Uwagi Związku Pracodawców Polska Miedź
do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw („projekt nr UC32”)

Lp.	Podmiot wnoszący uwagę	Jednostka redakcyjna, do której wnoszona jest uwaga	Treść uwagi	Propozycja brzmienia przepisu	Uzasadnienie
1	Związek Pracodawców Polska Miedź	art. 1 pkt 13 ustawy zmieniającej w zakresie art. 8f ust. 1 - 2	Wymogi dla osób realizujących zadania art. 8 i 11 powinny być bardziej precyzyjne w zw. z bardzo szerokim obszarem działań i uprawnień w zakresie dostępu do informacji, szczególnie w art. 8h w zakresie zdefiniowanych zakresów przekazywanych informacji, w tym w zakresie wymiany informacji w procesie zarządzania i obsługi incydentów.	Art. 8f 1. Osoba realizująca zadania, o których mowa w art. 8 i art. 11, osoba musi być zdolna do spełnienia wymogów dla zapewnienia ochrony informacji. 2. Weryfikacji, czy osoba realizująca zadania, o których mowa w art. 8 i art. 11 jest zdolna do spełnienia wymogów dla zapewnienia ochrony informacji, dokonuje podmiot kluczowy i podmiot ważny przez weryfikację niekaralności - brak skazania prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji. W uzasadnionych przypadkach podmiot kluczowy i podmiot ważny realizują weryfikacje zdolności osoby do spełnienia wymogów dla	Osoby wykonujące zadania określone m. in. w art. 8 i 11 projektowanej ustawy będą miały faktyczny dostęp do kluczowych informacji. Rekomenduje się doprecyzowanie poprzez jednoznaczne wskazanie katalogu przestępstw, które wykluczają możliwość zrekrutowania i trwania stosunku pracy (danie możliwości zweryfikowania w trakcie prowadzonego postępowania rekrutacyjnego, jak również w trakcie obowiązywano umowy przesłanki skazania za określone przestępstwo nastąpi). Nie tylko skazanie za przestępstwa przeciwko ochronie informacji mogą rzutować na należytą opinię i prawidłowe wykonywanie powierzonych obowiązków. Pod rozwagę należy wziąć okoliczność, czy i w jakim zakresie osoby wykonujące zadania określone w art. 8 i 11 projektowanej ustawy w pewnym zakresie nie powinny być kwalifikowane jako posiadające dostęp do informacji niejawnej (kwestia wskazania, że tak

				zapewnienia ochrony informacji przez uzyskanie poświadczenia bezpieczeństwa.	kwalifikować należy dostęp audytora do takiej informacji – zob. art. 15 ust. 4 projektowanej ustawy). W związku z tym, powinna istnieć podstawa prawna dla przeprowadzania postępowań sprawdzających w trybie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. z 2024 r. poz. 632 (dalej: ustawa o ochronie informacji niejawnych). Ograniczenie zakresu weryfikacji spełnienia wymogów dla zapewnienia ochrony informacji jedynie do potwierdzenia niekaralności za przestępstwa przeciwko ochronie informacji jest zbyt wąskie, i w konsekwencji ograniczy możliwości przekazywania informacji stanowiący tajemnice prawnie chronione, co szczególnie obniży skuteczność reagowania na incydenty. Z powyższych względów proponuje się rozszerzenie regulacji, tak aby dać możliwość zwiększenia zakresu weryfikacji o uzyskanie poświadczenia bezpieczeństwa (ustawa o ochronie informacji niejawnych) i w ten sposób umożliwić operacyjne „odblokowanie" działań dla obszarów szczególnie chronionych i obronnych państwa.
2	Związek Pracodawców	art. 1 pkt 12 ustawy zmieniające j w zakresie	W poleceniu zabezpieczającym jest wskazana na możliwość nałożenia obowiązkowego zachowania w postaci „nakazu przeglądu planów ciągłości	Proponuje się alternatywnie: a) zmienić polecenie zabezpieczające tak,	Możliwość nałożenia obowiązku dokonywania przeglądu planów bez uprzedniego wymagania ich prowadzenia stanowi niespójność, która wymaga

	Polska Miedź	art. 8 ust. 1 pkt. 2 lit. e) (w zw. z art. 67g ust. 10 pkt. 2 ustawy zmienianej)	działania i **planów odtworzenia działalności** pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;”. Jednocześnie, na liście zadań wskazanych w art. 8 ust. 1 nie wymienia się posiadania planów ciągłości działania ani planów odtworzenia działalności - mowa jest jedynie o planach awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie. Oczywistym jest, że czynności odtworzenia systemu informacyjnego nie wypełnia wymogów planu ciągłości działania ani odtworzenia działalności - dotyczy jedynie systemu informacyjnego, a nie powrotu do działalności biznesowej.	aby zawierało przegląd planów awaryjnych odtworzenia systemu informacyjnego, lub b) uzupełnić art. 8 o zadania obejmujące także opracowanie i utrzymanie planów ciągłości działania i planów odtworzenia działalności.	odpowiedniej korekty legislacyjnej. Rekomenduje się ponowną weryfikację zadań i obowiązków wynikających z art. 8 i nast. nowelizowanej ustawy. Celem powinno być zapewnienie kompletności w zakresie oczekiwanych obowiązków, które mogą być nałożone na mocy działań prowadzonych w ramach czynności audytowych, kontrolnych i nadzorczych.
3	Związek Pracodawców Polska Miedź	art. 1 pkt 11 ustawy zmieniającej, w zakresie art. 7a ust. 4, art. 7c	Rekomenduje się, aby działania organu właściwego miały formę decyzji administracyjnej, a nie jedynie innej czynności z zakresu administracji publicznej.	Adekwatnie do treści uwagi	Wpisanie lub odmowa wykreślenia podmiotu do/z wykazu niewątpliwie nakładać będzie na podmioty określone obowiązki prawne, w związku z czym rekomenduje się wskazanie, że będzie to dokonywane w drodze decyzji administracyjnej.
4	Związek Pracodawców Polska Miedź	art. 1 pkt 13 ustawy zmieniającej, w zakresie art. 8a	Ważne jest, aby w momencie wydania rozporządzeń na podstawie art. 8a wprowadzić adekwatny okres vacatio legis (rekomendujemy nie krótszy niż 6 miesiące), w zakresie dostosowania i wdrożenia w podmiocie zobowiązanym	Adekwatnie do treści uwagi	

			odpowiednich wymagań dla systemu zarządzania informacjami.		
5	Związek Pracodawców Polska Miedź	art. 1 pkt 20 ustawy zmieniającej, w zakresie art. 15 ust. 1b	Rekomenduje się doprecyzowanie sformułowania, zgodnie z którym nakazanie zlecenia audytu następuje jedynie w sytuacji, gdy podmiot kluczowy lub podmiot ważny nie daje należytej gwarancji wykonania audytu w terminie określonym w ustępie 1. Alternatywnie proponuje się jednoznacznie wskazanie katalogu przesłanek uzasadniających nakazanie takiego dodatkowego działania.	Adekwatnie do treści uwagi	Doprecyzowanie miałoby na celu wykluczenie interpretacji, zgodnie z którą organ właściwy ds. cyberbezpieczeństwa może nakazać przeprowadzenie innych dodatkowych audytów we wskazanym okresie referencyjnym.
6	Związek Pracodawców Polska Miedź	art. 1 pkt 56 ustawy zmieniającej, w zakresie art. 53 ust. 4 i 5 lit. a)	Rekomenduje się, aby także w zakresie nakazania podjęcia określonych czynności dotyczących obsługi incydentu lub wydania ostrzeżenia, które mogą nakładać na podmiot określone czynności, również następowało w formie decyzji administracyjnej.	Adekwatnie do treści uwagi	
7	Związek Pracodawców Polska Miedź	art. 1 pkt 56 ustawy zmieniającej, w zakresie art. 53 ust. 8	W zakresie stosowanych środków rekomendujemy, aby dokładnie wskazać kiedy faktycznie te środki będą mogły być zastosowane, w szczególności w sytuacji, gdy podmiot złoży skargę do WSA i zostanie uwzględniony wniosek złożony w trybie art. 61 ustawy - Prawo o postępowaniu przed sądami administracyjnymi z dnia 30 sierpnia 2002 r. (t.j. Dz. U. z 2023 r. poz. 1634 z późn. zm.).	Adekwatnie do treści uwagi	

8	Związek Pracodawców Polska Miedź	art. 7a ust. 3 oraz przepisy powiązane	Proponujemy zmienić brzmienie sformułowania „adres do doręczeń elektronicznych” na „adres do doręczeń elektronicznych lub adres pocztowy siedziby podmiotu”.	Adekwatnie do treści uwagi w odniesieniu do wszystkich wystąpień sformułowania w treści aktu.	Propozycja uzupełnienia o alternatywne metody komunikacji w okresie przejściowym przed pełnym uruchomieniem e-doręczeń oraz w przypadkach, gdy ten kanał komunikacji pozostawałby niedostępny. Zgodnie z art. 6 ust. 1 pkt 3 ustawy o doręczeniach elektronicznych z dnia 18 listopada 2020 r. (t.j. Dz. U. z 2023 r. poz. 285 z późn. zm.), dopuszczono wskazanie w przepisie odrębnym innych sposobów doręczeń.
9	Związek Pracodawców Polska Miedź	art. 1 pkt 2 lit. j) ustawy zmieniającej, w zakresie pkt 11f)	Projektowana definicja „przedsiębiorcy komunikacji elektronicznej”, pod którym rozumie się „przedsiębiorcę telekomunikacyjnego lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów” jest odmienna od definicji zawartej w rządowym projekcie ustawy - Prawo komunikacji elektronicznej (dalej: „projekt nr UC7”, „PKE”) w art. 2 pkt 39 (cyt. „przedsiębiorca komunikacji elektronicznej – przedsiębiorcę telekomunikacyjnego lub podmiot świadczący <u>publicznie dostępną</u> usługę komunikacji interpersonalnej niewykorzystującą numerów”). Definicja „usługa łączności interpersonalnej” ujęta w projekcie nr UC7 zawiera wyłączenie potencjalnie wpływające na finalną klasyfikację podmiotu zgodnie z proponowana definicją w pkt 11 f).	Adekwatnie do treści uwagi proponujemy zastosowanie jednej, spójnej definicji oraz utrzymanie publicznie dostępnego rejestru przedsiębiorców / dostawców usług komunikacji elektronicznej uznanych za podmioty kluczowe. Każdy podmiot świadczący usługi komunikacji elektronicznej na terenie RP i uznany za podmiot kluczowy powinien być ujęty w ww. rejestrze i podlegać łącznie pod rygor ustaw: Prawo komunikacji elektronicznej oraz o Krajowym Systemie Cyberbezpieczeństwa (dalej: „KSC”).	W zał. nr 1 do projektu (nr UC32) wskazano jako podmioty kluczowe w sektorze Infrastruktura cyfrowa podsektor „Komunikacja Elektroniczna”, a w nim: „Przedsiębiorcę telekomunikacyjnego” oraz „Podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów”. W rozumieniu projektodawcy, zastosowanie precyzyjnej definicji w przypadku „podmiotu kluczowego” jakim będą „dostawcy usług komunikacji elektronicznej” jest istotnym elementem skuteczności KSC. Rządowy projekt ustawy - Prawo Komunikacji Elektronicznej nr UC7, wniesiony do Sejmu RP w dniu 21.05.2024, posługuje się inaczej brzmiącą definicją. Jednoznaczne wskazanie podmiotu kluczowego oferującego usługi w zakresie komunikacji elektronicznej powinno być realizowane analogicznie jak w przypadku

					przedsiębiorców telekomunikacyjnych, z zastosowaniem adekwatnej definicji. Usługi świadczone przez podmioty posiadające status przedsiębiorców telekomunikacyjnych oraz przedsiębiorców komunikacji elektronicznej wykorzystywane między innymi przez inne podmioty kluczowe charakteryzować się powinny gwarantowanym poziomem zapewnienia cyberbezpieczeństwa, czemu w rozumieniu projektodawcy służy nowelizacja KSC. Należy zwrócić też uwagę, że definicja „usługa łączności interpersonalnej" ujęta w Dyrektywie 2018/1972 oraz rządowym projekcie nr UC7 zawiera wyłączenie usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej – co przy specyficznej interpretacji mogłoby prowadzić do wyłączenia podmiotu świadczącego taką usługę z obowiązków ujętych w KSC.
10	Związek Pracodawców Polska Miedź	art. 1 pkt 2 lit. d) ustawy zmieniającej, w zakresie art. 2 pkt 5	Definicja incydentu w brzmieniu: „zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych", w szczególności z uwagi na proponowaną definicję systemu informacyjnego, wydaje się niepełna.	5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, produktu ICT, usługi ICT lub procesu ICT, zdarzenie, które stanowi naruszenie lub	Spójne określenie definicji „incydentu" w ustawach KSC i PKE, a w przypadku stosowania odwołania do norm branżowych również z zapewnieniem zgodności z ich brzmieniem jest kluczowe dla zapewnienia właściwej identyfikacji zagrożeń, zdarzeń i ich obsługi. Spójne rozumienie definicji incydentu przez

			Dodatkowo przy przyjęciu założenia, że uznaje się za spełnienie wymagań art. 8 w sytuacji wdrożenia rozwiązań opartych o wymienione normy, należy przyjąć pogląd że definicja incydentu powinna pozostawać spójna z tymi normami. Również rządowy projekt ustawy nr UC7 odwołuje się do KSC w kwestii tzw. „incydentu telekomunikacyjnego”, który nie wpisuje się w ww. definicję.	bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania oraz każde zdarzenie, które stwarza znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagraża bezpieczeństwu informacji.	wszystkie podmioty zobowiązana do ich wykrywania i ograniczania sprzyja właściwej identyfikacji ryzyk i zagrożeń a przez to właściwemu doborowi zabezpieczeń technicznych i organizacyjnych wymienionych w art. 8.