Warszawa, 22 lipca 2024 roku

Szanowny Pan Zbigniew Muszyński
Dyrektor Rządowego Centrum Bezpieczeństwa
robert.tyszkiewicz@rcb.gov.pl
sekretariat@rcb.gov.pl
poczta@rcb.gov.pl

Szanowni Państwo,

Polska Izba Komunikacji Elektronicznej (dalej również „Izba" lub „PIKE") przedstawia stanowisko konsultacyjne w sprawie projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47, dalej „Projekt").

Na wstępie Izba zwraca się o prace nad ustawą w duchu zrozumienia wyzwań stojących przed podmiotami krytycznymi. Ustawa wprowadza szereg wymogów organizacyjnych i technicznych. Odpowiednie zorganizowanie struktur wewnętrznych podmiotów krytycznych, jak również przygotowanie dokumentacji i wdrożenie wymogów wskazanych w Projekcie, będzie zadaniem długotrwałym oraz kosztownym. Ustalony w ustawie zbyt krótki okres przygotowawczy bezpośrednio wpłynie na wzrost kosztów wdrożenia.

Zwracamy również uwagę, że problemem podmiotów krytycznych będzie brak w Polsce odpowiedniej ilości specjalistów, którzy mogą przygotować je do zgodności z Projektem. Z tym wyzwaniem będą się mierzyć wszystkie podmioty krytyczne przygotowujące się do stosowania ustawy w brzmieniu zmienionym Projektem.

Infrastruktura krytyczna stanowi fundament funkcjonowania nowoczesnych społeczeństw, obejmując zarówno sektor publiczny, jak i prywatny. W obecnych regulacjach prawnych dotyczących budowy i utrzymania infrastruktury krytycznej istnieją luki, które uniemożliwiają pełne zabezpieczenie oraz efektywne zarządzanie tą infrastrukturą. Dlatego Izba zachęca do szerszego przeglądu przepisów obejmujących to zagadnienie. Kluczowe obszary wymagające uregulowania to ustawa Prawo budowlane, ustawa o planowaniu i zagospodarowaniu przestrzennym oraz ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych.

Aktualne przepisy ustawy Prawo budowlane nie uwzględniają specyfiki infrastruktury krytycznej, którą dysponują przedsiębiorcy prywatni, jak i przedsiębiorcy telekomunikacyjni. Istnieje potrzeba wprowadzenia przepisów, które umożliwią lepszą ochronę oraz zarządzanie infrastrukturą krytyczną, niezależnie od jej właściciela. Obejmuje to min. wprowadzenie uproszczonych i przyspieszonych procedur dla inwestycji dotyczących infrastruktury krytycznej.

Obecne regulacje koncentrują się na uzgadnianiu miejscowych planów zagospodarowania przestrzennego z podmiotami publicznymi, pomijając przedsiębiorców prywatnych dysponujących infrastrukturą krytyczną lub planujących jej budowę. Proponujemy wprowadzenie obowiązku

uzgadniania planów zagospodarowania przestrzennego z przedsiębiorcami prywatnymi posiadającymi infrastrukturę krytyczną oraz umożliwienie przedsiębiorcom prywatnym wpływu na planowanie przestrzenne w celu zapewnienia ochrony i ciągłości funkcjonowania infrastruktury krytycznej.

W zakresie ustawy o wspieraniu rozwoju usługi i sieci telekomunikacyjnych, chociaż ustawa ta wprowadza ułatwienia dla budowy infrastruktury telekomunikacyjnej szerokopasmowej, pomija inne typy infrastruktury telekomunikacyjnej zaliczane właśnie do infrastruktury krytycznej, takie jak infrastruktura radiolokacyjna czy radionawigacyjna.

Kompleksowe uregulowanie kwestii budowy i utrzymania infrastruktury krytycznej w przepisach prawa jest niezbędne dla zapewnienia jej bezpieczeństwa oraz przyśpieszenia jej budowy. Uwzględnienie specyfiki przedsiębiorców prywatnych w przepisach takich jak ustawa Prawo budowlane, ustawa o planowaniu i zagospodarowaniu przestrzennym oraz ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych przyczyni się do lepszego zarządzania tą infrastrukturą i zapewnienia ciągłości jej funkcjonowania.

Poniżej przedstawiamy szczegółowe uwagi dotyczące przedstawionego projektu ustawy:

1. **[art. 6l ust. 1 pkt 5]**

   Zwracamy się o doprecyzowanie wymogu zapewnienia zdolności do ochrony informacji niejawnych, przez wskazanie, że zdolność ta powinna obejmować zdolność ochrony informacji zastrzeżonych. Brak ustalenia odpowiedniego poziomu w ustawie rodzi ryzyko ponoszenia zbędnych kosztów przez podmioty krytyczne.

   Wprowadzenie zdolności ochrony informacji zastrzeżonych będzie spójne z poziomem ochrony informacji o wpisie na listę infrastruktury krytycznej.

2. **[art. 6z ust. 2 pkt 1 oraz art. 6za ust. 2]**

   W wyżej wskazanych przepisach projektodawca faktycznie zobowiązuje podmioty krytyczne do wdrożenia norm PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301.

   Zdaniem Izby, wskazywanie w ustawie konkretnych norm, również tych dotyczących zapewnienia bezpieczeństwa, jest niewłaściwym podejściem do regulacji.

   Po pierwsze, może się zdarzyć, że nawet w ramach jednego systemu normalizacyjnego, zagadnienia regulowane w konkretnych normach będą (szerzej lub inaczej) regulowane w innych normach, co doprowadzi do nieaktualnych przepisów rangi ustawowej. Co więcej, normy są regularnie aktualizowane, co prowadzi do sytuacji w której podmiot prywatny, czyli organizacja tworząca normy ISO staje się de facto uprawniona do nakładania obowiązków na polskie podmioty krytyczne.

   Po drugie, wskazane przez Projektodawcę normy nie są jedynym zbiorem zasad. Istnieją również inne normy, które mogą prowadzić do osiągnięcia celu jakości, jak stosowanie norm ISO.

PIKE zwraca się o modyfikację przepisów w ten sposób, że podmiot krytyczny ma obowiązek stosować normy PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301 lub normy im równoważne.

3. **[art. 6z ust. 2 pkt 1]**

   Izba zwraca się o modyfikację art. 6z ust. 2 pkt 1 w ten sposób, że podmiot krytyczny w ogóle nie powinien być zobowiązany do odnoszenia się do Polskich Nom PN-EN 50131, PN-EN 60839 lub PN-EN 62676.

   Zobowiązanie do stosowania ww. norm, w sposób nieproporcjonalny i poza przeprowadzoną analizą ryzyka, zobowiązuje do stosowania konkretnych środków bezpieczeństwa. Prowadzi to do wzrostu kosztów związanych z koniecznością dostosowania i wymiany systemów do wymogów oraz ich utrzymania, w sposób nie wynikający w żaden sposób z prowadzonej przez podmioty krytyczne analizy ryzyka.

   Zwracamy także uwagę na legislacyjną wadliwość art. 6z ust. 2 pkt 1. Obecna treść rodzi wątpliwości czy wyliczenie stanowi koniunkcję czy alternatywę łączną i w jakim zakresie.

   W tym miejscu warto zwrócić uwagę, na specyfikę branży telekomunikacyjnej oraz infrastruktury telekomunikacyjnej jako infrastruktury krytycznej. Infrastruktura telekomunikacyjna jest infrastrukturą rozproszoną – w odróżnieniu od np. infrastruktury krytycznej w branży naftowej. Z tego powodu nie można wprowadzać takich samych wymogów dla wszystkich podmiotów krytycznych. Każdy podmiot krytyczny, po przeprowadzeniu analizy, powinien wdrażać odpowiednie i proporcjonalne środki zapewnienia ochrony.

4. **Modyfikacja projektu w ten sposób, aby wszystkie obowiązki nakładane na przedsiębiorców były wskazane w przepisach rangi ustawowej.**

   Izba w szczególności wskazuje procedurę przyjęcia Krajowej Oceny Ryzyka, Krajowego Planu Zarządzania Kryzysowego oraz Strategię Odporności Podmiotów Krytycznych, które mają być przyjmowane w drodze uchwały Rady Ministrów. Nie będą zatem przepisami rangi ustawowej. Nie będą nawet źródłami prawa powszechnie obowiązującego – gdyby to były np. rozporządzenia. Jednocześnie dokumenty te, pośrednio lub bezpośrednio, będą nakładały obowiązki na podmioty krytyczne.

   Ponadto niedopuszczalne jest ustalanie kryteriów pozwalających zidentyfikować obiekty, urządzenia oraz instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi jako infrastrukturę krytyczną (art. 6f ust. 1) również w uchwale Rady Ministrów, czyli w akcie nie będącym nie tylko ustawą, lecz w ogóle nie będącym aktem prawa powszechnie obowiązującego.

   PIKE zwraca się o modyfikację przepisów w ten sposób, aby wszelkie obowiązki nakładane na podmioty krytyczne znalazły się w przepisach rangi ustawowej, zaś w rozporządzeniach tylko ich ewentualne doszczegółowienie.

5. **[art. 6z ust. 1 i 4]**

Prowadzenie systematycznej oceny ryzyka z pewnością jest jednym z najefektywniejszych środków mitygacji już zidentyfikowanych ryzyk, jak i wprowadzanie do analizy nowych. Ocena ryzyka, jeżeli jest wykonywana rzetelnie, jest czynnością czasochłonną i angażującą znaczne środki – osobowe oraz finansowe.

Po pierwsze, zwracamy się, aby pierwsza ocena ryzyka, o której mowa w art. 6z ust. 1, odbywała się w terminie 18 miesięcy po wpisie do wykazu podmiotów krytycznych. Obawiamy się, że proponowany termin 9 miesięcy jest zbyt krótki, mając na uwadze okoliczność, że podmiotami krytycznymi mogą być przedsiębiorstwa o znacznej skali prowadzonej działalności. Obowiązek analizy ryzyka, uwzględniający m.in. stopień zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, prowadzi do znacznej rozbudowy prowadzonej analizy, co przełoży się na czas jej prowadzenia.

Zwracamy się również o zawężenie zakresu analizy wyłącznie do usług kluczowych świadczonych przez podmiot krytyczny, z pominięciem wpływu innych usług kluczowych. Podmiot krytyczny może nie posiadać wystarczającej wiedzy o usługach kluczowych świadczonych przez inne podmioty oraz informacji o ryzykach funkcjonowania tych usług.

6. **[art. 6za ust. 1]**

Izba zwraca się o wprowadzenie odpowiedniego terminu na przygotowanie przez podmiot krytyczny dokumentacji, o której mowa w art. 6za ust. 1. Wykonanie przedmiotowej dokumentacji to nie tylko znaczący koszt, lecz również odpowiedni czas niezbędny na przygotowanie dokumentacji.

Zwracamy się o wyznaczenie co najmniej 6-miesięcznego terminu na przygotowanie dokumentacji, o której mowa w art. 6za ust. 1.

Aktualne pozostają uwagi dotyczące obowiązku stosowania Polskiej Normy PN-EN ISO/IEC 27001 oraz Polskiej Normy PN-EN ISO 22301. Zdaniem PIKE, ustawodawca powinien dopuścić stosowanie norm równoważnych.

7. **[art. 6zb ust. 1]**

Obsługa incydentów, zapewne nieprzypadkowo, została w Projekcie wskazana na pierwszym miejscu wśród obowiązków podmiotów krytycznych. Jest to jedno z najważniejszych zadań tych podmiotów – i co za tym idzie, wymaga znacznych przygotowań.

Zwracamy się o wprowadzenie okresu, po jakim obowiązek pełnej, zgodnej z ustawą, obsługi następował nie wcześniej niż 6 miesięcy po wpisie do wykazu podmiotów krytycznych.

8. **[art. 6zf ust. 1]**

   Projektodawca wprowadza obowiązek przeprowadzania przez podmiot krytyczny audytu zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. W dalszych przepisach wskazane są szczegółowe, bardzo wysokie wymagania względem samego audytu, jak również podmiotów uprawnionych do przeprowadzania audytu. Wymagania te prowadzą do bardzo wysokich kosztów prowadzonych audytów.

   Między innymi z tego powodu, obowiązek przeprowadzania audytów co trzy lata jest nadmiarowy. Zwracamy się o zmniejszenie częstotliwości obowiązkowych audytów i zobligowanie podmiotów krytycznych do przeprowadzania audytów co sześć lat.

9. **[art. 6zh]**

   Izba zwraca się o modyfikację przepisu w zakresie proceduralnym.

   Po pierwsze, ze względu na wysokie wymogi formalne stawiane „osobie do kontaktu", podmiot krytyczny powinien mieć więcej czasu na zatrudnienie odpowiedniej osoby. Wnosimy o ustalenie terminu na wyznaczenie „osoby do kontaktu" na 6 miesięcy od ujęcia w wykazie podmiotów krytycznych.

   Po drugie, zwracamy się o wprowadzenie do Projektu postanowienia wskazującego, że jeżeli osoba ta nie posiada jeszcze certyfikatu bezpieczeństwa uprawniającego do dostępu do informacji niejawnych o klauzuli „poufne", wystarczające jest zwrócenie się przez tę osobę do właściwych służb o przyznanie odpowiedniego certyfikatu. Praktyka pokazuje, że badanie przez właściwe służby jest często bardzo długotrwałe. Przedmiotowy wymóg w obecnym kształcie nie tylko może sparaliżować prace podmiotu krytycznego, lecz może również znacząco podnieść koszty zatrudnienia osób spełniających wskazane w projekcie warunki formalne.

10. **Vacatio legis (art. 35 ustawy nowelizującej)**

    Proponowany 14-dniowy termin vacatio legis jest bardzo krótki. Argumenty, że przepisy europejskie powinny być stosowane już od października 2024 roku nie może być kluczowy. Opóźnienia w pracach legislacyjnych (wdrażana dyrektywa jest z grudnia 2022 r.!) nie mogą prowadzić do tego, że koszt przyspieszonego wdrożenia przepisów zostaje przerzucony na przedsiębiorców – podmioty krytyczne.

    Szeroki zakres ustawy, skomplikowanie przepisów oraz wprowadzanie szeregu wymagań organizacyjno-technicznych uzasadniają wprowadzenie 6-miesięcznego vacatio legis.

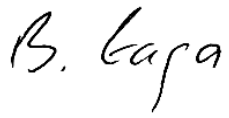
11. **Relacja z przepisami branżowymi (prawo komunikacji elektronicznej)**

    Zwracamy się do projektodawcy o konsekwentne wprowadzenie ochrony infrastruktury krytycznej również w innych przepisach.

    W szczególności podmioty krytyczne powinny móc odmawiać dostępu do infrastruktury krytycznej innym podmiotom. Do rozważenia przedstawiamy również obowiązki raportowe względem na przykład Prezesa UKE, określone w obecnie procedowanej

w Parlamencie ustawie Prawo komunikacji elektronicznej oraz w ustawie o wspieraniu rozwoju usług i sieci telekomunikacyjnych. Wyniki raportowania infrastruktury są publicznie dostępne. Wydaje się, że infrastruktura krytyczna powinna zostać wyłączona z obowiązków raportowych.

Z wyrazami szacunku,



Bogdan Łaga
Prezes Zarządu
Polska Izba Komunikacji Elektronicznej