UWAGI W RAMACH UZGODNIEŃ Z KOMISJĄ WSPÓLNĄ RZĄDU I SAMORZĄDU TERYTORIALNEGO

Informacja o projekcie:

Tytuł	Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw
Autor	Ministerstwo Cyfryzacji
Projekt z dnia	3 października 2024 r.

Informacje o zgłaszającym uwagi:

Urząd	----------
Organizacja samorządowa	Związek Powiatów Polskich
Osoba do kontaktu	Patrycja Grebla-Tarasek
e-mail	biuro@zpp.pl
tel.	18 477 86 00

Uwagi:

Lp.	Część dokumentu, do którego odnosi się uwaga (np. art., nr str., rozdział)	Treść uwagi (propozycja zmian)	Uzasadnienie uwagi	Stanowisko resortu	Odniesienie do stanowiska resortu
1.	Uwaga ogólna	Projektodawca zmienia w zasadzie całą treść ustawy o krajowym systemie cyberbezpieczeństwa. Przez to zmiany są nieczytelne. Z punktu widzenia przestrzegania zasad techniki prawodawczej (§84) powinna być opracowana nowa ustawa.			
2.	Uwaga ogólna	Konieczność dostosowania języka do odbiorców. Po raz kolejny mamy do czynienia z projektem ustawy przygotowanym przez resort cyfryzacji, który jest napisany językiem niezrozumiałym dla odbiorcy, nawet jeżeli posiada wykształcenie techniczne albo prawnicze.	Zgodnie z § 6 zasad techniki prawodawczej ustawy należy redagować tak aby dokładnie i w sposób zrozumiały dla adresatów zawartych w nich norm wyrażały intencje prawodawcy. Projektowana ustawa zasady tej nie wypełnia. Problemy z jej zrozumieniem pojawiają się już momencie czytania definicji zawartych w słowniku ustawy. Wyrażenia kluczowe zdefiniowane w nim są zdecydowanie za długie, co później		

			sprawia, że cała ustawa jest „przegadana”. Należy pamiętać do kogo projektodawca kieruje ustawę, w przypadku samorządów, problemem po raz kolejny nie będzie brak chęci wdrażania zmian a niezrozumienie jakie zmiany należy wprowadzić, właśnie ze względu na język jakim napisana jest ustawa. Nawet Dyrektywa 2022/2555 napisana jest w bardziej przystępny sposób. Ponadto, zwracamy uwagę, że ustawa nie jest napisana zgodnie z regułami składni języka polskiego (§7 zasad techniki prawodawczej). Przykład: art. Art. 7f ust. 6 W przypadki **niewyrażenia odmowy wykreślenia** z wykazu w terminie miesiąca organ właściwy do spraw cyberbezpieczeństwa wykreśla podmiot z wykazu w odpowiednim zakresie. W polskim systemie prawnym powszechnie stosuje się praktykę, że wpisanie/wykreślenie z różnych rejestrów następuje w trybie czynności materialno-technicznej a odmowa w formie decyzji albo innego aktu administracyjnego. Jednak konstrukcja przepisów jakie zaproponowano w omawianym projekcie jest niespotykana. Na marginesie z proponowanych przepisów ostatecznie nie wynika w jakim terminie nastąpi wykreślenie bowiem przy takiej konstrukcji		

			określony jest tylko termin na wydanie aktu odmowy. Pobocznie również niezrozumiałym jest dlaczego wybrano inną czynność z zakresu administracji publicznej a nie decyzję administracyjną z wyłączeniem przepisów o odwołaniu/ponownym rozpatrzeniu sprawy. Sąd administracyjny żeby ocenić zasadność odmowy i tak będzie wymagał uzasadnienia aktu.		
3.	Art. 2 pkt 8 a ustawy o krajowym systemie cyberbezpieczeństwa	Potrzeba wyjaśnienia kto będzie odpowiadał w przypadku naruszenia, w przypadku zarządu wieloosobowego, również w kontekście odpowiedzialności indywidualnej, o której mowa w art. 73a	Zgodnie z art. 3 ust. 1 pkt 6 ustawy o rachunkowości przez kierownika jednostki administracyjnej rozumie się członka zarządu lub innego organu zarządzającego, a jeżeli organ jest wieloosobowy - członków tego organu, z wyłączeniem pełnomocników ustanowionych przez jednostkę. W przypadku spółki jawnej i spółki cywilnej za kierownika jednostki uważa się wspólników prowadzących sprawy spółki, w przypadku spółki partnerskiej - wspólników prowadzących sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej - komplementariuszy prowadzących sprawy spółki. W świetle powyższego, należy zadać pytanie po pierwsze **jak będą odpowiadali członkowie zarządów kolegialnych** – czy pojedynczo czy solidarnie? Pytanie jest istotne w kontekście wieloosobowego zarządu		

			JST lub samorządowych spółek prawa handlowego.		
4.	Art. 2 pkt 11c ustawy o krajowym systemie cyberbezpieczeństwa	Wnosimy o zawężenie definicji podmiotu publicznego w zakresie zgodnym z Dyrektywą 2022/2555. Dyrektywa zobowiązuje do wprowadzenia przepisów dotyczących cyberbezpieczeństwa w samorządach na poziomie regionalnym. Ponadto przy takiej konstrukcji przepisów w przypadku JST pojawia się problem kto będzie podmiotem publicznym (dublowanie zadań i odpowiedzialności). Jest to szczególnie istotne w kontekście braku oszacowania kosztów wdrożenia ustawy po stronie JST, przy bardzo szczegółowym oszacowaniu kosztów administracji rządowej.	Zakres podmiotów publicznych zobowiązanych do stosowania przepisów Dyrektywy 2022/2555 zawarty jest w art. 2 ust. 2 pkt f pkt 11. Dyrektywa wskazuje, że zakresem powinny zostać objęte samorządy na poziomie regionalnym, tym czasem polski ustawodawca rozszerza zakres na podmioty na poziomie lokalnym jakim są niewątpliwie powiaty i gminy – z czym kategorycznie się nie zgadzamy. Przepisy projektowanej ustawy traktują wskazany zakres rozszerzająco. Zgodnie z zapisami zaproponowanymi przez projektodawcę wszystkie jednostki sektora finansów publicznych, traktowane będą jako kluczowe. Co oznacza, że pod definicję podmiotu publicznego będą podpadać zarówno samorządy jak i organy tych jednostek, de facto dublując pewne obowiązki (pobocznie zauważamy, że podobny problem wystąpił np. w ustawie o doręczeniach elektronicznych). Trzeba również zauważyć, że nie do końca zasadnym wydaje się nakładanie obowiązków, o których mowa w projekcie na małe podmioty np. przedszkola, żłobki, placówki opiekuńczo-wychowawcze, placówki wsparcia dziennego, domy kultury.		

5.	Art. 2 pkt 14 ustawy o krajowym systemie cyberbezpieczeństwa	Konieczność zawężenia definicji systemu informacyjnego.	Obecna definicja traktuje system informacyjny niezwykle szeroko. W jej świetle, smartfon może będzie traktowany jako system teleinformacyjny, co rodzi poważne konsekwencje w świetle obowiązków przedstawionych w projekcie ustawy.		
6.	Art. 2a ustawy o krajowym systemie cyberbezpieczeństwa	Doprecyzowanie przepisu, w obecnym kształcie przepis, wskazuje, że każde zadanie jakie realizuje samorząd będzie traktowane jak usługa w rozumieniu ustawy. Biorąc pod uwagę charakter zadań realizowanych przez samorządy przepis jest niezrozumiały i w naszej ocenie nieprzemyślany przez projektodawcę.	Po pierwsze w samej ustawie brakuje definicji pojęcia „usługa”, co rodzi wątpliwości natury interpretacyjnej – co w rozumieniu ustawy jest usługą i czy każde zadanie realizowane przez samorząd należy traktować jako usługę.		
7.	Art. 5 ust. 1 pkt 4 lit. d ustawy o krajowym systemie cyberbezpieczeństwa	Zawężenie definicji podmiotu publicznego, co powiązane jest z definicją podmiotu kluczowego.	Uzasadnienie uwagi jak do uwagi nr 4.		
8.	Art. 5 ust. 8 ustawy o krajowym systemie cyberbezpieczeństwa	Podwyższenie liczby zatrudnionych w podmiotach leczniczych, które determinują zakwalifikowanie do kategorii podmiotu ważnego lub kluczowego.	Projektodawca bardzo nisko stawia próg w zakresie liczby zatrudnionych w podmiotach leczniczych. Próg 50 osób zatrudnionych, jest w stanie osiągnąć nawet mała przychodnia, w której przejmują pacjentów lekarze kilku specjalności w wymiarze dziesiętnych części etatu, stąd też progi te wymagają podniesienia.		
9.	Art. 7b ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa	Potrzeba doprecyzowania w zakresie możliwości odwołania od wpisu do wykazu z urzędu.	Wyjaśnienia wymaga czy podmioty publiczne będą mogły wnieść sprzeciw do wpisu do wykazu podmiotów kluczowych lub podmiotów ważnych. Czy wpis będzie dokonywał się automatycznie, po numerze REGON.		

10.	Art. 7b ust. 6 ustawy o krajowym systemie cyberbezpieczeństwa	Od kiedy liczony będzie termin na wykreślenie – od niewyrażenia odmowy wykreślenia czy od dnia złożenia wniosku.			
11.	Art. 8 uwaga ogólna ustawy o krajowym systemie cyberbezpieczeństwa	W ustawie pominięto definicję wielu pojęć, dla przykładu nie jasne są: - personel podmiotu (brak definicji w projekcie i w ustawie o krajowym systemie cyberbezpieczeństwa), - polityka tematyczna (brak definicji w projekcie i w ustawie o krajowym systemie cyberbezpieczeństwa).			
12.	Art. 8 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa	Obowiązki określone w ustawie wskazane są po pierwsze bardzo szeroko po drugie na poziomie całkowicie abstrakcyjnym i niezrozumiałym.	Należy obowiązki te poddać ponownemu przeglądowi i nadać im po pierwsze sensowne znaczenie, które da się przełożyć na rzeczywistość po drugie zaś doprecyzować. Tak wyrażone obowiązki, będą miały wpływ na ich wykonywanie przez samorządy. Dla przykładu co ustawodawca ma na myśli pod sformułowaniem: „ bezpieczeństwo i ciągłość dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym”? **Proszę o wyjaśnienie i wskazanie jakie konkretne działania ma podjąć samorząd, aby wypełnić ten obowiązek.** **Istnieje poważna obawa, że tak niezrozumiałe zapisy przyczynią się jedynie do konieczności zakupu (od kilku firm, które znalazły niszę w rynku) sztampowych dokumentów**		

			zasad i polityk, nijak nie mających przełożenia na zadania realizowane w samorządach i ich zasady działania.		
13.	Art. 8 ust. 2 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa	Konieczność doprecyzowania obowiązku.	Co projektodawca ma na myśli wskazując, że podmiot kluczowy uwzględnia podatności związane z dostawcą sprzętu lub oprogramowania. Zdanie to nie jest wyrażone w języku polskim – jest to kalka z tłumaczenia. Brakuje jakie „podatności" należy wziąć pod uwagę albo "podatności" na co. Samo słowo podatności nie wskazuje co konkretnie należy wziąć pod uwagę.		
14.	Art. 8c ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa	Przepis wymaga doprecyzowania.	Projekt ustawy w dalszej części zakłada możliwość wspólnej obsługi w zakresie obowiązków nakładanych w projekcie ustawy – w związku z tym rodzi się pytanie czy odpowiedzialność, a jeżeli tak to jaka poniesie kierownik jednostki, której obowiązki wynikające z ustawy będą realizowane przez jednostkę obsługującą?		
15.	Art. 8c ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa	Skreślenie lub modyfikacja przepisu.	Przepis budzi wątpliwości. Nie po to kierownik, ceduje na kogoś obowiązki, aby później ponosił odpowiedzialność za ich niewłaściwe wykonanie. Musimy mieć na uwadze, że kierownik może nie mieć zarówno wpływu na osobę której powierzono obowiązek jak i kompetencji do tego, żeby badać prawidłowość realizacji obowiązku. Logicznym jest, że skoro kierownik jednostki organizacyjnej nie posiada wiedzy w		

			jakiejś specjalistycznej dziedzinie zatrudnia do tego celu specjalistę. Nie można wymagać np. od dyrektora szpitala, aby był ekspertem w zakresie cyberbezpieczeństwa.		
16.	Art. 8e ustawy o krajowym systemie cyberbezpieczeństwa	Urealnienie obowiązku, poprzez wydłużenie ważności szkolenia lub nałożenie obowiązku na MC organizacji takich szkoleń dla sektora publicznego.	Obowiązek szkolenia raz w roku kierowników, w szczególności podmiotów ważnych, w zakresie cyberbezpieczeństwa jest całkowitą fikcją. Przepis spowoduje jedynie, zwiększenie sprzedaży szkoleń (i wydatków jednostek samorządu terytorialnego na ten cel) przez komercyjne firmy, a nie zwiększenie wiedzy kierowników jednostek.		
17.	Art. 9 ust. 1 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa	Liczba osób wyznaczonych winna być dostosowana do wielkości podmiotu.	Kogo należy wyznaczyć w małych jednostkach np. przedszkolach – po dwóch nauczycieli, należy pamiętać, że kadra w takich jednostkach jest bardzo ograniczona liczbowo. Ustawa winna rozróżniać podmioty ze względu na ich wielkość i stopień znaczenia dla systemu cyberbezpieczeństwa.		
18.	Art. 9 ust. 1 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa	Przepis wymaga doprecyzowania.	Po pierwsze nie wiadomo do jakiej usługi należy przygotować informację. Do każdej usługi świadczonej w samorządach osobno? Czy do usługi „udostępniania karty usługi" w sieci za pośrednictwem strony internetowej czyli mówiąc wprost wskazania jakie dokumenty należy wypełnić i przynieść do urzędu, aby np. zarejestrować samochód należy przygotować odrębną informację w zakresie cyberbezpieczeństwa? W końcu jest		

			to usługa publiczna świadczona przez podmiot zobowiązany, zgodnie z przepisami ustawy. Pobocznie zwracamy uwagę, że projekt ustawy jest pełen takich niedomówień i absurdów.		
19.	Art. 10 ust. 3 i ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa	Proszę o wskazanie w sposób precyzyjny jak dokumenty te mają wyglądać, bo nijak nie idzie informacji tej wywieść z przygotowanej przez projektodawcę definicji. Prosimy posłużyć się konkretnymi przykładami.			
20.	Art. 15 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa	W świetle wskazanego przepisu należy wskazać, że audytów jaki i zapewnienia bezpieczeństwa systemów informacyjnych nie da się wykonać bezkosztowo.	Co prawda, ustawodawca wydłuża okres na przeprowadzenie audytu z 2 do 3 lat, zakres audytu będzie kilkukrotnie zwiększony w porównaniu do obecnej ustawy.		
21.	Art. 15 ust. 2a ustawy o krajowym systemie cyberbezpieczeństwa	Uwaga techniczna.	Przepis w praktyce spowoduje, kupowanie „sztampowych” audytów od firm komercyjnych, bo w praktyce w małych podmiotach trzeba będzie zlecać audyty firmom zewnętrznym. Po raz kolejny zadajemy sobie pytanie czy projektodawca ma na celu zwiększenie cyberbezpieczeństwa czy pozyskanie kolejnych klientów przez firmy wyspecjalizowane w tym temacie.		
22.	Art. 16c ustawy o krajowym systemie cyberbezpieczeństwa	Zakres obowiązków określony jest bardzo szeroko.	Uwaga ta powiązana jest zarówno z definicją podmiotu publicznego (uwaga nr 4) jak i brakiem definicji usługi, która determinuje to co jest usługą publiczną (uwaga 6).		
23.	Art. 16d ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa	Przepis wymaga doprecyzowania na kilku płaszczyznach.	Przy tak skonstruowanych przez projektodawcę przepisach rodzą się wątpliwości w zakresie tego kto będzie odpowiadał za naruszenie i w		

			jakim zakresie? Czy kierownik jednostki obsługiwanej będzie odpowiadał za naruszenie, a jeżeli tak to na jakich konkretnie zasadach? Problematyczna jest kwestia zasad wyznaczania jednostki do wspólnej obsługi. Ustawy samorządowe określają zasady powierzania obsługi zadań jednostce obsługującej w drodze uchwały organu stanowiącego jst. Przepisy projektowanej ustawy dopuszczają wspólną obsługę ze spółkami prawa handlowego, podczas gdy przepisy ustaw ustrojowych nie dają już takiej możliwości.		
24.	Art. 53 ust. 5 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa	W jaki sposób należy poinformować odbiorców usługi o cyberzagrożeniu?	Od razu zaznaczamy, że nie ma naszej zgody na informowanie odbiorców w sposób listowny z uwagi na gigantyczne koszty takiej operacji.		
25.	Art. 53c ust. 2 pkt 5 ustawy o krajowym systemie cyberbezpieczeństwa	Proponujemy wydłużenie terminu.	Termin przekazania żądanej dokumentacji jest zdecydowanie za krótki, w szczególności w sytuacji gdy będziemy mieli do czynienia z podmiotem obsługiwanym w ramach wspólnej obsługi.		
26.	Art. 53c ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa	Nie jest jasne w jakiej formule, zgodnie z jakimi przepisami należy dokonywać doręczenia żądania.	Czy projektodawcy, chodzi o system informacyjny służący do prowadzenia rejestru podmiotów ważnych i kluczowych? Jeżeli tak to odwołanie do art. 46 ust. 1 pkt 6 jest błędne.		
27.	Art. 53d ust. 1 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa	Zakres dostępu jest określony zdecydowanie zbyt szeroko i może naruszać inne dobra chronione, wskazane w ustawach szczegółowych.	Urzędnik monitorujący powinien mieć dostęp przede wszystkim do miejsc, które są kluczowe z punktu widzenia cyberbezpieczeństwa – ustawa nie może dawać mu prawa do poruszania się swobodnie po		

			całym budynku podmiotu kluczowego czy ważnego. Dla przykładu należy podać wstęp do szpitala np. do sal zabiegowych, gdzie zarówno trzeba przestrzegać standardów sanitarno – epidemiologicznych jak i przepisów dotyczących antyseptyki jak i praw pacjenta do prywatności a także zachowania tajemnicy medycznej. Innym przykładem jest szkoła, gdzie osoby postronne nie powinny mieć wstępu, ze względu na obowiązek chronienia uczniów.		
28.	Art. 67c ust. 1 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa	Data nabycia jest nieprecyzyjna. Decydujące znaczenie w wycofywaniu produktów, powinna mieć data rozstrzygnięcia postępowania o udzielenie zamówienia tak aby nie zachodziła konieczność przeprowadzania ponownie zamówień przetargowych, ewentualnie data zawarcia umowy.			
29.	Art. 67e ustawy o krajowym systemie cyberbezpieczeństwa	Przepis wymaga przeredagowania i doprecyzowania.	Treść przepisu rodzi znaczące wątpliwości w jakim terminie sąd powinien rozpatrzyć skargę na decyzję, o której mowa w art. 67b ust. 15? Proponujemy, aby termin ten wynosił 1 miesiąc, w innym wypadku przepis nie będzie spełniał swojej roli.		
30.	Art. 72a ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa	Potrzeba doprecyzowania.	Wyjaśnienia wymaga, czy Krajowy plan reagowania na incydenty i sytuacje kryzysowe będzie dotyczył także jednostek samorządu terytorialnego? W końcu samorządy realizują również zadania z zakresu zarządzania kryzysowego.		

			Jeżeli odpowiedź na pierwsze pytanie jest twierdząca to wówczas, Rada Ministrów powinna przyjąć plan w drodze rozporządzenia a nie uchwały (czyli aktu wewnętrznego nie wiążącego dla JST).		
31.	Art. 73a ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa	Konieczność weryfikacji przepisów w zakresie kar pieniężnych dla kierowników podmiotów kluczowych i ważnych rozumianych jako samorządy i jego jednostki.	Weryfikacji wymaga, czy aby na pewno uzasadnionym wydaje się, nakładanie kar o tak horrendalnych wysokościach na kierowników jednostek. Dyrektywa nie wymaga, aby środki egzekucyjne wobec kierowników jednostek miały taki charakter i taki wymiar jak przewidziano w projekcie.		
32.	Art. 73a ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa	Zbyt wysoka kara finansowa dla kierowników.	Co prawda kwestionujemy same kary finansowe dla kierowników jednostek co do zasady. Jednak, sama wysokość kary finansowej jest znacząco przesadzona. W świetle problemów z kadrami z jakimi zmagają się samorządy kolejne kary finansowe i to w wysokości aż 6 krotności miesięcznej pensji, mogą problemy te jeszcze bardziej pogłębić.		
33.	Art. 73a ust. 1 w zw. z ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa	Rodzi się pytanie czy karze będą podlegać wszystkie naruszenia łącznie czy też każde osobno?			
34.	Art. 38	Termin wejścia w życie przepisów jest zdecydowanie za krótki.	Nie ma praktycznie żadnej możliwości, aby wdrożyć wszelkie wymagania i zmiany w tak krótkim czasie w jednostkach samorządu terytorialnego. Z przykrością przypominamy, że strona rządowa miała wystarczająco dużo czasu, aby wdrożyć Dyrektywę 2022/2555 w sensownym czasie, pozwalającym na dostosowanie się		

			podmiotów do nowych obowiązków. Nie jest winą samorządów, że po raz kolejny, przygotowanie ustawy wdrażającej przepisy UE, pozostawiono na ostatnią chwilę, o czym świadczy również jakość przedłożonego projektu. **Pobocznie zauważamy, że termin na wdrożenie przepisów minie 17 października br.**		
35.	OSR	OSR przygotowany jest nierzetelnie, w zakresie kosztów jakie będą zmuszone ponieść samorządy w związku z wprowadzeniem przepisów ustawy.	Projektodawca, bardzo dokładnie, wręcz z ogromną skrupulatnością wyliczył sobie koszty, jakie poniesie w związku z dostosowaniem się do przepisów ustawy. Podczas, gdy nie wskazano, żadnych kosztów jakie poniosą samorządy co w konsekwencji prowadzi do tego, że samorządy nie dostaną żadnych środków finansowych na realizację nowych obowiązków.		
36.	OSR Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	W zakresie nałożenia nowych zadań na podmioty lecznicze zauważamy rażące niedofinansowanie. Nie da się wprowadzić tak wyśrubowanych zmian z zakresu cyberbezpioeczeństwa przy braku dodatkowych środków finansowych, skierowanych na ten cel.	Źródłem finansowania samorządowych podmiotów leczniczych są głównie kontrakty z NFZ. Zatem, wprowadzenie nowych obowiązków w zakresie cyberbezpieczeństwa powinno zostać przeprowadzone w ramach zmiany i podniesienia wyceny świadczeń zdrowotnych. Wedle naszej wiedzy AOTMiT nie uwzględnia jednak takich kosztów w wycenie świadczeń zdrowotnych.		