Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dnia 24 października 2022 r.
KIGEiT/1780/10/2022

Sz. P. Janusz Cieszyński
Sekretarz stanu,
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Kancelaria Prezesa Rady Ministrów
ul. Królewska 27, 00-060 Warszawa

Dotyczy: *projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa produktów z elementami cyfrowymi oraz zmieniającego rozporządzenie (UE) 2019/1020*

Szanowny Panie Ministrze,

działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (zwanej dalej „KIGEiT" lub „Izbą"), niniejszym przedstawiam uwagi do projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa produktów z elementami cyfrowymi oraz zmieniającego rozporządzenie (UE) 2019/1020.

I. Uwagi ogólne.

1.1. Wykluczenie dostawców i produktów z rynków Państwa Członkowskich i UE

W art. 46 Aktu dot. Cyberodporności (dalej „**CRA**") określono procedurę, w ramach której poszczególne państwa członkowskie mogą usuwać z rynku produkty. Komisja Europejska będzie musiała zostać o tym powiadomiona i uruchomi proces oceny ryzyka (z pomocą ENISA), który może skutkować usunięciem tych produktów z całego rynku Unii Europejskiej, jeżeli stwarzają one „*istotne zagrożenie cyberbezpieczeństwa*" i stanowią zagrożenie dla podmiotów objętych dyrektywą NIS2 lub „*ochrony interesu publicznego*". Nasze poważne wątpliwości odnoszą się do pojęcia „*istotnego zagrożenia cyberbezpieczeństwa*" (ang. „*a significant cybersecurity risk*"), z tej przyczyny, że równolegle w NIS2 przy ocenie takiego zagrożenia bierze się pod uwagę czynniki nietechniczne, podlegające dużej arbitralności i dyskrecjonalności organu, nawet w sytuacji gdy z technicznego punktu widzenia produkt będzie całkowicie bezpieczny. Nasze obawy zatem budzi szeroki zakres interpretacji tego pojęcia. W tym zakresie dostrzegamy ryzyko fragmentacji jednolitego europejskiego rynku z uwagi na wykluczenie z niektórych rynków niektórych producentów i jednoczesne pozostawienie ich na pozostałych, lub też nakładanie przez Komisję Europejską decyzji o konieczności usunięcia produktów z danego rynku, nawet jeśli dane Państwo Członkowskie nie zgadza się z taką oceną. Co więcej sprzeciwiamy się w tym zakresie by niewiążący dokument o charakterze politycznych rekomendacji (5G Toolbox) był wykorzystany jako punkt odniesienia dla takiej oceny ryzyka, co znacząco zwiększa poziom arbitralności interpretacji pojęcia „*istotnego zagrożenia cyberbezpieczeństwa"*. Uważamy, że rozwiązania związane z ograniczeniami na rynku jednolitym powinny być stosowane wyłącznie wtedy, gdy istnieje poważne i uzasadnione ryzyko związane z cyberbezpieczeństwem oparte na technicznej ocenie.

Warto podkreślić, że mniejsza liczba dostawców na rynku UE, spowodowana wdrożeniem mechanizmów, o których mowa w art. 46 CRA, wbrew pozorom, może zmniejszyć poziom

cyberbezpieczeństwa, a nie go zwiększyć. Różnorodność dostawców utrudnia bowiem atakującym wykorzystanie luk w zabezpieczeniach (zob. motyw 58 CRA). Uzasadnione jest zatem wpieranie reguł wolnego rynku jako optymalnego środka do zapewnienia bezpieczeństwa produktów na terytorium Unii. Wyeliminowanie znaczącego dostawcy z rynku UE może również wywołać poważne negatywne konsekwencje, takie jak (i) brak współpracy w zakresie testowania interoperacyjności, przekładające się wprost na zwiększenie podatności na zagrożenia (ii) powstanie niekorzystnej sytuacji z punktu widzenie przepisów antymonopolowych (monopolu, duopolu lub oligopolu), skutkujących zawyżonymi cenami (iii) stosowanie tzw. klauzul wyłączności lub najwyższego uprzywilejowania w umowach z wykonawcami lub podwykonawcami przez poszczególne Państwa Członkowskie, co bezpośrednio niweczyć będzie ideę jednolitego rynku.

1.2. Relacje z NIS 2 wymagają ponownej analizy (stosowanie kryteriów nietechnicznych)

Dyrektywa NIS2 i CRA są ze sobą ściśle powiązane, ponieważ produkty używane przez podmioty niezbędne (odpowiedzialne za infrastrukturę krytyczną) w ramach Dyrektywy NIS2 również wchodzą w zakres CRA (zob. art. 6 ust. 2 lit. (b) CRA). Wszelkie zasadnicze wymogi w Dyrektywie NIS2 i CRA powinny jednak opierać się na technicznych ocenach czynników ryzyka, a nie na nadmiernym wpływie państwa trzeciego na dostawców (zob. motyw 33 CRA). Wszelkie wymagania w tym zakresie nie powinny zachęcać do dyskryminacji dostawców ze względu na upolitycznione przesłanki – takie rozwiązania nie powinny być oparte na kraju pochodzenia, ale raczej koncentrować się na samym produkcie lub urządzeniu. Poleganie na nieprecyzyjnych, a także wysoce politycznych i arbitralnych kryteriach może prowadzić do spadku tempa innowacji w Unii Europejskiej. Jak już wskazano, idea takiej wysoce dyskrecjonalnej oceny politycznej znajduje odzwierciedlenie w art. 46 CRA, który odnosi się do produktów, które stwarzają „*istotne zagrożenie cyberbezpieczeństwa*", mimo że są zgodne z Aktem Cyberodporności, gdy: *„stanowią one znaczne zagrożenie dla bezpieczeństwa cybernetycznego, a ponadto stwarzają zagrożenie dla zdrowia lub bezpieczeństwa osób, dla wypełnienia obowiązków wynikających z prawa unijnego lub krajowego mających na celu ochronę praw podstawowych, autentyczności dostępności integralności lub poufności usług oferowanych przy użyciu elektronicznego systemu informacyjnego przez istotne podmioty typu, o którym mowa w załączniku I do Dyrektywy NIS2, lub dla innych aspektów ochrony interesu publicznego".*

Pragniemy podkreślić, że poleganie na kryteriach politycznych takich jak „*inne aspekty ochrony interesu publicznego*" czy stworzenie „*zagrożenia dla bezpieczeństwa osób"* doprowadzi do zmniejszenia uczciwej konkurencji i poziomu bezpieczeństwa. Wszelkie takie kryteria mogą skutkować używaniem urządzeń lub produktów znacznie mniej bezpiecznych pochodzących od dostawcy, który przeszedł pozytywnie „*test polityczny*", podczas gdy bezpieczeństwo jego produktów może pozostawiać wiele do życzenia. W naszej ocenie wskazane byłoby również w tym zakresie, oprócz zmiany art. 46 CRA oraz ponownej analizy relacji z Dyrektywą NIS2, usunięcie odniesień do zestawu narzędzi UE dotyczących cyberbezpieczeństwa 5G (5G Toolbox) w motywie 33, ponieważ odnoszą się on do tzw. *soft law* i nie stanowią wiążącego prawa Unii Europejskiej. Rozumiemy, że interesy polityczne i gospodarcze powinny mieć zasadnicze znaczenie dla prawodawstwa w Unii Europejskiej. Mimo to Unia Europejska już wdrożyła kilka narzędzi umożliwiających dynamiczne i elastyczne reagowanie na sytuację międzynarodową (por. rozporządzenie (UE) nr 833/2014 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainę, czy przyjęte już osiem pakietów sankcji przeciwko Rosji). To właśnie takie regulacje, odwołujące się do konkretnych zagrożeń, jest proporcjonalne i właściwe. Apelujemy zatem, aby przepisy techniczne miały charakter techniczny, a przepisy polityczne miały

charakter polityczny – mieszanie tych dwóch reżimów przyniesie tylko szkody dla jednolitego rynku Unii Europejskiej i rozwoju innowacyjności.

1.3. Zduplikowane wymagania

Przyjęcie Aktu ds. Cyberodporności daje ogromną szansę zmniejszenia różnych, często sektorowych i silosowych podejść do cyberbezpieczeństwa produktów oraz harmonizację otoczenia regulacyjnego w ramach jednego horyzontalnego, spójnego punktu odniesienia. W naszej ocenie szansa ta nie została w pełni wykorzystana. Zwracamy uwagę, że konieczne jest doprecyzowanie relacji i powiązań między CRA a certyfikacją cyberbezpieczeństwa na podstawie Rozporządzenia (UE) 2019/881 (Akt o cyberbezpieczeństwie), Aktu w sprawie sztucznej inteligencji, Rozporządzenia eIDAS oraz DORA. Wszystkie te akty powinny umożliwiać harmonizację i interoperacyjność. Nawet dużym podmiotom, z rozbudowanymi zasobami prawnymi i technicznymi, coraz trudniej zidentyfikować jest i ocenić wszystkie skutki różnych regulacji. Może to prowadzić do braku interoperacyjności systemów i produktów w całej UE oraz ryzyka niezgodności dla producentów i dostawców.

Ewidentnym przykładem pokrywania się wymagań jest art. 6 ust. 2 lit. (b) i ust. 5 lit. (b) CRA. Podmioty niezbędne w ramach NIS2 korzystające z produktów cyfrowych w swoim łańcuchu dostaw będą musiały spełnić wymogi CRA, przy jednoczesnym zachowaniu zgodności z NIS2. W praktyce zatem, taki podmiot, musi upewniać się za każdym razem czy wykorzystywane przez niego produkty są zgodne z tymi wymaganiami, podczas gdy ideą jest przecież harmonizacja wymagań (por. wyjaśnienie podstaw prawnych, zasady subsydiarności i proporcjonalności w projekcie CRA).

W naszej ocenie CRA powinno przede wszystkim opierać się na podejściu opartym na współpracy, umożliwiając globalną współpracę i interoperacyjność – w tym zakresie CRA powinno bazować na Nowych Ramach Prawnych (New Legislative Framework (NLF)). Celem CRA powinno być wspieranie zmniejszania złożoności między różnymi sektorowymi politykami regulacyjnymi poprzez wprowadzenie zrównoważonych regulacji horyzontalnych i stosowanie zharmonizowanych norm międzynarodowych w przepisach UE dotyczących produktów. Jeżeli istnieją normy krajowe, należy je dostosować do norm międzynarodowych. Ponieważ normalizacja ICT ma już charakter globalny, istniejącą infrastrukturę normalizacyjną można wykorzystać przy zaangażowaniu wszystkich zainteresowanych stron (ISO/IEC JTC1, CEN/CLC/JTC 13, ETSI TC CYBER). Akt ds. Cyberodporności, w naszej ocenie, w zbyt małym stopniu opiera się już na istniejących ramach dotyczących zgodności produktów (NLF) i wymaga dalej idących zmian.

1.4.Nieadekwatny zakres Rozporządzenia

Uważamy, że zakres CRA został określony zbyt szeroko. W czasach rosnących cen, zaburzenia łańcucha dostaw i zbliżającego się kryzysu ekonomicznego i energetycznego, w naszej ocenie należy znaleźć równowagę lub kompromis pomiędzy wyższym bezpieczeństwem, a lepszą wydajnością i innowacją na rynku (zob. art. 3 ust. 1, 3, 4 i 14 CRA). Arbitralne egzekwowanie prawa i obciążanie sektora może wywołać efekt domina w stosunku do cen i kosztów, rozlewając się także na inne sektory gospodarki Unii Europejskiej. W tym zakresie podkreślamy także że lista krytycznych produktów (klasa 2) w załączniku 3 powinna zostać zawężona, a nie odnosić się do bardzo ogólnych kategorii produktów – w zasadzie obejmujących każdy komponent systemu lub urządzenia (np. systemy operacyjne dla serwerów, komputerów stacjonarnych i urządzeń mobilnych, routery, modemy przeznaczone do połączenia z Internetem i przełączniki przeznaczone do użytku przemysłowego).

Dostrzegamy również negatywny wpływ uciążliwych dla sektora obowiązków dotyczących produktów, w tym nowe standardy i wymagania, takie jak Software Bill of Materials (SBOM – patrz art. 3 pkt 37 CRA), a także dotyczących obsługi luk w zabezpieczeniach i zgłaszania

incydentów. Kwestie te wymagają wyjaśnienia i ustalenia, czy regulacje aby na pewno się nie pokrywają. W naszej ocenie paradygmatem powinna być proporcjonalność i zwiększanie pewności biznesowej i prawnej (zob. motyw 37, 63 i art. 3 (37) i art. 11) CRA), a nie nakładanie nowych obciążeń. W tym zakresie absolutnym minimum jest usunięcie odwołania do SBOM w załączniku I, cz. 2 z uwagi na nadmierność i nieproporcjonalność obciążenia.

1.5. Zakres krytycznych produktów, kategorii i specyfikacji (wymóg zapewnienia niedyskryminacji i zapewnienia równych warunków działania dla dostawców spoza UE)

Art. 6 ust. 2 CRA przyznaje Komisji w akcie delegowanym uprawnienia do włączenia nowego typu do wykazu kategorii produktów krytycznych lub wycofania istniejącego. W tym celu Komisja musi określić poziom ryzyka cyberbezpieczeństwa zgodnie z kryteriami wskazanymi w lit. (a) tego przepisu. Kryteria te w sposób bardzo szeroki odnoszą się do kwestii zarządzania dostępem i kontroli nad technologią. Natomiast w lit. (e) określono również, że zakres, w jakim korzystanie z produktów z elementami cyfrowymi spowodowało już materialną lub niematerialną stratę lub zakłócenia lub wzbudziło poważne obawy dotyczące materializacji negatywnego wpływu, stanowi kryterium dodania lub usunięcia produktów do załącznika nr III. Takie uprawnienia pozwalają Komisji Europejskiej na rozszerzenie zakresu obowiązywania CRA bez jakiejkolwiek kontroli, powodując dodatkową niepewność po stronie nie tylko dostawców, ale całego sektora. Podkreślamy, że z punktu widzenia zasad prawidłowej legislacji oraz podstawowych zasad prawnych Unii Europejskiej materia taka powinna zostać uregulowana bezpośrednio w rozporządzeniu, a nie w akcie delegowanym Komisji Europejskiej. Takie podejście ma również wymierny efekt ekonomiczny i innowacyjny, zmniejsza niepewność, kluczową w sektorach badawczo-rozwojowym, innowacyjnym i cyfrowym.

Ponadto, zwracamy uwagę, że prawodawca unijny w tym przepisie stosuje bardzo niejasne sformułowania, np. „*obawy*" lub „*podwyższone przywileje*" (ang. *elevated privilege*) i „*istotne obawy*", co może prowadzić do różnych interpretacji i uznaniowości, nieograniczonych standardowymi mechanizmami kontroli demokratycznej. Komisja Europejska przyznała sobie bowiem uprawnienia do rozszerzenia zakresu produktów krytycznych przy użyciu kryteriów obejmujących produkty, które „budzą poważne obawy" (wysoka zdolność do upolitycznienia), a także produkty w „warunkach przemysłowych" (dowolne określanie zakresu). Te same obawy pojawiają się w art. 6 ust. 2 lit (e), w którym prawodawca UE stosuje „znaczące ryzyko cyberbezpieczeństwa" w odniesieniu do produktów krytycznych (zdefiniowanych w NIS2 w odniesieniu do czynników nietechnicznych). Takie arbitralne podejście może prowadzić do fragmentacji jednolitego rynku (por. pkt 1.2 i 1.3. niniejszego stanowiska).

1.6. Ocena zgodności

Naszym zdaniem producenci powinni mieć możliwość decydowania o odpowiednim dla siebie poziomie zaufania, a wszelkie zapewnienia powinny być oparte na systemie dobrowolności. Stoimy na stanowisku, że to od samych producentów zależy dostosowanie się do wymogów bezpieczeństwa, których wolny rynek zawsze będzie wiarygodnym weryfikatorem. Oczywiście nie kwestionujemy potrzeby wdrażania określonych standardów, ale nie powinny one być tak szerokie, jak te przyjęte w CRA. Podkreślamy, że wszelkie wyższe wymagania dotyczące oceny zgodności powinny mieć wyłącznie charakter techniczny.

1.7.Wymagania dotyczące pełnego cyklu życia

Obawiamy się, że wymagania w zakresie całego cyklu życia produktu, mogą prowadzić do nieefektywności ekonomicznej. Producenci zainwestują znaczne kwoty w zapewnienie odpowiedniego poziomu bezpieczeństwa przez cały cykl życia produktu, zamiast koncentrować się na innowacjach. W naszej ocenie ciężar regulacji powinien zostać raczej

przeniesiony na możliwość określenia całego cyklu życia produktu i przejrzystych sposobów komunikacji użytkownikom końcowym. Niezbędnym jest ustanowienie samooceny jako standardowej procedury zgodności, podobnie jak w ramach NFL. W obecnej sytuacji gospodarczej dodatkowe koszty przestrzegania przepisów powinny być jak najniższe i nie prowadzić do nowej niepewności prawnej w sektorze, w szczególności, gdy koszt ten poniesie ostatecznie użytkownik lub nabywca danego produktu.

1.8. Uprawnienia do wpływania i kształtowania ocen zgodności

Art. 6 ust. 5 CRA umożliwia Komisji Europejskiej określanie kategorii produktów wysoce krytycznych, w przypadku których producenci będą musieli uzyskać europejski certyfikat cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa, zgodnie z Aktem o cyberbezpieczeństwie (Rozporządzenie PE i Rady (UE) 2019/881) w celu wykazania zgodność z zasadniczymi wymaganiami. Określając takie kategorie, Komisja weźmie pod uwagę (1), czy podmioty objęte Dyrektywą NIS2 będą korzystać z kategorii produktu lub będą z niego korzystać w przyszłości (tak lit. (a) tego przepisu) oraz (2) czy kategoria produktu wpływa na łańcuch dostaw (tak lit. (b) tego przepisu). W naszej ocenie jednak, w przypadku braku odpowiednich określonych przepisów, Komisja Europejska powinna opierać na międzynarodowych standardach i normach (np. ISO). Takie postanowienie powinno zostać dodane, również w przypadku krytycznych produktów.

Chcielibyśmy również wskazać, iż w art. 18 ust. 4 CRA Komisja Europejska powinna jako zasadę móc wymagać od producentów przedstawienia unijnego certyfikatu cyberbezpieczeństwa a tylko w wyjątkowych przypadkach przeprowadzana powinna być ocena zgodności przez stronę trzecią (zob. motyw 39).

II. Kluczowe propozycje

Poza ogólnymi uwagami, przedstawiamy następujące propozycje, które naszym zdaniem powinny zostać wdrożone w celu ulepszenia proponowanej regulacji:

1. <u>Zmniejszenie arbitralności i dyskrecjonalności oceny produktów poprzez zwiększenie precyzji proponowanej regulacji:</u>
   a. **Artykuł 6 ust. 2**: **CRA**: Wnosimy o ponowną analizę wykorzystywanych pojęć, takich jak „*istotne obawy związane z wystąpieniem negatywnego wpływu*" z uwagi na ich niejasny i ogólny charakter, skutkujący nieproporcjonalnie szerokim zakresem kompetencji i zestawem środków Komisji Europejskiej. Przede wszystkim w tym zakresie wnosimy o usunięcie fragmentu „*or has given rise to significant concerns in relation to the materialisation of an adverse impact"* z art. 6 ust. 2 lit. (e) CRA z uwagi na jego wysoką arbitralność.
   b. **Artykuł 6 CRA**: Komisja Europejska powinna opierać się na międzynarodowych standardach i normach (np. ISO) i ten zapis powinien zostać dodany, nawet w przypadku produktów krytycznych (art. 6 ust. 5 CRA).
   c. **Artykuł 6 CRA**: Komisja Europejska przyznała sobie uprawnienia do rozszerzenia zakresu produktów krytycznych przy użyciu kryteriów obejmujących produkty, które „*budzą poważne obawy*", a także produkty „*w warunkach przemysłowych*". Tak szeroką delegację należy usunąć ze względu na jej dowolność i arbitralność w interpretacji.
   d. **Rozdział II CRA:** Producenci powinni na podstawie samooceny decydować o odpowiednich środkach, zgodnie z systemem NFL. Warto również byłoby podkreślić w całym rozdziale, konieczność niedyskryminacji, także w ujęciu narodowościowym.

e. **Artykuł 46 CRA:** Postanowienie powinno zostać przeredagowane w taki sposób ,aby zgodnie z zasadą proporcjonalności i subsydiarności ograniczyć szerokie uprawnienia Komisji Europejskiej o uznaniowych charakterze, które zwiększają ryzyko całkowitego upolitycznienia cyberbezpieczeństwa, bez uwzględnienia przesłanek o charakterze technicznym.

2. Ponownie zweryfikować zakres i zasadność uprawnień do usuwania z rynku produktów zgodnych z wymaganiami:

a. W art. 46 CRA zawarto mechanizm umożliwiający Państwom Członkowskim i Komisji Europejskiej uruchomienie procesu usuwania produktów zgodnych z Aktem ds. Cyberodporności, jeśli niosą ze sobą „znaczne zagrożenie cyberbezpieczeństwa" i stanowią zagrożenie dla podmiotów NIS2 lub „ochrony interesu publicznego". Przepisy w tym zakresie powinny zawierać jednak zabezpieczenia, by instrument nie był nadużywany, a sam mechanizm wykluczenia był proporcjonalny i niedyskryminacyjny.

3. Szeroki zakres regulacji powoduje nieefektywność rynku i zwiększa koszty:

a. W czasach rosnących cen oraz kryzysu ekonomicznego i energetycznego należy znaleźć równowagę pomiędzy wyższymi wymaganiami, a lepszą wydajnością i innowacją na rynku UE. Arbitralne egzekwowanie prawa i obciążenie branży mogą wywołać efekt domina w zakresie cen i kosztów, powiększając jeszcze niepokojące zjawiska związane z brakiem surowców energetycznych. Szeroki zakres regulacji będzie stanowić również obciążenie dla MŚP i przemysłu, dlatego też wymagania należy zminimalizować, a producenci powinni mieć możliwość samodzielnego ustalania poziomu zaufania. Ponadto, wskazane byłaby ponowna analiza przepisów CRA pod kątem dostosowania ich do zakresu Aktu o Cyberbezpieczeństwie.

4. Obecne kryteria zmniejszają różnorodność dostawców i cyberbezpieczeństwo:

a. Arbitralne kryteria, takie jak te oparte na „*kraju pochodzenia*", otwierają drzwi dla wymogów, które mogą podlegać interpretacji politycznej przez państwa członkowskie. Zestaw narzędzi 5G (5G Toolbox) przyczynił się nie tylko do rozdrobnienia, ale także do dyskryminacji ze względu na kraj pochodzenia i nie jest zgodny z *acquis communautaire*. Zmniejsza to różnorodność dostawców i w rezultacie sprawia, że Unia Europejska i jej obywatele będą mniej bezpieczni.

5. Zmniejszenie niepewności w ocenie zgodności:

a. Komisja powinna zezwolić zarówno na unijne schematy cyberbezpieczeństwa, jak i na własną deklarację zgodności z podobnymi lub równoważnymi normami międzynarodowymi. Zasadą powinno być wymaganie od producentów przedstawienia unijnego certyfikatu cyberbezpieczeństwa zamiast indywidualnych zwolnień z oceny zgodności przez stronę trzecią (klasa I) i podejmowania decyzji, czy jest to wystarczające.

b. W zakresie art. 24 CRA istnieje znacząca niepewność prawna związana z definicją „*produktów krytycznych*" jako że odesłanie do Dyrektywy NIS2 powoduje nie jest wiadome, które produkty będą wymagały wysokiego uzasadnienia zaufania (ocena zgodności przez stronę trzecią). Ponadto Komisja Europejska nadała sobie uprawnienia do definiowania dodatkowych kategorii produktów w tym zakresie, a także dodawania nowych, co naturalnie powoduje znaczącą niepewność po stronie sektora.

6. Zminimalizowanie wymagań stawianych deweloperom, start-upom, MŚP itp.:
   a. Chociaż MŚP (a także deweloperzy aplikacji, start-upy) powinny wdrażać również wysokie wymagania w zakresie bezpieczeństwa, niezbędne jest zapewnienie im wsparcia umożliwiającego im konkurowanie. Niezbędne jest uniknięcie nadmiernie nakazowych wymogów technicznych i utrzymanie horyzontalnego charakteru CRA, a jednocześnie usunięcie wszelkich możliwości włączenia przez państwa członkowskie kryteriów nietechnicznych, z uwagi na ryzyko zaburzeń na jednolitym rynku europejskim. Innym rozwiązaniem byłoby również niewłączanie do zakresu regulacji obszarów i produktów niekrytycznych lub samodzielnego oprogramowania (nie jest bowiem wiadome, czy MŚP będą w stanie spełnić wymogi wynikające z CRA).
7. Weryfikacja odesłań do NIS2 i zapewnienie spójności legislacji europejskiej:
   a. W świetle możliwych zakłóceń na jednolitym rynku spowodowanych wdrożeniem NIS2, wskazane byłoby usunięcie art. 6 ust. 5 CRA, z uwagi na pokrywanie się regulacji NIS2 i CRA w tym zakresie. Podmioty niezbędne w ramach NIS2 korzystające z produktów cyfrowych w swoim łańcuchu dostaw powinny móc spełniać wymogi CRA, podczas gdy jednocześnie NIS 2 zawiera własne wymogi w tym zakresie. Efektem będzie niepewność regulacyjna i ryzyko politycznych ocen związanych z cyberbezpieczeństwem.
8. Zachowanie tzw. Efektu Brukselskiego:
   a. Zgodnie z proponowanym brzmieniem Aktu ds. Cyberodporności, Komisja Europejska mogłaby wskazać nowe kategorie produktów do zakresu i zastosować elastyczne kryteria uzasadnienia decyzji, np. „*biorąc pod uwagę poważne obawy związane z materializacją negatywnego wpływu*". Jak już podkreślano odesłanie do zestawu narzędzi 5G (5G Toolbox) oznacza również dalsze pole do nieuzasadnionego upolitycznienia kwestii cyberbezpieczeństwa. Wykluczenie i nieuzasadnione upolitycznienie oceny cyberbezpieczeństwa tylko ograniczają autonomię strategiczną i szkodzą przywództwu UE, jako twórcy zasad ogólnoświatowych, z poszanowaniem neutralności i praworządności. Wskazane byłoby raczej oparcie się na międzynarodowych standardach w obszarze cyberbezpieczeństwa i zapewnienie wysokiego poziomu przejrzystości niż opieranie się na dyskrecjonalnych procedurach.

Jednocześnie, zgodnie z prośbą otrzymaną w toku konsultacji wewnątrz-izbowych od jednego z członków Izby, firmy EXATEL S.A., informuję o wyłączeniu poparcia tej firmy dla treści powyższego stanowiska

z poważaniem

Prezes Zarządu

Stefan Kamiński

Signature Not Verified
Dokument podpisany przez Stefan Kamiński
Data: 2022.10.24 13:37:10 CEST
Powód: Złożenie podpisu