Warszawa, 6 października 2020 r.

STANOWISKO SEKTOROWEJ RADY DO SPRAW KOMPETENCJI TELEKOMUNIKACJA I CYBERBEZPIECZEŃSTWO DOTYCZĄCE PROJEKTU ZMIAN W USTAWIE O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Komitet ds. rozwiązań legislacyjnych Sektorowej Rady Do Spraw Kompetencji Telekomunikacja i Cyberbezpieczeństwo przedstawia poniżej swoje stanowisko w sprawie projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (projekt z 7 września 2020 r.)

1. *Uwagi ogólne*

Rolą Sektorowej Rady ds. kompetencji Telekomunikacja i Cyberbezpieczeństwo jest przede wszystkim działanie na styku edukacji i praktyki w obu wskazanych dziedzinach. Obejmuje to m. in. rekomendowanie rozwiązań legislacyjnych w obszarze edukacji i dostosowanie do potrzeb rynku pracy oraz formułowanie rekomendacji dotyczących zapotrzebowania na kompetencje w danym sektorze. Z powyższych względów, w kręgu zainteresowania Rady są wszelkie rozwiązania legislacyjne, które mają wpływ na kształt rynku pracy oraz potrzeby edukacyjne w dziedzinie telekomunikacji i cyberbezpieczeństwa.

Sektorowa Rada do spraw Kompetencji Telekomunikacja i Cyberbezpieczeństwo uczestniczy w konsultacjach i wypracowuje rekomendacje zmian regulacji m.in. organizując konferencje naukowe ekspertów z administracji, biznesu i edukacji.

Debaty skupiają się na problemach kompetencji w ich podwójnym znaczeniu: „wiedzy i umiejętności" oraz „uprawnień i obowiązków" a także na elementach „siatki pojęciowej" w regulacjach, które dotyczą obu dziedzin.

Rada była głównym organizatorem konferencji „Leksykon cyberbezpieczeństwa" (31.07.2020), „Działalność w zakresie cyberbezpieczeństwa. Aspekty prawne, organizacyjne i techniczne", 7.08.2020 oraz „Potrzeby kompetencyjne w zakresie cyberbezpieczeństwa i łączności elektronicznej w świetle planowanych zmian w przepisach" (2.10.2020), podczas których omawiano m. in. kwestie związane z kwalifikacjami i kompetencjami w związku z projektem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Rezultatem konferencji są poniższe uwagi i propozycje do ww. projektu.

2. *Problemy definicyjne*

W pierwszej kolejności, Rada pragnie zwrócić uwagę na problemy związane z definiowaniem cyberbezpieczeństwa w różnych aktach prawnych.

W ustawie o krajowym systemie cyberbezpieczeństwa (UKSC) cyberbezpieczeństwo jest definiowane jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (art. 2 pkt 4). Definicja ta jest zbliżona do definicji „bezpieczeństwa sieci i systemów informatycznych" zawartej w art. 4 ust. 2 Dyrektywy NIS, które „oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne". Pomimo, że UKSC to implementacja Dyrektywy NIS to jednak powyższe, zasadnicze pojęcia są określane i definiowane w różny sposób.

W akcie o cyberbezpieczeństwie (Rozporządzenie 2019/881), „cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami (art. 2 ust. 1). „Cyberzagrożenie" oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych [information system], użytkowników takich systemów oraz innych osób.

Z kolei projekcie nowelizacji UKSC z 7.09.2020 r. proponuje się nowy termin – „bezpieczeństwo sieci i usług" i definiuje się go jako zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność: a) tych sieci lub usług, b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej, c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy [art. 2 pkt 8f projektu]. Jednocześnie, pozostawia się dotychczasową definicję cyberbezpieczeństwa.

Rada zwraca uwagę na niejednoznaczność terminu „cyberbezpieczeństwo". Termin ten jest również wadliwie tłumaczony z języka angielskiego, często jako „bezpieczeństwo cybernetyczne", i „bezpieczeństwo systemów informatycznych" – co, zdaniem Rady wymaga korekty.

Wymagałoby pogłębionej analizy ustalenie czy i w jaki sposób do różnic pomiędzy polską ustawą a unijnym rozporządzeniem odnoszą się reguły kolizyjne, ponieważ przyjęcie poglądu o krzyżowaniu się zakresów ustawy o ksc i rozporządzenia UE 2019/881 pociągałoby za sobą konieczność uchylenia dotychczasowej definicji cyberbezpieczeństwa. Niewątpliwie potrzebne jest wdrożenie procedury corrigendum nieodpowiednich spolszczeń w Dz. Urz. UE Pl. [m.in. cybersecurity jako „bezpieczeństwa cybernetycznego" zamiast cyberbezpieczeństwa, a information systems jako systemów informatycznych zamiast systemów informacyjnych] a także zestawienie i adekwatnie objaśnienie innych elementów leksykonu cyberbezpieczeństwa.

Rada rekomenduje uzgodnienie znaczenia terminu cyberbezpieczeństwo jako zbiorczego określenia o rosnącej wadze w różnych kontekstach, dla uzyskania spójności

wielopoziomowej regulacji oraz zestawienie i adekwatne objaśnienie innych elementów siatki pojęciowej. Ułatwi to jasne określenie uprawnień i obowiązków podmiotów krajowego systemu cyberbezpieczeństwa.

Jednocześnie Rada zwraca uwagę na brak cyberbezpieczeństwa w klasyfikacjach rodzajów działalności. Dotyczy to zarówno Międzynarodowej Standardowej Klasyfikacji Rodzajów Działalności (ISIC), Statystycznej Klasyfikacji Rodzajów Działalności Gospodarczej w Unii Europejskiej (NACE), jak i Polskiej Klasyfikacji Działalności (PKD). Działalność ma miejsce wówczas, gdy czynniki takie jak: wyposażenie, siła robocza, technologia produkcji, sieci informacyjne lub produkty są powiązane w celu wytworzenia określonego wyrobu lub wykonania usługi. Działalność charakteryzowana jest przez produkty wejściowe (wyroby lub usługi), proces technologiczny oraz przez produkty wyjściowe. Wyróżnia się działalność: przeważającą, drugorzędną i pomocniczą. Cyberbezpieczeństwo nie jest wyodrębniane jako rodzaj działalności.

Klasyfikacja PKD 2007 stosowana jest do podmiotów gospodarczych dla potrzeb: Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), Krajowego Rejestru Sądowego (KRS), Krajowego Urzędowego Rejestru Podmiotów Gospodarki Narodowej (REGON), Krajowej Ewidencji Podatników (KEP).

Niewyodrębnienie w PKD cyberbezpieczeństwa utrudnia realizację zadań publicznych wyznaczonych podmiotom krajowego systemu cyberbezpieczeństwa i rozwój działalności gospodarczej. Uwaga powyższa dotyczy wprawdzie tylko pośrednio projektu nowelizacji UKSC, ale Rada stoi na stanowisku, że minister właściwy do spraw informatyzacji powinien zainicjować kompleksowe uporządkowanie kwestii związanych z terminologią oraz klasyfikacją działalności związaną z tematyką cyberbezpieczeństwa.

3. Kwalifikacje i umiejętności związane z cyberbezpieczeństwem

Rada zwraca uwagę, że w UKSC brak wyraźnych wymogów w zakresie kwalifikacji, wiedzy i umiejętności.

Art. 14 stanowi, że operator usługi kluczowej w celu realizacji niektórych zadań powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (po nowelizacji ma to być SOC)

Według § 1 ust. 1 pkt 4 rozporządzenia Ministra Cyfryzacji z 4.12.2019. podmiot świadczący usługi z zakresu cyberbezpieczeństwa jest obowiązany w zakresie realizowanych obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 UKSC, dysponować personelem posiadającym umiejętności szczegółowo określone w punktach a-d.

Pojawiają się wątpliwości dotyczące dokumentowania faktu dysponowania odpowiednim personelem [czy ma on posiadać stosowne certyfikaty, szkolenia, itp.] oraz braku wymogów w odniesieniu do personelu wewnętrznych struktur.

Rada zdaje sobie sprawę z różnicy w podejściu do wymogów kwalifikacyjnych w sferze prywatnej i publicznej. Sfera prywatna jest z jednej strony często lepiej motywowana do podnoszenia kwalifikacji, z drugiej – wszelkie ustawowe wymogi tego typu traktuje jako dodatkowe, kosztowne obowiązki nakładane na sektor gospodarczy. W sferze publicznej z kolei, brak ustawowych wymogów co do posiadania określonych kwalifikacji powoduje niechęć do wydawania publicznych pieniędzy na te cele, a tym samym brak motywacji do podnoszenia poziomu umiejętności. W raporcie NIK z 2019 r. dotyczącym zapewniania bezpieczeństwa e-usług oceniono krytycznie 70% badanych podmiotów publicznych.

Pewnym wzorem mogą być przepisy dotyczące ochrony danych osobowych dotyczące inspektorów ochrony danych. W art. 37 ust. 5 RODO stanowi, że Inspektor ochrony danych wyznaczany jest na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk ochrony danych oraz umiejętności wypełniania swoich zadań. Do szkolenia innych osób upoważnianych do przetwarzania, mobilizują administratorów zasada rozliczalności i dolegliwe sankcje.

Rada stoi na stanowisku, że efektywność nowych regulacji cyberbezpieczeństwa może być ograniczona ze względu na niewystarczający potencjał kadrowy, zwłaszcza SOC i CSIRT sektorowych. W związku z tym Rada rekomenduje, aby w UKSC umieścić przepisy skłaniające do podnoszenia kwalifikacji.

Wiesław Paluszyński

Dokument podpisany przez Wiesław Paluszyński
Data: 2020.10.06 09:55:09 CEST

Przewodniczący Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Polskie Towarzystwo Informatyczne; Lider Projektu
ul. Solec 38 lok. 103 | 00-394 Warszawa
tel.: + 48 22 838 47 05 | fax: + 48 22 636 89 87
e-mail: wieslaw.paluszynski@piit.org.pl
www.radasektorowa.pl

PARP Grupa PFR

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo