnego za dostawcę wysokiego ryzyka. Aspekt ten dotyczy zarówno podmiotów kluczowych, jak i ważnych. Zatem z tego punktu widzenia nie ma żadnych rozbieżności w różnicowaniu w/w podmiotów na kluczowe i ważne. Procedura dostawcy wysokiego ryzyka (HRV – high risk vendor) wprowadzona została przez projektodawcę w 18 sektorach. Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa wprowadzając powyższą procedurę zawiera nadregulację w stosunku do dyrektywy NIS 2. Tym samym każda firma lub jednostka samorządu terytorialnego (szerzej - administracja publiczna), które w projekcie ustawy zakwalifikowane są jako podmioty kluczowe lub ważne, stoi przed perspektywą uznania swojego dostawcy (np. sprzętu komputerowego) za dostawcę wysokiego ryzyka. Przesłanki do takiego uznania przez organ (Minister Cyfryzacji) są bardzo nieostre, a konsekwencje bardzo daleko idące. Dostawcę wysokiego ryzyka produktów, usług, procesów informacyjno – komunikacyjnych (ICT) wskazuje Minister Cyfryzacji w oparciu o opinię (art. 67 b ust. 10 projektu ustawy o KSC), sporządzoną przez tzw. Kolegium ds. cyberbezpieczeństwa (organ polityczny, w którym przewodniczącym jest Prezes Rady Ministrów), w której to opinii bierze się pod uwagę nieostre i polityczne kryteria takiej jak: prawdopodobieństwo, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem np. struktury własnościowej dostawcy sprzętu lub oprogramowania lub zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Dla firmy lub administracji publicznej oznacza to konieczność usunięcia przez nią takiego dostawcy, co jak nie trudno sobie wyobrazić, pociągnie za sobą gigantyczne koszty. Przykładowo uznanie w danej firmie dostawcy podzespołów komputerowych za dostawcę wysokiego ryzyka, z uwagi np. na kraj pochodzenia, będzie nakładało na daną firmę obowiązek pozbycia się tego sprzętu. Przykłady można tutaj szerzyć. W konsekwencji, doprowadzi to do osłabienia konkurencyjności polskich przedsiębiorców na rynku obejmującym podmioty kluczowe i ważne, a nawet do powstania duopoli czy monopoli. Wycofanie z użytkowania dostawcy wysokiego ryzyka (co do zasady w ciągu 7 lat) ma się odbywać na koszt danego przedsiębiorcy lub jednostki samorządu terytorialnego, i projektodawca nie przewiduje tutaj jakiejkolwiek rekompensaty, co zresztą przyznane jest wprost w Ocenie Skutków Ryzyka (s. 30

OSR). Projekt nie zakłada nawet możliwości poprawy (w zakresie zabezpieczeń) swojego produktu, usługi przez danego dostawcę, uznanego za dostawcę wysokiego ryzyka. To wręcz niedopuszczalne, żeby nie przewidzieć jakiegokolwiek postępowania sanacyjnego dla takiego dostawcy, który powinien mieć prawo do poprawy swojego produktu lub usługi w zakresie zabezpieczeń. Sam już proces, w ramach którego rozstrzygane będzie, czy dany dostawca jest dostawcą wysokiego ryzyka, będzie wiązał się dla niego ze swoistego rodzaju ostracyzmem ze strony jego klientów, niezależnie od wyniku zakończenia tego procesu. Biorąc pod uwagę szeroką definicję dostawcy sprzętu lub oprogramowania zawartą w projekcie ustawy o KSC – mowa tu o dostawcy w rozumieniu importera, dystrybutora, jak i producenta oraz upoważnionego przedstawiciela (art. 2 pkt 4 c projektu ustawy o KSC), to decyzja o uznaniu takiego dostawcy za dostawcę wysokiego ryzyka dotknie bardzo dużej liczby podmiotów.

Należy tutaj zwrócić jeszcze uwagę na fakt, że polski projektodawca w Ocenie Skutków Ryzyka nie wskazał, w jaki sposób dokonywać recyklingu oprogramowania, sprzętu, którego dany podmiot kluczowy lub ważny będzie musiał się pozbyć, a jest to przecież bardzo ważny aspekt z punktu widzenia założeń, którymi kieruje się Unia Europejska.

III.1 Wyeliminowanie możliwości udziału podmiotów kluczowych w charakterze strony postępowania w przedmiocie uznania dostawcy za dostawcę wysokiego ryzyka

Podkreślenia wymaga fakt, że w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka (art. 67b ust. 1 projektu ustawy o KSC), stroną postępowania jest jedynie dostawca wysokiego ryzyka. Wyłączono tutaj bowiem zastosowanie art. 28 kpa stanowiącego, że: „stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie". Wyłączony jest tutaj zatem podmiot kluczowy lub podmiot ważny, który korzysta z oprogramowania takiego dostawcy wysokiego ryzyka. Podmioty te powinny mieć prawo wziąć udział w tym postępowaniu, gdyż zwyczajnie mają w tym interes prawny. Wyjątkiem jest tutaj przedsiębiorca komunikacji elektronicznej, który spełnia określony w przepisach projektu ustawy census majątkowy (co najmniej dwudziestotysięczna krotność przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa GUS). Jest to bardzo specyficzne uregulowanie, które zaburza zasadę równowagi, zwłaszcza biorąc pod uwagę fakt, że decyzja o wycofaniu sprzętu, zgodnie z projektem ustawy ma dotyczyć 18 branż, a nie tylko branży telekomunikacyjnej. W tym postępowaniu wyłączono również przepis art. 31 kpa i tym samym wyeliminowano udział organizacji społecznych, co również zasługuje na krytykę.

Udział organizacji społecznych wyłączony również został w postępowaniu administracyjnym, w którym rozpatrywana będzie skarga na decyzję o uznaniu dostawcy za dostawcę wysokiego ryzyka (art. 67b ust. 15 projektu ustawy o KSC). Warto także wskazać na niepokojący fakt, że wyrok sądu administracyjnego, który rozpatruje skargę doręczany jest skarżącemu z częścią uzasadnienia,

która nie zawiera informacji niejawnych. Skarżący nie posiądzie zatem do końca wiedzy o motywach wykluczenia go jako dostawcy produktów lub usług dla danego podmiotu kluczowego lub ważnego.

IV. Uwagi końcowe

Działanie projektodawcy, polegające na dokonaniu swoistego rodzaju „transferu" wybranych sektorów (podsektorów) z sektora ważnego do sektora kluczowego, rozszerzenie w ramach podmiotów kluczowych sektorów o inne podsektory, wprowadzenie nieznanej w dyrektywie NIS 2 procedury wydania decyzji, co do uznania danego dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (HRV), pozostaje w sprzeczności z prawem unijnym, a to z racji, że wprowadza środki nieprzewidziane w dyrektywie. Implementacja dyrektywy NIS 2 z tak daleko idącymi różnicami (obostrzeniami) w stosunku do tejże dyrektywy nakłada na projektodawcę obowiązek przygotowania tzw. tabeli niezgodności, który to obowiązek nie został wykonany.

Na tle innych państw Unii Europejskiej, które wprowadziły już w swoim porządku prawnym dyrektywę NIS 2, polski projekt ustawy regulujący cyberbezpieczeństwo jest najbardziej restrykcyjny. Dotyczy największej liczby sektorów i podmiotów oraz wprowadza nieuregulowaną w dyrektywie NIS 2 procedurę umożliwiającą uznanie danego dostawcy za dostawcę wysokiego ryzyka (HRV – high risk vendor), czego konsekwencje finansowe – liczone niekiedy w wielu milionach złotych – ponosić będą podmioty kluczowe i ważne, a na koniec, co przyznaje zresztą projektodawca w Ocenie Skutków Ryzyka – konsumenci (s. 29 i s. 30 OSR), gdyż podmioty kluczowe i ważne doliczą do swoich towarów (usług) koszty związane z operacją wyeliminowania i zakupu nowych produktów lub usług.

Należy zwrócić uwagę na niemalże całkowity brak świadomości podmiotów objętych nową regulacją, co do obowiązków i możliwości skorzystania z procedury uznania dostawcy tychże podmiotów za dostawcę wysokiego ryzyka i związanych z tym konsekwencji (wyeliminowanie produktów). Na krytykę zasługuje również nieskierowanie projektu ustawy o KSC do konsultacji z uwzględnieniem wszystkich ujętych w regulacji sektorów.

Nowe przepisy mają wejść w życie po upływie 1 miesiąca od dnia ogłoszenia, a podmioty kluczowe i ważne będą miały 6 miesięcy na zrealizowanie niektórych już obowiązków wskazanych w projekcie ustawy.

W kontekście powyższych uwag do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa strona pracodawców, strona pracowników oraz strona samorządowa Wojewódzkiej Rady Dialogu Społecznego w województwie mazowieckim postulują o:

1. Dostosowanie zakresu podmiotów kluczowych i ważnych do zakresu wynikającego z dyrektywy NIS 2, w tym usunięcie z kategorii podmiotów kluczowych jednostek samorządu terytorialnego – dostosowanie zakresu podmiotowego ustawy do zakresu wynikającego z dyrektywy NIS 2;

2. Wyeliminowanie procedury uznania w drodze decyzji danego dostawcy sprzętu, usługi dla podmiotu kluczowego lub podmiotu ważnego, za dostawcę wysokiego ryzyka.
3. Wyeliminowanie konieczności przeprowadzenia audytów dla podmiotów ważnych.
4. Odstąpienie od rygorystycznego wymagania stosowania norm technicznych do wytworzenia dokumentacji, zgodnie z wymaganiami ISO 27001 lub normy jej równoważnej i ISO 22301 lub normy jej równoważnej.
5. Oszacowanie w Ocenie Skutków Regulacji kosztów wdrożenia obowiązków przez podmioty kluczowe i ważne oraz kosztów przeprowadzania cyklicznych obowiązkowych audytów bezpieczeństwa; oszacowanie wpływu wydania decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka.

Stanowisko zostało zaakceptowane przez stronę pracodawców, stronę pracowników oraz stronę samorządową Wojewódzkiej Rady Dialogu Społecznego w województwie mazowieckim. Podpis w imieniu stron złożył Przewodniczący Wojewódzkiej Rady Dialogu Społecznego w województwie mazowieckim.

Przewodniczący
Wojewódzkiej Rady Dialogu Społecznego
w województwie mazowieckim

Dariusz Paczuski

Stanowisko otrzymują:
1. Prezydent RP
2. Marszałek Senatu RP
3. Marszałek Sejmu RP
4. Prezes Rady Ministrów
5. Minister Cyfryzacji
6. Minister Rozwoju i Technologii
7. Sekretarze Stanu w Ministerstwie Cyfryzacji
8. Członkowie Komisji Cyfryzacji, Innowacyjności i Nowych Technologii
9. Prezes Zarządu NASK
10. Przewodnicząca Rady Dialogu Społecznego
11. Przewodniczący Wojewódzkich Rad Dialogu Społecznego
12. Prezes Zarządu Związku Województw Rzeczpospolitej Polskiej
13. Prezes Zarządu Miast Polskich
14. Prezes Zarządu Związku Powiatów Polskich
15. Przewodniczący Zarządu Związku Gmin Wiejskich RP
16. Komisja Wspólna Rządu i Samorządu Terytorialnego
17. ACF Doradcy Samorządu sp. z o.o.