|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Nazwa projektu dokumentu: Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i ustawy – Prawo telekomunikacyjne (UD 68)*** | | | | |
| **L.p.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** |
|  | **RCL** | Definicje | Projektowana definicja „cyberzagrożenia” (art. 1 pkt 2 lit f projektu ustawy zmieniającej) wymaga uzupełnienia, gdyż w wersji przekazanej w przedstawionym projekcie jej druga cześć jest trudna do odczytania. (…) „w inny sposób niekorzystnie wpłynąć w przypadku systemów informacyjnych, użytkowników takich systemów oraz innych osób;” Nie wiadomo na co może niekorzystnie wpłynąć cyberzagrożenie i do przypadku jakich systemów informacyjnych się odnosi. | Uzupełnienie definicji, zgodnie z merytoryczną decyzją projektodawcy |
|  | **RCL** | Upoważnienia ustawowe | W nowym projekcie ustawy są dokonywane zmiany w przepisach upoważaniających. Przykładowo dokonywana jest zmiana w art. 10 ust. 5 ustawy o KSC. Zgodnie z § 32 ust. 2 ZTP jeżeli zmiana dotyczy zakresu spraw przekazanych do uregulowania, rodzaju aktu lub wytycznych „przyjmuje się, że akt wykonawczy wydany na podstawie tego przepisu upoważniającego traci moc obowiązującą z dniem wejścia w życie przepisu zmieniającego treść przepisu upoważniającego.” W upoważnieniu z art. 10 ust. 5 pojęcie „cyberbezpieczeństwo” zostało zastąpione pojęciem „bezpieczeństwo systemów informacyjnych”. Będzie to powodowało zmianę sposobu określenia zakresu przedmiotowego aktu, co będzie skutkowało koniecznością modyfikacji tytułu oraz § 1 rozporządzenia. | Zasadnym wydaje się zastosowanie przepisu czasowo utrzymującego w mocy zgodnie z § 33 ZTP, w związku z dokonywanymi zmianami przepisów upoważniających. |
|  | **RCL** | Rozdział 5. Obowiązki podmiotu publicznego. Art. 21-25 ustawy o KSC | W zakresie art. 21-25 ustawy o KSC (art. 1 pkt 13-16 projektu ustawy zmieniającej) ponownej analizy wymaga katalog podmiotów objętych obowiązkami, kierowanymi do podmiotów publicznych. Weryfikacji wymaga odesłanie do art. 4 pkt 7-15 ustawy o KSC. Na skutek zmian w katalogu podmiotów objętych krajowym systemem cyberbezpieczeństwa (art. 4 ustawy o KSC), przy jednoczesnym zastosowaniu niezmienionego odesłania do art. 4 pkt 7-15 ustawy o KSC, jako taki podmiot publiczny klasyfikowany będzie również ISAC, o którym mowa w art. 4 pkt 7b ustawy o KSC. Ani ustawa ani uzasadnienie nie wskazują, że ISAC jest obligatoryjnie podmiotem o charakterze publicznym, który powinien być objęty obowiązkami, o których mowa w art. 21-25 ustawy o KSC. | Analiza odesłań do art. 4 ustawy o KSC w związku z projektowaną zmianą treści tego przepisu w zakresie katalogu podmiotów objętych obowiązkami, o których mowa w rozdziale 5 ustawy o KSC. |
|  |  | Art. 22 ustawy o KSC | Krajowym systemem cyberbezpieczeństwa są objęte również związki jednostek samorządu terytorialnego oraz związki metropolitalne (na mocy odesłania do art. 9 pkt 2 i 2a ustawy o finansach publicznych) oraz samorządowe zakłady budżetowe (odesłanie do art. 9 pkt 4 ustawy o finansach publicznych). Zmiana w art. 22 ustawy o KSC, wprowadzana projektem ustawy zmieniającej, zobowiązuje jednostki samorządu terytorialnego do przekazywania informacji o incydentach również wojewodzie. | Wymaga wyjaśnienia czy związki jednostek samorządu terytorialnego, związki metropolitalne czy samorządowe zakłady budżetowe będą również zobowiązane do zgłaszania incydentów wojewodzie czy też obowiązek ten będzie dotyczył jedynie jednostek samorządu terytorialnego. |
|  |  | Rozdział 5a. Zadania i obowiązki ISAC w ramach krajowego systemu cyberbezpieczeństwa | Ze względu na to, że wpis do wykazu ISAC nie warunkuje prowadzenia działalności jako ISAC ani umożliwia współpracy z podmiotami krajowego systemu cyberbezpieczeństwa funkcja wykazu ISAC prowadzonego przez ministra właściwego do spraw informatyzacji nie jest zrozumiała. W projektowanym kształcie może on stanowić bazę danych kontaktowych podmiotów gotowych do wykonywania zadań ISAC. Powstaje także wątpliwość czy mogą wykonywać zadania ISAC podmioty nie objęte wykazem i czy wykreślenie z wykazu, o którym mowa w art. 24a ust. 11 stanowi skuteczny środek zapobiegania naruszeniom przepisów i zasad współpracy w ramach krajowego systemu cyberbezpieczeństwa. | Przedstawienie wyjaśnienia i stosowna korekta przepisów po ich ponownej analizie. |
|  |  | Art. 26 ustawy o KSC | W związku z poszerzeniem katalogu podmiotów krajowego systemu cyberbezpieczeństwa weryfikacji wymaga zakres właściwości poszczególnych CSIRT poziomu krajowego, o którym mowa w art. 26 ust. 5-7 ustawy o KSC. Przykładowo, zgodnie z art. 26 ust. 6 ustawy o KSC, do zadań CSIRT NASK należy koordynacja obsługi incydentów zgłaszanych przez jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2-6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Tymczasem zgodnie z art. 4 ustawy o KSC, podmioty, o których mowa w art. 9 pkt 11 i 12 ustawy o finansach publicznych – czyli uczelnie publiczne oraz Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne – nie zostały objęte odesłaniem do art. 9 pkt 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Na gruncie ustawy o KSC funkcjonują jako podmioty systemu szkolnictwa wyższego na mocy odesłania do art. 7 ust. 1 pkt 1 i 3-7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce. Katalog z art. 7 ustawy – Prawo o szkolnictwie wyższym i nauce obejmuje również instytuty badawcze, takie jak instytuty naukowe PAN, instytuty badawcze, działające na podstawie ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, międzynarodowe instytuty naukowe utworzone na podstawie odrębnych ustaw działające na terytorium Rzeczypospolitej Polskiej, Centrum Łukasiewicz, działające na podstawie ustawy z dnia 21 lutego 2019 r. o Sieci Badawczej Łukasiewicz, instytuty działające w ramach Sieci Badawczej Łukasiewicz oraz Polską Akademię Umiejętności. Tymczasem art. 26 w ust. 6 pkt 1 lit. c ustawy o KSC wskazuje jedynie, że zakresem właściwości CSIRT NASK są objęte instytuty badawcze – bez odwoływania się do specyfiki tych instytutów określonej w art. 7 ustawy – Prawo o szkolnictwie wyższym i nauce, co może powodować trudności interpretacyjne. Kwestia ta wymaga uzupełnienia. Podobnie nie zostało rozstrzygnięte do właściwości którego z CSIRT poziomu krajowego należeć będzie obsługa incydentów zgłaszanych przez osobno wskazane w art. 4: Wody Polskie oraz Polski Funduszu Rozwoju (art. 1 pkt 4 lit. d projektu ustawy zmieniającej). Ogólny przepis art. 26 ust. 6 pkt 1 lit. k ustawy o KSC wskazujący na właściwość CSIRT NASK w zakresie innych podmiotów niż wymienione w lit. a-j i ust. 5 i 7 art. 26 nie jest w tym przypadku wystarczający. Weryfikacji wymaga również zakres właściwości przekazanej w drodze porozumienia pomiędzy poszczególnymi CSIRT na podstawie art. 26 ust. 10 i 11 ustawy o KSC. Sugeruje się przegląd zawartych porozumień celem dostosowania właściwości rzeczowej CSIRT poziomu krajowego, która jest określona w ustawie do zakresu faktycznie wykonywanych zadań. Nie kwestionując możliwości zawarcia porozumień, co do zakresu zadań wykonywanych na rzecz niektórych podmiotów, zwłaszcza w przypadku powstania nowych kategorii podmiotów objętych krajowym systemem cyberbezpieczeństwa, zasadnym wydaje się dostosowanie przepisów ustawy do praktyki jej stosowania wynikającej z zawartych porozumień. Kwestię te pozostawia się jednakże do decyzji merytorycznej projektodawcy. W razie wzięcia pod uwagę tego problemu, konieczne będzie uzupełnienie projektu o stosowne przepisy przejściowe i dostosowujące dotyczące zwartych porozumień ich utrzymania, uchylenia czy wygaszenia. | Rozstrzygnięcie właściwości CSIRT poziomu krajowego dla:  1. podmiotów systemu szkolnictwa wyższego i nauki  2. Państwowego Gospodarstwa Wodnego „Wody Polskie”  3. Polskiego Funduszu Rozwoju  4. Rozstrzygnięcie o właściwości CSIRT w kontekście porozumień zawartych pomiędzy CSIRT poziomu krajowego. |
|  |  | Relacja do ustawy o ponownym wykorzystywaniu informacji sektora publicznego, art. 37 ustawy o KSC | W związku z szeroką definicją pojęcia „informacja sektora publicznego”, które jest projektowane w ustawie o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego,[ *informacja sektora publicznego – każdą treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będącą w posiadaniu podmiotu zobowiązanego]* oraz faktem, że katalog podmiotów zobowiązanych do udostępniania informacji sektora publicznego pokrywa się z katalogiem podmiotów objętych systemem cyberbezpieczeństwa wymaga analizy możliwość wyłączenia stosowania przepisów ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego do części informacji będących w posiadaniu podmiotów zobowiązanych dotyczących cyberbezpieczeństwa. Definicja informacji sektora publicznego nie wiąże tego pojęcia z zakresem pojęcia „informacja publiczna” w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Tym samym nie będzie wystarczające wyłączenie stosowanie ustawy o dostępie do informacji publicznej, o którym mowa w art. 37 ustawy o KSC. Ustawa o KSC nie formułuje także osobnej definicji prawnie chronionej tajemnicy w zakresie cyberbezpieczeństwa, a zatem informacje te nie będą objęte wyłączeniem dotyczącym tych tajemnic zawartym w projekcie ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. | Wyłączenie informacji przetwarzanych przez poszczególne podmioty systemu cyberbezpieczeństwa lub poszczególnych kategorii informacji sektora publicznego z możliwości ich ponownego wykorzystywania. Wyłączenie to jak się wydaje nie powinno obejmować danych stanowiących informacji publiczną, które są publikowane w BIP. |
|  |  | Art. 39 ustawy o KSC | W związku z wprowadzeniem CSIRT sektorowych oraz ISAC i SOC wymaga analizy czy przepis art. 39 dotyczący przetwarzania danych o incydentach, w tym danych osobowych, nie wymaga uzupełnienia o zadania realizowane przez CSIRT sektorowe, ISAC czy SOC. Zwłaszcza w kontekście przetwarzania danych osobowych. | Przeanalizowanie przepisów pod kątem nowych zadań i nowych podmiotów oraz ewentualne uzupełnienie odesłań w art. 39 ustawy o KSC lub stworzenie osobnej regulacji dotyczącej przetwarzania danych, w tym danych osobowych przez SOC i ISAC. |
|  |  | Rozdział 11a. Krajowy system certyfikacji cyberbezpieczeństwa | W opisanej procedurze dotyczącej zatwierdzenia certyfikatu (art. 59o i art. 59q ustawy o KSC) projektodawca posługuje się pojęciem „przesłania” i „doręczenia” nie precyzując jednak w jakim trybie następuje przesłanie wniosku oraz doręczenia decyzji. Czy odnosi się ono do doręczenia za pośrednictwem operatora pocztowego czy przy użyciu środków komunikacji elektronicznej.  Podobnie rozstrzygnięcia wymagają kwestie proceduralne dotyczące sposobu informowania o cofnięciu certyfikatu przez jednostkę oceniającą zgodność (art. 59u ustawy o KSC).  Upoważnienie ustawowe z art. 59w ustawy o KSC, przekazujące do uregulowania w drodze rozporządzenia wysokość opłat za zatwierdzenie certyfikatu, może wymagać uzupełnienia, gdyż przepisy ustawy nie rozstrzygają sposobu czy trybu wnoszenia takiej opłaty.  W zakresie art. 59za ustawy o KSC, który wskazuje, że jednostki oceniające zgodność publikują na swojej stronie internetowej „procedurę postępowania ze skargami, o których mowa w art. 63 rozporządzenia 2019/881” (art. 59za ust. 1 ustawy o KSC) i „informują o prawie do skierowania sprawy do sądu” (art. 59za ust. 4) ustawa powinna przesądzać do jakiego sądu może być skierowana taka sprawa (powszechnego czy administracyjnego), a co a tym idzie w jakiej procedurze będzie rozpatrywana. Procedurę administracyjną (zgodnie z ar. 59zc ustawy o KSC) stosuje się jedynie do skarg na jednostkę oceniającą zgodność kierowanych do ministra właściwego do spraw informatyzacji. | Uzupełnienie regulacji o przepisy proceduralne dotyczące sposobu wnoszenia wniosku i sposobu dokonywania doręczeń lub o stosowne odesłanie.  Analiza i ewentualne uzupełnienie upoważnienia ustawowego.  Określenie sądu właściwego, procedury i trybu rozpoznawania spraw związanych, ze skargami o których mowa w art. 63 rozporządzenia 2019/881. |
|  |  | Rozdział 11b. Operator sieci komunikacji strategicznej | Szczegółowego uzasadnienia wymaga umieszczenie regulacji dotyczących operatora sieci komunikacji strategicznej w ustawie o krajowym systemie cyberbezpieczeństwa, nie natomiast w ustawie – Prawo telekomunikacyjnej lub ustawie o zarządzaniu kryzysowym. Art. 59zd ustawy o KSC wskazuje, że zadania operatora sieci komunikacji strategicznej odnoszą się do „(…) zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji”. Nie dotyczą zatem zadań z zakresu krajowego systemu cyberbezpieczeństwa. Nie kwestionując związku funkcjonalnego pomiędzy zapewnieniem bezpieczeństwa sieci telekomunikacyjnej a wykonywaniem zadań dotyczących cyberbezpieczeństwa przepisy ustawy powinny wskazywać jakie zadania z zakresu krajowego systemu cyberbezpieczeństwa wykonuje operator sieci strategicznej. Należy również zauważyć, że zgodnie z art. 2 ust. 2 pkt 1 ustawy o KSC nie stosuje się do przedsiębiorców telekomunikacyjnych w zakresie wymogów bezpieczeństwa i zgłaszania incydentów, zaś operator sieci strategicznej zgodnie z projektowanymi przepisami jest przedsiębiorcą telekomunikacyjnym. Odesłania do przepisów Prawa telekomunikacyjnego (np.: w projektowanym art. 59ze) oraz wskazanie, że w razie niezawarcia umowy o dostęp do sieci telekomunikacyjnej przez operatora telekomunikacyjnego Prezes UKE wydaje decyzję w tym zakresie, wskazują, że przepisy te należy wiązać z wykonywaniem zadań na rzecz obronności i bezpieczeństwa państwa przez operatorów telekomunikacyjnych. Przepisy te regulował dotychczas dział VIII ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne pt. „Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego”. W projektowanych przepisach pojawiają się także pojęcia i zadania dotyczące „ zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej”, a zatem powiązane z wykonywaniem zadań na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Wymaga zatem wyjaśnienia czy projektowane przepisy nie stanowią materii ustawy – Prawo telekomunikacyjnej lub ustawy o zarządzaniu kryzysowym. | Przedstawienie szczegółowego wyjaśnienia oraz powiązanie regulacji zgodnie z jej zakresem przedmiotowym, na poziomie normatywnym, z wykonywaniem zadań z zakresu cyberbezpieczeństwa. |
|  |  | Art. 62a ustawy o KSC | Przepisy dotyczące przyznawania dodatkowego wynagrodzenia dla osób zatrudnionych przy wykonywaniu zadań dotyczących cyberbezpieczeństwa wymagają korekty. Z przepisów nie wynika, czy dodatkowe wynagrodzenie ma charakter jednorazowy, stanowi dodatek do wynagrodzenia zasadniczego, stanowi dodatek za wykonywanie konkretnego zadania czy ma charakter stały, wypłacany miesięcznie? Budzi wątpliwości umieszczenie tej regulacji w przepisach ustawy o krajowym systemie cyberbezpieczeństwa, bez odniesienia zasad i trybu przyznawania tego wynagrodzenia w przepisach stanowiących podstawę wynagradzania dla osób zatrudnionych w tych podmiotach. Może to rodzić trudności w ich stosowaniu, gdyż na podstawie projektowanego aktu nie można przesądzić czy podstawą do wypłaty dodatkowych środków będzie zawierana dodatkowo umowa (nie przesądzając o dopuszczalności jej zawarcia w poszczególnych podmiotach), fakt wykonywania zadań, wydane polecenie w tym zakresie czy sam fakt zajmowania stanowiska związanego z cyberbezpieczeństwem? Podobnie nie został przesądzony charakter tego świadczenia z punktu widzenia przepisów dotyczących ubezpieczenia społecznego oraz pobierania zaliczki na podatek dochodowy czy wliczania ich wysokości do obliczania innych świadczeń pracowniczych, zależnych od średniego wynagrodzenia w danym okresie (np.: dodatkowe wynagrodzenie roczne). Kwestie te mogą wymagać odrębnego uregulowania w przypadku każdego pracodawcy, należy zatem powiązać te regulacje z przepisami dotyczącymi zasad zatrudniania i wynagradzania w tych jednostkach.  Ponadto budzi wątpliwości wskazanie w normie ustawowej liczby osób, którym takie dodatkowe wynagrodzenie przysługuje. Nie wskazano jak ten limit przełoży się na możliwość przyznawania wynagrodzenia i finansowania w poszczególnych podmiotach: CSIRT NASK, CSIRT MON, ABW oraz w urzędzie obsługującym Pełnomocnika. Normy ustawowe powinny w sposób abstrakcyjny i generalny ustalać warunki przyznawania takiego wynagrodzenia, kwestie zaś limitowania środków i ich podziału na etaty powinny zostać powiązane z zasadami finansowania poszczególnych jednostek oraz obsadzania stanowisk w tych jednostkach. | Powiązanie wynagrodzenia dodatkowego z przepisami normującymi pierwotnie zasady zatrudnienia oraz przyjęcia do służby, a także wynagradzania osób zatrudnionych w CSIRT NASK, CSIRT MON i CSIRT GOV oraz urzędzie obsługującym Pełnomocnika do wskazanych zadań. |
|  |  | art. 62b ustawy o KSC | Uregulowanie wskazujące, że w Dzienniku Urzędowym RP „Monitor Polski” zamieszczane są ogłoszenia zawierające odnośnik do strony internetowej zawierającej treść rekomendacji dotyczących „podejmowania środków technicznych i organizacyjnych mających na celu zwiększenie cyberbezpieczeństwa” budzi wątpliwości. Celem publikowania w dzienniku urzędowym jest praktyczna realizacji konstytucyjnej zasady pewności prawa i zaufania obywateli do państwa przez utrwalenie w sposób nie budzących wątpliwości treści aktów władzy publicznej. Mając na uwadze, że rekomendacje będą skierowane do podmiotów krajowego systemu cyberbezpieczeństwa, a zatem również podmiotów które nie są podmiotami publicznymi (takich jak ISAC czy SOC), zamieszczenie ogłoszenia z odnośnikiem do strony internetowej, która będzie zawierała treść rekomendacji wydaje się nie realizować ww. celu publikacji. Należy podnieść, że treść publikacji na stronie internetowej będzie mogła podlegać modyfikacjom niezależnie od opublikowania odnośnika do jej adresu w Dzienniku Urzędowym RP „Monitor Polski”. Na gruncie projektowanych przepisów nie będzie możliwe ustalenie, w sposób niebudzący wątpliwości, treści rekomendacji na podstawie ogłoszenia opublikowanego w Dzienniku Urzędowym. Dodatkowych, szczegółowych ustaleń wymagają również kwestie techniczne związane z tą publikacją Niezależnie od powyższego należy zauważyć, że projektowane przepisy nie wskazują czy treść rekomendacji może podlegać zmianom oraz czy czas stosowania tych rekomendacji jest określony, a także czy informacja o takiej zmianie jest publikowana, podobnie jak informacja o wygaśnięciu danej rekomendacji. | Ponowna analiza i zmiana przepisów. |
|  |  | Art. 66b ust. 3 ustawy o KSC | Zgodnie z projektowaną regulacją „3. Podmioty o których mowa w art. 66 ust. 1 pkt 1-4, do których stosuje się ustawa – Prawo zamówień publicznych, nie dokonują zamówień sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 8”, a zatem decyzji o uznaniu dostawcy usług lub oprogramowania za dostawcę wysokiego ryzyka. Przepis budzi wątpliwości, gdyż sformułowanie „nie dokonuje zamówień” nie precyzuje jaki skutek dla postępowania w sprawach zamówień publicznych wywołuje decyzja o uznaniu dostawcy za podmiot wysokiego ryzyka. Skutek ten będzie się różnił w zależności od etapu postępowania o udzielenie zamówienia publicznego. W tym kształcie regulacja nie przesądza czy zamawiający powinien umorzyć postępowanie w sprawie zamówienia publicznego (wówczas należałoby uzupełnić przesłanki umorzenia postępowania zawarte w ustawie PZP), odrzucić ofertę wykonawcy, który został uznany za dostawcę wysokiego ryzyka (wówczas koniecznym wydaje się uzupełnienie przesłanek odrzucenia oferty), ani nie wskazuje jaki skutek wywołuje uznanie dostawcy za dostawcę wysokiego ryzyka w sytuacji, w której została zawarta umowa, która przewiduje realizację zamówienia w częściach albo umowa periodyczna. Czy umowa ta powinna zostać wypowiedziana, i wszczęte nowe postępowanie w sprawie o udzielenie zamówienia publicznego czy też umowa ta może być kontynuowana aż do upływu okresu, w którym dany sprzęt lub oprogramowanie powinny zostać wycofane?  Należy również podnieść, że zaproponowana redakcja przepisu wydaje się nieadekwatna do jej celu. Przyjmując, że celem regulacji jest ograniczenie możliwości nabywania sprzętu lub oprogramowania, które zostały objęte decyzją, o której mowa w art. 66a ust. 8 ustawy o KSC, to nie ma znaczenia w jakiej procedurze nabywana jest ten sprzęt lub oprogramowanie i czy podmiot stosuje do tej procedury zakupu postępowanie w sprawach zamówień publicznych. Przepis w takim przypadku powinien stanowić o niemożliwości zakupu przedmiotów objętych decyzją z art. 66a ust. 8 ustawy o KSC. | Przepis wymaga ponownej analizy, w szczególności co do trafności przyjętego rozwiązania, i korekty. |
|  |  | Art. 66d ustawy o KSC | Przepisy dotyczące ograniczenia zakresu doręczanego uzasadnienia wyroku oraz wyłączenia możliwości wstrzymania natychmiastowej wykonalności decyzji o uznaniu dostawcy usług za podmiot wysokiego ryzyka wymagają ponownej analizy w zakresie spójności z regulacjami ustawy – Prawo o postępowaniu przed sądami administracyjnymi i ustawą o ochronie informacji niejawnych. Niezależnie od dopuszczalności ograniczenia doręczenia pocztowego ze względu na ochronę informacji niejawnych, z uwagi na prawo do rzetelnego postępowania, strona nie powinna być ograniczona w samym dostępie do uzasadnienia rozstrzygnięcia podejmowanego przez sąd, aby mieć możliwość ich zaskarżenia. | Przepisy wymagają ponownej analizy, w szczególności co do trafności przyjętego rozwiązania, i ewentualnej korekty. |